Report for Domain: unimi.it

Generated by Apollo

September 11, 2024

Contents

1 Summary of Findings

Below are some key statistics from the data provided:

- **Number of IPs**: 733

- **Number of Domains**: 1102

- **Number of Emails**: 81

- **Number of Resolved Hosts**: 1042

- **Number of Mail Servers**: 5

- **Number of URLs**: 61

2 IP Addresses found

Below is the list of IP addresses found:

- 159.149.118.165
- 159.149.116.147
- 159.149.117.157
- 159.149.145.158
- 159.149.47.101
- 3.126.205.183
- 159.149.116.132
- 159.149.117.190
- 159.149.118.106
- 159.149.117.148
- 159.149.117.152
- 159.149.117.142
- 34.252.50.82
- 159.149.116.34
- 159.149.116.104
- 159.149.118.207
- 3.70.101.28
- 159.149.118.191
- 159.149.119.203
- 159.149.70.151
- 159.149.47.225
- 159.149.116.192
- 159.149.118.200
- 159.149.119.147
- 159.149.118.108
- 159.149.116.145
- 159.149.117.109
- 159.149.117.131
- 159.149.53.51
- 159.149.117.13
- 159.149.116.169
- 159.149.119.183
- 159.149.119.122

- 159.149.117.19
- 159.149.129.249
- 159.149.118.173
- 159.149.118.101
- 159.149.116.214
- 159.149.116.14
- 159.149.119.27
- 159.149.116.238
- 159.149.118.187
- 159.149.116.107
- 159.149.119.191
- 159.149.119.121
- 159.149.116.235
- 159.149.130.178
- 185.221.216.115
- 35.185.199.199
- 159.149.116.22
- 159.149.116.193
- 159.149.116.186
- 159.149.116.232
- 159.149.116.109
- 159.149.118.196
- 159.149.53.244
- 159.149.53.34
- 159.149.119.189
- 159.149.119.29
- 159.149.116.188
- 159.149.117.189
- 159.149.119.158
- 159.149.118.19
- 3.66.141.129
- 159.149.119.170
- 159.149.116.167
- 159.149.118.118
- 159.149.116.124
- 159.149.116.240

- 159.149.116.134
- 159.149.118.181
- 159.149.119.106
- 34.83.160.150
- 159.149.117.200
- 159.149.117.17
- 159.149.118.252
- 2606:4700::6812:a1d
- 159.149.119.100
- 159.149.119.118
- 159.149.118.179
- 159.149.118.20
- 159.149.119.209
- 172.64.151.32
- 159.149.118.237
- 159.149.118.176
- 159.149.118.103
- 159.149.15.70
- 159.149.118.205
- 159.149.117.130
- 159.149.116.123
- 159.149.116.24
- 159.149.117.150
- 159.149.47.77
- 159.149.53.140
- 159.149.53.236
- 159.149.117.16
- 159.149.117.141
- 159.149.119.108
- 52.59.135.101
- 159.149.118.22
- 159.149.119.136
- 159.149.118.154
- 159.149.118.153
- 159.149.119.196
- 159.149.105.179

- 159.149.130.188
- 159.149.119.184
- 159.149.116.141
- 159.149.116.27
- 52.101.68.8
- 159.149.117.188
- 159.149.118.121
- 216.147.214.138
- 159.149.116.117
- 159.149.119.162
- 159.149.118.211
- 159.149.118.213
- 159.149.119.126
- 159.149.119.117
- 159.149.118.24
- 159.149.45.8
- 159.149.118.128
- 159.149.118.18
- 159.149.47.22
- 159.149.53.100
- 159.149.116.158
- 159.149.116.118
- 159.149.117.121
- 159.149.116.152
- 159.149.118.180
- 159.149.145.240
- 159.149.145.148
- 159.149.119.135
- 159.149.118.195
- 159.149.119.13
- 159.149.45.32
- 159.149.118.155
- 159.149.118.209
- 159.149.118.194
- 159.149.118.111
- 159.149.117.21

- 159.149.118.33
- 159.149.118.243
- 159.149.118.167
- 159.149.119.212
- 159.149.116.200
- 159.149.145.2
- 159.149.116.172
- 159.149.118.169
- 159.149.116.168
- 159.149.53.239
- 52.101.73.12
- 159.149.53.196
- 159.149.117.107
- 159.149.119.110
- 159.149.119.25
- 159.149.104.154
- 159.149.118.102
- 159.149.118.16
- 159.149.117.32
- 35.156.221.86
- 159.149.119.123
- 159.149.119.132
- 159.149.116.159
- 159.149.117.127
- 159.149.116.181
- 159.149.117.12
- 159.149.53.172
- 159.149.118.203
- 159.149.118.162
- 159.149.118.132
- 159.149.116.234
- 159.149.70.95
- 159.149.119.125
- 159.149.119.142
- 159.149.119.254
- 159.149.119.177

- 18.192.231.252
- 159.149.116.10
- 159.149.118.131
- 159.149.119.164
- 159.149.116.153
- 159.149.118.189
- 159.149.116.115
- 35.199.181.187
- 159.149.116.213
- 159.149.117.173
- 159.149.53.252
- 159.149.116.163
- 159.149.118.10
- 159.149.118.193
- 159.149.116.144
- 159.149.118.11
- 159.149.117.174
- 159.149.53.247
- 159.149.118.113
- 88.99.2.212
- 159.149.116.110
- 159.149.116.113
- 159.149.116.138
- 159.149.116.165
- 159.149.15.26
- 159.149.130.79
- 159.149.119.148
- 159.149.10.101
- 159.149.116.155
- 159.149.119.105
- 159.149.30.18
- 193.205.78.171
- 159.149.117.136
- 159.149.117.252
- 159.149.116.121
- 159.149.118.109

- 159.149.119.20
- 159.149.117.153
- 159.149.118.125
- 159.149.117.163
- 159.149.117.178
- 159.149.117.197
- 159.149.117.180
- 159.149.116.179
- 159.149.116.185
- 159.149.118.160
- 159.149.118.143
- 159.149.118.246
- 159.149.116.205
- 159.149.116.106
- 159.149.119.154
- 159.149.119.32
- 159.149.116.183
- 159.149.117.187
- 159.149.117.170
- 159.149.116.177
- 159.149.116.29
- 159.149.119.157
- 159.149.118.241
- 159.149.116.18
- 159.149.147.114
- 159.149.118.141
- 159.149.116.161
- 159.149.145.169
- 159.149.117.177
- 159.149.117.159
- 159.149.119.176
- 159.149.117.158
- 159.149.119.252
- 159.149.30.3
- 159.149.117.167
- 159.149.117.15

- 159.149.116.23
- 159.149.119.130
- 159.149.118.116
- 159.149.118.133
- 159.149.119.115
- 159.149.129.169
- 159.149.117.193
- 159.149.129.229
- 159.149.119.16
- 159.149.133.37
- 159.149.45.149
- 10.3.100.2
- 104.18.36.224
- 159.149.118.136
- 159.149.117.134
- 159.149.117.176
- 159.149.118.240
- 159.149.142.185
- 159.149.118.188
- 159.149.118.29
- 159.149.116.209
- 159.149.10.1
- 159.149.117.172
- 159.149.147.186
- 159.149.116.212
- 159.149.129.213
- 159.149.118.186
- 159.149.119.156
- 159.149.116.28
- 159.149.116.20
- 159.149.117.108
- 159.149.119.10
- 159.149.117.185
- 159.149.116.180
- 159.149.116.135
- 159.149.116.199

- 159.149.119.124
- 159.149.130.187
- 159.149.118.159
- 159.149.116.162
- 159.149.116.160
- 159.149.119.199
- 159.149.119.179
- 159.149.117.254
- 159.149.119.33
- 159.149.117.124
- 159.149.117.169
- 159.149.118.115
- 159.149.116.154
- 159.149.117.198
- 78.47.83.247
- 159.149.117.101
- 18.184.101.234
- 159.149.116.25
- 159.149.119.143
- 159.149.119.204
- 159.149.118.185
- 159.149.118.23
- 159.149.116.136
- 159.149.119.19
- 159.149.118.107
- 159.149.117.144
- 159.149.145.95
- 159.149.117.149
- 159.149.118.100
- 159.149.116.236
- 159.149.47.62
- 159.149.119.103
- 159.149.119.197
- 159.149.119.141
- 159.149.119.188
- 159.149.116.195

- 159.149.119.111
- 159.149.119.15
- 159.149.117.147
- 159.149.116.12
- 159.149.118.114
- 159.149.118.202
- 34.252.198.25
- 159.149.119.190
- 159.149.116.237
- 159.149.118.182
- 159.149.116.198
- 159.149.118.212
- 159.149.130.85
- 159.149.116.119
- 159.149.119.134
- 159.149.117.145
- 159.149.118.140
- 159.149.117.29
- 159.149.118.166
- 159.149.117.26
- 159.149.119.140
- 159.149.116.116
- 159.149.119.112
- 159.149.119.28
- 159.149.10.20
- 159.149.10.90
- 159.149.119.210
- 159.149.116.11
- 159.149.119.155
- 159.149.118.177
- 159.149.116.111
- 159.149.118.120
- 159.149.119.139
- 159.149.117.120
- 159.149.53.132
- 159.149.118.127

- 159.149.118.105
- 159.149.117.151
- 159.149.118.148
- 159.149.117.247
- 159.149.117.166
- 159.149.118.144
- 159.149.116.215
- 159.149.116.103
- 159.149.117.203
- 159.149.118.137
- 159.149.53.209
- 159.149.116.32
- 159.149.116.201
- 159.149.130.189
- 159.149.119.214
- 159.149.117.105
- 159.149.15.22
- 34.168.30.71
- 159.149.117.192
- 159.149.119.178
- 159.149.119.14
- 159.149.116.126
- 159.149.53.246
- 130.186.7.246
- 159.149.118.124
- 159.149.119.173
- 159.149.117.117
- 159.149.119.161
- 159.149.119.159
- 159.149.53.27
- 159.149.117.171
- 159.149.117.164
- 159.149.117.119
- 159.149.119.194
- 159.149.118.164
- 159.149.119.101

- 159.149.119.109
- 159.149.118.158
- 159.149.119.145
- 159.149.118.192
- 159.149.119.185
- 159.149.118.21
- 159.149.117.211
- 159.149.118.198
- 159.149.117.161
- 159.149.116.194
- 159.149.130.110
- 159.149.116.142
- 159.149.145.84
- 159.149.119.253
- 159.149.119.114
- 159.149.117.23
- 159.149.117.129
- 159.149.117.208
- 159.149.119.195
- 159.149.118.150
- 159.149.116.114
- 159.149.53.90
- 159.149.205.26
- 159.149.117.135
- 159.149.117.191
- 159.149.116.184
- 159.149.117.168
- 159.149.116.102
- 159.149.117.194
- 159.149.119.163
- 159.149.118.149
- 159.149.118.126
- 159.149.117.253
- 159.149.119.166
- 159.149.118.117
- 159.149.117.113

- 159.149.118.208
- 159.149.145.168
- 159.149.53.16
- 159.149.130.182
- 159.149.129.170
- 159.149.117.111
- 104.18.11.29
- 159.149.145.167
- 159.149.119.151
- 2606:4700::6812:b1d
- 159.149.116.178
- 159.149.117.27
- 159.149.118.145
- 159.149.116.191
- 159.149.117.201
- 159.149.116.100
- 159.149.119.175
- 159.149.119.146
- 159.149.118.236
- 159.149.119.200
- 159.149.119.186
- 159.149.117.25
- 159.149.118.31
- 159.149.116.31
- 34.83.23.240
- 159.149.119.249
- 159.149.116.208
- 159.149.53.216
- 52.101.68.27
- 159.149.119.207
- 159.149.119.116
- 159.149.116.202
- 159.149.116.15
- 159.149.119.107
- 159.149.119.129
- 159.149.118.152

- 159.149.117.137
- 159.149.119.26
- 159.149.116.143
- 159.149.119.131
- 159.149.117.196
- 159.149.118.123
- 159.149.118.171
- 159.149.116.176
- 159.149.117.122
- 18.200.39.12
- 159.149.117.181
- 18.157.120.162
- 159.149.116.130
- 159.149.47.69
- 159.149.116.206
- 159.149.116.164
- 159.149.116.182
- 159.149.118.190
- 159.149.147.194
- 159.149.117.100
- 159.149.119.169
- 159.149.117.250
- 159.149.119.248
- 159.149.119.171
- 159.149.117.186
- 159.149.117.155
- 159.149.119.12
- 159.149.116.197
- 159.149.106.180
- 159.149.118.197
- 159.149.118.253
- 159.149.133.61
- 159.149.53.130
- 159.149.118.135
- 159.149.116.105
- 159.149.116.139

- 159.149.117.212
- 159.149.116.127
- 159.149.133.208
- 159.149.145.162
- 159.149.116.101
- 159.149.117.183
- 159.149.117.28
- 159.149.117.154
- 35.247.66.204
- 159.149.118.130
- 159.149.119.165
- 159.149.117.209
- 159.149.118.178
- 159.149.119.18
- 159.149.116.166
- 159.149.117.24
- 159.149.119.213
- 159.149.117.156
- 159.149.117.139
- 159.149.10.89
- 159.149.118.214
- 159.149.116.174
- 159.149.118.248
- 159.149.117.114
- 159.149.117.160
- 159.149.116.204
- 159.149.118.156
- 159.149.117.214
- 159.149.116.151
- 159.149.118.210
- 159.149.118.32
- 159.149.104.138
- 159.149.116.173
- 159.149.118.183
- 159.149.129.248
- 159.149.116.19

- 159.149.118.139
- 159.149.53.241
- 159.149.116.131
- 159.149.119.172
- 159.149.116.156
- 159.149.118.27
- 159.149.116.149
- 159.149.118.28
- 159.149.117.213
- 159.149.119.208
- 104.18.10.29
- 159.149.116.175
- 159.149.118.129
- 159.149.15.42
- 159.149.118.170
- 159.149.119.251
- 159.149.117.205
- 159.149.117.206
- 159.149.129.224
- 159.149.15.69
- 159.149.116.137
- 159.149.147.136
- 159.149.118.242
- 159.149.118.184
- 159.149.116.157
- 159.149.205.60
- 159.149.119.202
- 159.149.117.103
- 159.149.117.140
- 159.149.118.147
- 159.149.53.221
- 159.149.116.140
- 159.149.118.174
- 159.149.116.150
- 159.149.118.25
- 159.149.117.116

- 159.149.118.30
- 159.149.119.215
- 159.149.116.13
- 159.149.118.122
- 159.149.15.43
- 159.149.136.4
- 159.149.116.122
- 159.149.47.38
- 159.149.53.242
- 159.149.116.108
- 159.149.117.30
- 159.149.117.123
- 159.149.117.126
- 159.149.119.152
- 159.149.117.18
- 159.149.118.204
- 159.149.145.228
- 159.149.119.150
- 159.149.117.251
- 159.149.119.138
- 159.149.118.250
- 159.149.117.10
- 159.149.53.202
- 159.149.116.196
- 159.149.118.151
- 159.149.116.187
- 159.149.118.215
- 159.149.119.174
- 159.149.118.251
- 159.149.118.157
- 159.149.119.24
- 159.149.117.106
- 159.149.117.112
- 159.149.116.17
- 159.149.118.238
- 159.149.117.143

- 159.149.119.34
- 159.149.117.14
- 159.149.116.146
- 159.149.47.56
- 159.149.118.134
- 50.18.142.31
- 159.149.209.135
- 159.149.119.193
- 159.149.145.216
- 159.149.117.195
- 159.149.145.136
- 159.149.119.128
- 159.149.117.128
- 185.199.110.153
- 159.149.116.129
- 159.149.117.31
- 159.149.117.215
- 159.149.145.161
- 50.18.215.94
- 159.149.116.16
- 159.149.53.164
- 159.149.119.31
- 159.149.118.112
- 159.149.118.175
- 159.149.119.120
- 159.149.119.167
- 159.149.145.164
- 159.149.117.179
- 159.149.117.132
- 159.149.117.184
- 159.149.117.146
- 159.149.119.113
- 92.42.111.202
- 159.149.119.182
- 159.149.117.204
- 159.149.117.110

- 159.149.118.172
- 159.149.119.21
- 159.149.116.128
- 159.149.118.142
- 52.101.68.29
- 159.149.119.104
- 159.149.70.130
- 159.149.147.181
- 159.149.53.224
- 159.149.118.104
- 159.149.116.210
- 159.149.117.248
- 159.149.119.198
- 159.149.117.199
- 159.149.116.21
- 159.149.117.138
- 159.149.119.133
- 159.149.117.165
- 159.149.118.168
- 159.149.118.163
- 159.149.119.144
- 159.149.10.83
- 159.149.133.149
- 159.149.145.130
- 159.149.117.20
- 159.149.119.127
- 159.149.116.211
- 159.149.116.120
- 159.149.119.247
- 159.149.117.210
- 159.149.116.207
- 159.149.118.249
- 159.149.116.190
- 159.149.116.203
- 159.149.119.119
- 159.149.116.244

- 159.149.119.180
- 159.149.119.11
- 159.149.117.202
- 159.149.119.160
- 159.149.116.148
- 159.149.116.189
- 159.149.116.125
- 159.149.116.171
- 159.149.118.17
- 159.149.118.110
- 159.149.116.112
- 159.149.119.149
- 159.149.117.33
- 159.149.118.138
- 159.149.53.191
- 159.149.119.137
- 159.149.118.119
- 159.149.119.102
- 159.149.117.162
- 159.149.130.139
- 159.149.117.125
- 159.149.118.199
- 159.149.116.170
- 159.149.117.118
- 159.149.117.11
- 159.149.119.205
- 159.149.117.115
- 159.149.53.217
- 159.149.118.12
- 159.149.117.207
- 159.149.118.247
- 159.149.118.161
- 159.149.117.133
- 159.149.117.175
- 130.186.28.54
- 159.149.117.102

- 159.149.119.153
- 159.149.117.182
- 159.149.117.104
- 159.149.53.144
- 159.149.116.133
- 159.149.116.243
- 159.149.119.187
- 159.149.119.192
- 159.149.53.215
- 159.149.119.168
- 159.149.130.90
- 159.149.119.201
- 159.149.118.239
- 159.149.119.246
- 159.149.118.201
- 159.149.119.206

3   Domain found

Below is the list of Domain found:

- teaching.basilico.di.unimi.it
- mediazione-k21.cdl.unimi.it
- 107-119-dhcp.agra.unimi.it
- Studente.unimi.it
- dsiutils.di.unimi.it
- 194-116-dhcp.agra.unimi.it
- webdev.ewlab.di.unimi.it
- riviste.unimi.it
- 211-116-dhcp.agra.unimi.it
- 122-118-dhcp.agra.unimi.it
- 150-118-dhcp.agra.unimi.it
- 127-116-dhcp.agra.unimi.it
- whoami.cloud.di.unimi.it
- 130-117-dhcp.agra.unimi.it
- 106-118-dhcp.agra.unimi.it
- 160-116-dhcp.agra.unimi.it
- culthum.unimi.it
- mailergw-db.di.unimi.it
- ariel.unimi.it
- newsfeedtest.di.unimi.it
- di.unimi.it
- 137-117-dhcp.agra.unimi.it
- 173-118-dhcp.agra.unimi.it
- 166-116-dhcp.agra.unimi.it
- 182-119-dhcp.agra.unimi.it
- 236-118-statico.agra.unimi.it
- 130-118-dhcp.agra.unimi.it
- grafana.ricerca.sesar.di.unimi.it
- 213-119-dhcp.agra.unimi.it
- 127-118-dhcp.agra.unimi.it
- 133-118-dhcp.agra.unimi.it
- 198-116-dhcp.agra.unimi.it
- 117-119-dhcp.agra.unimi.it

- 202-117-dhcp.agra.unimi.it
- servizi.di.unimi.it
- 106-116-dhcp.agra.unimi.it
- hdfs.ricerca.sesar.di.unimi.it
- sp-ex-pwn-2-61acc51e.laser.di.unimi.it
- 140-119-dhcp.agra.unimi.it
- 112-117-dhcp.agra.unimi.it
- 178-117-dhcp.agra.unimi.it
- mpradali.ariel.ctu.unimi.it
- 11-118-statico.agra.unimi.it
- ims.cdl.unimi.it
- orari-be.divsi.unimi.it
- 157-116-dhcp.agra.unimi.it
- 18-118-dhcp.agra.unimi.it
- 212-118-dhcp.agra.unimi.it
- 172-116-dhcp.agra.unimi.it
- 117-118-dhcp.agra.unimi.it
- 201-116-dhcp.agra.unimi.it
- 248-118-statico.agra.unimi.it
- s3domain.unimi.it
- 205-117-dhcp.agra.unimi.it
- 199-116-dhcp.agra.unimi.it
- 172-119-dhcp.agra.unimi.it
- 20-119-dhcp.agra.unimi.it
- patrimonioold.di.unimi.it
- escapes.unimi.it
- 15-116-statico.agra.unimi.it
- incontriarea.di.unimi.it
- 147-117-dhcp.agra.unimi.it
- 128-116-dhcp.agra.unimi.it
- 12-118-statico.agra.unimi.it
- borghese.di.unimi.it
- ciss11.unimi.it
- myc3place.di.unimi.it
- dataverse.unimi.it
- 100-119-dhcp.agra.unimi.it

- 156-119-dhcp.agra.unimi.it
- an-icon.unimi.it
- 131-117-dhcp.agra.unimi.it
- 108-116-dhcp.agra.unimi.it
- postlaureaonline.unimi.it
- intranet.divsi.unimi.it
- ptab.slam.unimi.it
- 235-116-statico.agra.unimi.it
- ggobors.ariel.ctu.unimi.it
- vbellandipwm.ariel.ctu.unimi.it
- sedutedilaurea.agraria.unimi.it
- valchiavenna.unimi.it
- 155-117-dhcp.agra.unimi.it
- 135-118-dhcp.agra.unimi.it
- hue.bapherd.ricerca.sesar.di.unimi.it
- iqis2019.fisica.unimi.it
- 196-116-dhcp.agra.unimi.it
- striptest.fisica.unimi.it
- glossarioinclusione.unimi.it
- rproject.economia.unimi.it
- 140-116-dhcp.agra.unimi.it
- 191-116-dhcp.agra.unimi.it
- eesms2010.di.unimi.it
- traefik-epyc.laser.di.unimi.it
- archive4j.di.unimi.it
- 119-118-dhcp.agra.unimi.it
- 104-118-dhcp.agra.unimi.it
- 203-119-dhcp.agra.unimi.it
- 194-118-dhcp.agra.unimi.it
- longhorn.ricerca.sesar.di.unimi.it
- 147-119-dhcp.agra.unimi.it
- filibusta.crema.unimi.it
- wikirank.di.unimi.it
- 32-119-dhcp.agra.unimi.it
- gatus.ricerca.sesar.di.unimi.it
- 127-117-dhcp.agra.unimi.it

- fmpc.ariel.ctu.unimi.it
- superset.bapherd.ricerca.sesar.di.unimi.it
- 163-118-dhcp.agra.unimi.it
- 150-119-dhcp.agra.unimi.it
- 191-117-dhcp.agra.unimi.it
- 250-118-statico.agra.unimi.it
- 145-119-dhcp.agra.unimi.it
- 10-117-statico.agra.unimi.it
- marchi.ricerca.di.unimi.it
- vigna.di.unimi.it
- czds.unimi.it
- matematica.unimi.it
- spoc.unimi.it
- 169-116-dhcp.agra.unimi.it
- 135-119-dhcp.agra.unimi.it
- 105-118-dhcp.agra.unimi.it
- 156-116-dhcp.agra.unimi.it
- newsfeedtestapi.di.unimi.it
- 158-117-dhcp.agra.unimi.it
- 133-117-dhcp.agra.unimi.it
- 214-117-dhcp.agra.unimi.it
- air.unimi.it
- diart.fisica.unimi.it
- progettopalmira.unimi.it
- 11-116-statico.agra.unimi.it
- wikirank-2022.di.unimi.it
- 175-116-dhcp.agra.unimi.it
- 207-117-dhcp.agra.unimi.it
- incase.di.unimi.it
- 253-118-statico.agra.unimi.it
- broker.cloudtest.di.unimi.it
- 196-117-dhcp.agra.unimi.it
- 181-117-dhcp.agra.unimi.it
- fisica.unimi.it
- jhub.ricerca.sesar.di.unimi.it
- pwncollege-si.laser.di.unimi.it

- neurofisiopatologia.cdl.unimi.it
- 157-117-dhcp.agra.unimi.it
- fastutil.di.unimi.it
- console.s3.ricerca.sesar.di.unimi.it
- 209-118-dhcp.agra.unimi.it
- dialects.changes.unimi.it
- portainer.laser.di.unimi.it
- 157-118-dhcp.agra.unimi.it
- 28-117-dhcp.agra.unimi.it
- 111-118-dhcp.agra.unimi.it
- 174-117-dhcp.agra.unimi.it
- 120-116-dhcp.agra.unimi.it
- studentitest.di.unimi.it
- ibp2025.unimi.it
- 155-118-dhcp.agra.unimi.it
- musicblockly.lim.di.unimi.it
- 104-117-dhcp.agra.unimi.it
- laser.di.unimi.it
- webdbtest.studenti.di.unimi.it
- 144-117-dhcp.agra.unimi.it
- 27-118-dhcp.agra.unimi.it
- 129-118-dhcp.agra.unimi.it
- legato.lim.di.unimi.it
- 19-118-dhcp.agra.unimi.it
- 159-118-dhcp.agra.unimi.it
- phd.fisica.unimi.it
- work.unimi.it
- 148-116-dhcp.agra.unimi.it
- 197-118-dhcp.agra.unimi.it
- unitech.unimi.it
- 18-119-dhcp.agra.unimi.it
- basilico.di.unimi.it
- upload.di.unimi.it
- 199-118-dhcp.agra.unimi.it
- api.accounts.di.unimi.it
- logbookveterinaria.unimi.it

- xoroshiro.di.unimi.it
- sunfloat.unimi.it
- ml4pm2023.di.unimi.it
- 34-116-dhcp.agra.unimi.it
- master-user4-novnc.laser.di.unimi.it
- pseudorandom.di.unimi.it
- 126-117-dhcp.agra.unimi.it
- argocd.ricerca.sesar.di.unimi.it
- convegnodipchi.unimi.it
- phabtest.divsi.unimi.it
- bellettini.di.unimi.it
- samarati.di.unimi.it
- eng.dept.unimi.it
- 163-116-dhcp.agra.unimi.it
- vpn.unimi.it
- 151-118-dhcp.agra.unimi.it
- esamimoodle.unimi.it
- 27-117-dhcp.agra.unimi.it
- 16-118-dhcp.agra.unimi.it
- 213-116-dhcp.agra.unimi.it
- changes.lim.di.unimi.it
- dottorato.di.unimi.it
- 173-116-dhcp.agra.unimi.it
- 148-118-dhcp.agra.unimi.it
- 124-116-dhcp.agra.unimi.it
- lifemega.unimi.it
- mediacomm.unimi.it
- 251-117-statico.agra.unimi.it
- rsu.unimi.it
- prestitodb.cloudtest.di.unimi.it
- 101-118-dhcp.agra.unimi.it
- 161-119-dhcp.agra.unimi.it
- 123-118-dhcp.agra.unimi.it
- 155-119-dhcp.agra.unimi.it
- sites.unimi.it
- alertmanager.cloud.di.unimi.it

- eng.dbs.unimi.it
- 181-116-dhcp.agra.unimi.it
- 131-116-dhcp.agra.unimi.it
- islab.dico.unimi.it
- registrazione.unimi.it
- 103-116-dhcp.agra.unimi.it
- 18-117-dhcp.agra.unimi.it
- mailergw.di.unimi.it
- smtpbridge.unimi.it
- traefik-mirco.laser.di.unimi.it
- 122-117-dhcp.agra.unimi.it
- 176-118-dhcp.agra.unimi.it
- 111-117-dhcp.agra.unimi.it
- siem.laser.di.unimi.it
- 29-116-dhcp.agra.unimi.it
- 247-119-statico.agra.unimi.it
- calamperetest.di.unimi.it
- master-mainettim-novnc.laser.di.unimi.it
- 198-119-dhcp.agra.unimi.it
- sux4j.di.unimi.it
- 116-117-dhcp.agra.unimi.it
- 171-119-dhcp.agra.unimi.it
- 167-117-dhcp.agra.unimi.it
- xorshift.di.unimi.it
- 16-117-dhcp.agra.unimi.it
- anticorruzione.ariel.ctu.unimi.it
- eng.beccaria.unimi.it
- 143-119-dhcp.agra.unimi.it
- sesar.di.unimi.it
- 154-118-dhcp.agra.unimi.it
- cimaina2.fisica.unimi.it
- harbor.ricerca.sesar.di.unimi.it
- 119-116-dhcp.agra.unimi.it
- shrinkai.di.unimi.it
- 22-116-dhcp.agra.unimi.it
- 200-116-dhcp.agra.unimi.it

- 136-118-dhcp.agra.unimi.it

- next.unimi.it

- podologia.cdl.unimi.it

- 174-118-dhcp.agra.unimi.it

- oracleserver.srv.di.unimi.it

- qtech2.fisica.unimi.it

- 207-119-dhcp.agra.unimi.it

- 123-116-dhcp.agra.unimi.it

- 237-118-statico.agra.unimi.it

- orienteantico.unimi.it

- sp-ex-pwn-1-kfd7fr2.laser.di.unimi.it

- 108-118-dhcp.agra.unimi.it

- mail.laser.di.unimi.it

- sedutedilaurea.scienzemfn.unimi.it

- veterinaria.cdl.unimi.it

- 124-117-dhcp.agra.unimi.it

- musicstudio.lim.di.unimi.it

- 169-119-dhcp.agra.unimi.it

- scuolasisa.unimi.it

- farmacia.cdl.unimi.it

- 202-116-dhcp.agra.unimi.it

- geocareers.unimi.it

- whoami.cloudstaff.di.unimi.it

- 139-116-dhcp.agra.unimi.it

- multimech.fisica.unimi.it

- progettocalvatone.unimi.it

- 110-116-dhcp.agra.unimi.it

- spdp.di.unimi.it

- tirocinitest.di.unimi.it

- 193-118-dhcp.agra.unimi.it

- reda.unimi.it

- 166-119-dhcp.agra.unimi.it

- master-lefossem-novnc.laser.di.unimi.it

- easystaff.divsi.unimi.it

- 120-119-dhcp.agra.unimi.it

- 153-118-dhcp.agra.unimi.it

- 120-118-dhcp.agra.unimi.it
- 189-118-dhcp.agra.unimi.it
- 18-116-dhcp.agra.unimi.it
- sux.di.unimi.it
- sp-ex-pwn-1-a01gk49f.laser.di.unimi.it
- mailergw-test.di.unimi.it
- 135-116-dhcp.agra.unimi.it
- cloud.di.unimi.it
- 203-118-dhcp.agra.unimi.it
- 145-116-dhcp.agra.unimi.it
- 143-118-dhcp.agra.unimi.it
- genovese.di.unimi.it
- dashboard.laser.di.unimi.it
- 204-117-dhcp.agra.unimi.it
- 169-118-dhcp.agra.unimi.it
- 141-118-dhcp.agra.unimi.it
- beccaria.unimi.it
- 10-118-statico.agra.unimi.it
- 129-116-dhcp.agra.unimi.it
- iebil.di.unimi.it
- cazzola.di.unimi.it
- 115-118-dhcp.agra.unimi.it
- 103-117-dhcp.agra.unimi.it
- prenotazione-new.di.unimi.it
- uploadapi.di.unimi.it
- 122-119-dhcp.agra.unimi.it
- 142-116-dhcp.agra.unimi.it
- arkive.unimi.it
- 102-118-dhcp.agra.unimi.it
- 184-119-dhcp.agra.unimi.it
- socialcampus.di.unimi.it
- 105-119-dhcp.agra.unimi.it
- 127-119-dhcp.agra.unimi.it
- adipascaledds.ariel.ctu.unimi.it
- 147-116-dhcp.agra.unimi.it
- ayw2023.di.unimi.it

- ctf.cdl.unimi.it
- 154-119-dhcp.agra.unimi.it
- 144-119-dhcp.agra.unimi.it
- 161-117-dhcp.agra.unimi.it
- 30-118-dhcp.agra.unimi.it
- rel.cdl.unimi.it
- wikirank-2016.di.unimi.it
- sliver.docenti.di.unimi.it
- 197-117-dhcp.agra.unimi.it
- lsr.dsi.unimi.it
- prestitoapi.cloudtest.di.unimi.it
- sp-ex-pwn-1-61acc51e.laser.di.unimi.it
- 196-119-dhcp.agra.unimi.it
- 200-119-dhcp.agra.unimi.it
- 137-119-dhcp.agra.unimi.it
- 134-119-dhcp.agra.unimi.it
- 249-118-statico.agra.unimi.it
- hesabu.fisica.unimi.it
- informastudenti.unimi.it
- crypto.club.di.unimi.it
- 145-117-dhcp.agra.unimi.it
- 195-116-dhcp.agra.unimi.it
- fsdattackerserver.laser.di.unimi.it
- pwncollege.laser.di.unimi.it
- 177-119-dhcp.agra.unimi.it
- spaziofilosofico.filosofia.unimi.it
- laila.di.unimi.it
- 194-119-dhcp.agra.unimi.it
- 181-118-dhcp.agra.unimi.it
- studenti.unimi.it
- 104-119-dhcp.agra.unimi.it
- scienzegiuridiche.unimi.it
- 121-117-dhcp.agra.unimi.it
- 24-119-dhcp.agra.unimi.it
- 175-119-dhcp.agra.unimi.it
- 11-119-statico.agra.unimi.it

- 138-119-dhcp.agra.unimi.it
- 24-116-dhcp.agra.unimi.it
- wp-temp2.fisica.unimi.it
- let.di.unimi.it
- 27-119-dhcp.agra.unimi.it
- mediazione.cdl.unimi.it
- 148-119-dhcp.agra.unimi.it
- 25-119-dhcp.agra.unimi.it
- 210-118-dhcp.agra.unimi.it
- adapt-lab.di.unimi.it
- 195-118-dhcp.agra.unimi.it
- 156-117-dhcp.agra.unimi.it
- stickybeak.cybersecurity.unimi.it
- midimonitor.lim.di.unimi.it
- 141-119-dhcp.agra.unimi.it
- autoconfig.laser.di.unimi.it
- cosp.unimi.it
- 247-117-statico.agra.unimi.it
- 254-119-statico.agra.unimi.it
- biotecnologiemediche.cdl.unimi.it
- prestito.cloudtest.di.unimi.it
- lam.cdl.unimi.it
- 124-118-dhcp.agra.unimi.it
- 164-116-dhcp.agra.unimi.it
- 189-117-dhcp.agra.unimi.it
- 34-119-dhcp.agra.unimi.it
- matematica-lm.cdl.unimi.it
- 21-118-dhcp.agra.unimi.it
- corbellasummerschool.unimi.it
- 129-119-dhcp.agra.unimi.it
- ext.unimi.it
- riassuntitesi.scienzemfn.unimi.it
- 19-117-dhcp.agra.unimi.it
- 170-116-dhcp.agra.unimi.it
- alos.di.unimi.it
- auth.unimi.it

- glitter.di.unimi.it

- smartbear-it.di.unimi.it

- 113-118-dhcp.agra.unimi.it

- 192-119-dhcp.agra.unimi.it

- 113-119-dhcp.agra.unimi.it

- 244-116-statico.agra.unimi.it

- 17-118-dhcp.agra.unimi.it

- 125-119-dhcp.agra.unimi.it

- vaultwarden.ricerca.sesar.di.unimi.it

- chimica.unimi.it

- ciriani.di.unimi.it

- 236-116-statico.agra.unimi.it

- fileserver.laser.di.unimi.it

- 110-117-dhcp.agra.unimi.it

- ines.unimi.it

- 205-119-dhcp.agra.unimi.it

- 10-116-statico.agra.unimi.it

- 14-119-statico.agra.unimi.it

- 140-118-dhcp.agra.unimi.it

- 25-117-dhcp.agra.unimi.it

- algofeed.unimi.it

- polcrises.unimi.it

- 193-116-dhcp.agra.unimi.it

- 125-117-dhcp.agra.unimi.it

- kb.di.unimi.it

- riassuntitesi.agraria.unimi.it

- 185-118-dhcp.agra.unimi.it

- 240-116-statico.agra.unimi.it

- master-veninie-novnc.laser.di.unimi.it

- webdbtestapi.studenti.di.unimi.it

- llmsd.cdl.unimi.it

- law.di.unimi.it

- 31-116-dhcp.agra.unimi.it

- rustdesk.di.unimi.it

- 125-118-dhcp.agra.unimi.it

- fsd-manconi-novnc.laser.di.unimi.it

- master-elachmary-novnc.laser.di.unimi.it
- lettere.cdl.unimi.it
- 178-116-dhcp.agra.unimi.it
- accountstest.di.unimi.it
- minatore.divtlc.unimi.it
- api.minio.ricerca.sesar.di.unimi.it
- 25-116-dhcp.agra.unimi.it
- 250-117-statico.agra.unimi.it
- 190-118-dhcp.agra.unimi.it
- unsee.cloud.di.unimi.it
- masterdsebf.unimi.it
- apegeo.unimi.it
- eng.discco.unimi.it
- 172-117-dhcp.agra.unimi.it
- 189-116-dhcp.agra.unimi.it
- 115-117-dhcp.agra.unimi.it
- reception.cloudtest.di.unimi.it
- mathup2425.mat.unimi.it
- minerva.unimi.it
- 208-117-dhcp.agra.unimi.it
- 16-119-dhcp.agra.unimi.it
- 164-117-dhcp.agra.unimi.it
- 120-117-dhcp.agra.unimi.it
- 183-118-dhcp.agra.unimi.it
- germoplasma.unimi.it
- 114-119-dhcp.agra.unimi.it
- 115-116-dhcp.agra.unimi.it
- 118-119-dhcp.agra.unimi.it
- 234-116-statico.agra.unimi.it
- 101-117-dhcp.agra.unimi.it
- bollatilab.unimi.it
- prenotabiblio.sba.unimi.it
- instrumentaloptics.fisica.unimi.it
- phddb.cloudtest.di.unimi.it
- 201-119-dhcp.agra.unimi.it
- 144-118-dhcp.agra.unimi.it

- 100-118-dhcp.agra.unimi.it
- contrabass.fisica.unimi.it
- 147-118-dhcp.agra.unimi.it
- 152-118-dhcp.agra.unimi.it
- 214-119-dhcp.agra.unimi.it
- 213-118-dhcp.agra.unimi.it
- cas.unimi.it
- erogatore.unimi.it
- materia.fisica.unimi.it
- textgen.ricerca.sesar.di.unimi.it
- 190-117-dhcp.agra.unimi.it
- oramigis.unimi.it
- bacheca2lv.fisica.unimi.it
- 141-117-dhcp.agra.unimi.it
- 210-117-dhcp.agra.unimi.it
- 209-119-dhcp.agra.unimi.it
- 141-116-dhcp.agra.unimi.it
- 150-117-dhcp.agra.unimi.it
- 33-119-dhcp.agra.unimi.it
- 211-118-dhcp.agra.unimi.it
- ml4pm2022.di.unimi.it
- 31-119-dhcp.agra.unimi.it
- 158-116-dhcp.agra.unimi.it
- 151-117-dhcp.agra.unimi.it
- openscience.unimi.it
- mermaid.unimi.it
- icona.crc.unimi.it
- ricercamix.unimi.it
- labanof.unimi.it
- 167-119-dhcp.agra.unimi.it
- oncolab.unimi.it
- smartpen.aislab.di.unimi.it
- 100-117-dhcp.agra.unimi.it
- 211-117-dhcp.agra.unimi.it
- 192-118-dhcp.agra.unimi.it
- vaultwarden.laser.di.unimi.it

- 151-116-dhcp.agra.unimi.it
- fuellab.unimi.it
- 180-118-dhcp.agra.unimi.it
- 17-116-dhcp.agra.unimi.it
- 142-119-dhcp.agra.unimi.it
- 203-116-dhcp.agra.unimi.it
- astro.fisica.unimi.it
- piuri.di.unimi.it
- 144-116-dhcp.agra.unimi.it
- wikirank-2019.di.unimi.it
- 146-116-dhcp.agra.unimi.it
- 101-119-dhcp.agra.unimi.it
- 186-119-dhcp.agra.unimi.it
- digit-manzoni.divsi.unimi.it
- istitutoconfucio.unimi.it
- 142-118-dhcp.agra.unimi.it
- centenario.unimi.it
- 19-116-dhcp.agra.unimi.it
- 180-119-dhcp.agra.unimi.it
- 187-118-dhcp.agra.unimi.it
- videoconf.unimi.it
- guest.unimi.it
- mg4j.di.unimi.it
- wp-temp.fisica.unimi.it
- 134-116-dhcp.agra.unimi.it
- delletto.fisica.unimi.it
- bioscienzebio.unimi.it
- 207-116-dhcp.agra.unimi.it
- ecare.unimi.it
- 126-116-dhcp.agra.unimi.it
- 100-116-dhcp.agra.unimi.it
- 196-118-dhcp.agra.unimi.it
- master-user5-novnc.laser.di.unimi.it
- smartbear.di.unimi.it
- 143-116-dhcp.agra.unimi.it
- bioscienze.unimi.it

- 19-119-dhcp.agra.unimi.it
- com.cdl.unimi.it
- etruscologia.di.unimi.it
- 143-117-dhcp.agra.unimi.it
- helpdesk.divsi.unimi.it
- wikirank-2017.di.unimi.it
- master-user3-novnc.laser.di.unimi.it
- 29-119-dhcp.agra.unimi.it
- minio.bapherd.ricerca.sesar.di.unimi.it
- 177-117-dhcp.agra.unimi.it
- econ.cdl.unimi.it
- farmacognosia.unimi.it
- uploadold.di.unimi.it
- asardellapd.ariel.ctu.unimi.it
- 32-118-dhcp.agra.unimi.it
- scienzeumanistichecomunicazione.cdl.unimi.it
- 28-116-dhcp.agra.unimi.it
- 194-117-dhcp.agra.unimi.it
- skynet.unimi.it
- spa.cdl.unimi.it
- 32-117-dhcp.agra.unimi.it
- 134-117-dhcp.agra.unimi.it
- 187-117-dhcp.agra.unimi.it
- ne.di.unimi.it
- 184-116-dhcp.agra.unimi.it
- 10-119-statico.agra.unimi.it
- 170-118-dhcp.agra.unimi.it
- wireguard.laser.di.unimi.it
- bookstack.laser.di.unimi.it
- 137-118-dhcp.agra.unimi.it
- 26-117-dhcp.agra.unimi.it
- newsmail.islab.di.unimi.it
- elearning.unimi.it
- 113-116-dhcp.agra.unimi.it
- 205-118-dhcp.agra.unimi.it
- play4physio.di.unimi.it

- dcfs2017.di.unimi.it
- 21-119-dhcp.agra.unimi.it
- 201-117-dhcp.agra.unimi.it
- 190-116-dhcp.agra.unimi.it
- 148-117-dhcp.agra.unimi.it
- 186-118-dhcp.agra.unimi.it
- 170-117-dhcp.agra.unimi.it
- 165-119-dhcp.agra.unimi.it
- 134-118-dhcp.agra.unimi.it
- 12-116-statico.agra.unimi.it
- 214-116-dhcp.agra.unimi.it
- 118-118-dhcp.agra.unimi.it
- 119-119-dhcp.agra.unimi.it
- 176-117-dhcp.agra.unimi.it
- seclab.dti.unimi.it
- 109-117-dhcp.agra.unimi.it
- 27-116-dhcp.agra.unimi.it
- 23-118-dhcp.agra.unimi.it
- gpu.di.unimi.it
- wikirank-2020.di.unimi.it
- 103-118-dhcp.agra.unimi.it
- 31-118-dhcp.agra.unimi.it
- aqm4.fisica.unimi.it
- 21-116-dhcp.agra.unimi.it
- ml4pm.di.unimi.it
- germoplasmatest.sesar.di.unimi.it
- tirocini.di.unimi.it
- 154-116-dhcp.agra.unimi.it
- intranet.di.unimi.it
- securemail.unimi.it
- thor.di.unimi.it
- 162-119-dhcp.agra.unimi.it
- 133-119-dhcp.agra.unimi.it
- 161-116-dhcp.agra.unimi.it
- changes.unimi.it
- h2020.fisica.unimi.it

- srv-moodle-4.ctu.unimi.it

- qureco.fisica.unimi.it

- 117-116-dhcp.agra.unimi.it

- 164-118-dhcp.agra.unimi.it

- 180-116-dhcp.agra.unimi.it

- 182-116-dhcp.agra.unimi.it

- 200-118-dhcp.agra.unimi.it

- cgil.unimi.it

- 20-118-dhcp.agra.unimi.it

- 158-119-dhcp.agra.unimi.it

- aaa.unimi.it

- 119-117-dhcp.agra.unimi.it

- 177-118-dhcp.agra.unimi.it

- 214-118-dhcp.agra.unimi.it

- 195-117-dhcp.agra.unimi.it

- 138-118-dhcp.agra.unimi.it

- 126-119-dhcp.agra.unimi.it

- 112-118-dhcp.agra.unimi.it

- registry.cloud.di.unimi.it

- newsfeed.di.unimi.it

- frontend.serenade.ewlab.di.unimi.it

- phdlog.cloudtest.di.unimi.it

- dairysmart.unimi.it

- trino.bapherd.ricerca.sesar.di.unimi.it

- 168-116-dhcp.agra.unimi.it

- 109-116-dhcp.agra.unimi.it

- 193-117-dhcp.agra.unimi.it

- 20-117-dhcp.agra.unimi.it

- 253-119-statico.agra.unimi.it

- myariel.unimi.it

- postlaurea.myariel.unimi.it

- dwtest.di.unimi.it

- 121-116-dhcp.agra.unimi.it

- commiati.di.unimi.it

- adapt-lab.ricerca.di.unimi.it

- 114-117-dhcp.agra.unimi.it

- coding.lim.di.unimi.it
- 200-117-dhcp.agra.unimi.it
- 160-118-dhcp.agra.unimi.it
- prometheus.cloud.di.unimi.it
- 208-118-dhcp.agra.unimi.it
- pls.fisica.unimi.it
- biosciences.unimi.it
- 168-119-dhcp.agra.unimi.it
- 152-119-dhcp.agra.unimi.it
- random.di.unimi.it
- 208-119-dhcp.agra.unimi.it
- dantona.di.unimi.it
- 139-117-dhcp.agra.unimi.it
- master-parruccir-novnc.laser.di.unimi.it
- xoshiro.di.unimi.it
- cusmibio-prenota.unimi.it
- libri.unimi.it
- master-contel-novnc.laser.di.unimi.it
- 251-118-statico.agra.unimi.it
- 107-116-dhcp.agra.unimi.it
- mta-sts.laser.di.unimi.it
- 207-118-dhcp.agra.unimi.it
- 248-119-statico.agra.unimi.it
- helpdesk.unimi.it
- 139-118-dhcp.agra.unimi.it
- cooml.di.unimi.it
- webgraph.di.unimi.it
- 175-118-dhcp.agra.unimi.it
- 29-117-dhcp.agra.unimi.it
- oldweb.laser.di.unimi.it
- 243-116-statico.agra.unimi.it
- 131-118-dhcp.agra.unimi.it
- 123-117-dhcp.agra.unimi.it
- pcg.di.unimi.it
- 152-117-dhcp.agra.unimi.it
- dataloading.bapherd.ricerca.sesar.di.unimi.it

- 121-118-dhcp.agra.unimi.it
- master-user2-novnc.laser.di.unimi.it
- kas.gitlab.ricerca.sesar.di.unimi.it
- 12-119-statico.agra.unimi.it
- 183-116-dhcp.agra.unimi.it
- bioms2013.di.unimi.it
- environsci.unimi.it
- 117-117-dhcp.agra.unimi.it
- 13-119-statico.agra.unimi.it
- 24-117-dhcp.agra.unimi.it
- wikirank-2018.di.unimi.it
- 106-117-dhcp.agra.unimi.it
- 138-116-dhcp.agra.unimi.it
- 190-119-dhcp.agra.unimi.it
- 183-117-dhcp.agra.unimi.it
- prinhealing.unimi.it
- ricesmart.unimi.it
- 33-118-dhcp.agra.unimi.it
- 128-117-dhcp.agra.unimi.it
- newdottorato.di.unimi.it
- trm.cdl.unimi.it
- 24-118-dhcp.agra.unimi.it
- nextcloud.laser.di.unimi.it
- 109-118-dhcp.agra.unimi.it
- 122-116-dhcp.agra.unimi.it
- 170-119-dhcp.agra.unimi.it
- 14-116-statico.agra.unimi.it
- 145-118-dhcp.agra.unimi.it
- 128-119-dhcp.agra.unimi.it
- 162-118-dhcp.agra.unimi.it
- orientamento.di.unimi.it
- 108-117-dhcp.agra.unimi.it
- 137-116-dhcp.agra.unimi.it
- esp.unimi.it
- 123-119-dhcp.agra.unimi.it
- smtp.unimi.it

- fca-namirial.unimi.it
- eesms2009.di.unimi.it
- grew.di.unimi.it
- 239-118-statico.agra.unimi.it
- colorist.di.unimi.it
- 215-119-dhcp.agra.unimi.it
- 116-119-dhcp.agra.unimi.it
- 130-119-dhcp.agra.unimi.it
- 15-119-statico.agra.unimi.it
- 103-119-dhcp.agra.unimi.it
- 204-119-dhcp.agra.unimi.it
- cimeamilano.unimi.it
- raton.anacleto.di.unimi.it
- qbio.cdl.unimi.it
- cookiepolicy.di.unimi.it
- 182-117-dhcp.agra.unimi.it
- viticolturaenologia.cdl.unimi.it
- 209-116-dhcp.agra.unimi.it
- 116-116-dhcp.agra.unimi.it
- studente.divsi.unimi.it
- visconti.di.unimi.it
- 165-116-dhcp.agra.unimi.it
- 182-118-dhcp.agra.unimi.it
- 153-119-dhcp.agra.unimi.it
- users.mat.unimi.it
- 124-119-dhcp.agra.unimi.it
- 132-119-dhcp.agra.unimi.it
- 131-119-dhcp.agra.unimi.it
- etruscologia.unimi.it
- tracesofmobility.unimi.it
- discco.unimi.it
- 210-119-dhcp.agra.unimi.it
- 215-117-dhcp.agra.unimi.it
- lin.cdl.unimi.it
- 22-118-dhcp.agra.unimi.it
- mjessoulacws.ariel.ctu.unimi.it

- 212-117-dhcp.agra.unimi.it
- wizarduniclloud.unimi.it
- 249-119-statico.agra.unimi.it
- 138-117-dhcp.agra.unimi.it
- divas.dire.unimi.it
- test.laser.di.unimi.it
- 179-117-dhcp.agra.unimi.it
- 32-116-dhcp.agra.unimi.it
- 174-119-dhcp.agra.unimi.it
- 176-116-dhcp.agra.unimi.it
- ciccio.fisica.unimi.it
- master-user1-novnc.laser.di.unimi.it
- 171-116-dhcp.agra.unimi.it
- 180-117-dhcp.agra.unimi.it
- 252-117-statico.agra.unimi.it
- tirociniapi.di.unimi.it
- 206-117-dhcp.agra.unimi.it
- rng.di.unimi.it
- 199-119-dhcp.agra.unimi.it
- 101-116-dhcp.agra.unimi.it
- livinglab.di.unimi.it
- 110-118-dhcp.agra.unimi.it
- 146-117-dhcp.agra.unimi.it
- 192-116-dhcp.agra.unimi.it
- calamperetestapi.di.unimi.it
- humanhall.unimi.it
- web.laser.di.unimi.it
- ioi.di.unimi.it
- ranger.bapherd.ricerca.sesar.di.unimi.it
- 129-117-dhcp.agra.unimi.it
- 204-118-dhcp.agra.unimi.it
- phanlab.unimi.it
- infocom.di.unimi.it
- epaganirec.ariel.ctu.unimi.it
- 113-117-dhcp.agra.unimi.it
- 165-117-dhcp.agra.unimi.it

- 188-117-dhcp.agra.unimi.it
- master-villanim-novnc.laser.di.unimi.it
- 13-117-statico.agra.unimi.it
- 132-117-dhcp.agra.unimi.it
- dsrctracker.islab.di.unimi.it
- 118-117-dhcp.agra.unimi.it
- pong.di.unimi.it
- 106-119-dhcp.agra.unimi.it
- 238-116-statico.agra.unimi.it
- 160-117-dhcp.agra.unimi.it
- traefikllama.laser.di.unimi.it
- anomalie.unimi.it
- unimix3.unimi.it
- bibliotecamattioli.unimi.it
- 248-117-statico.agra.unimi.it
- 169-117-dhcp.agra.unimi.it
- ercshare.unimi.it
- phd.cloudtest.di.unimi.it
- traefik.laser.di.unimi.it
- 166-118-dhcp.agra.unimi.it
- 192-117-dhcp.agra.unimi.it
- 247-118-statico.agra.unimi.it
- mailergw-db-test.di.unimi.it
- portainer.eduvirt.di.unimi.it
- 30-117-dhcp.agra.unimi.it
- dpm2016.di.unimi.it
- 150-116-dhcp.agra.unimi.it
- master-lembog-novnc.laser.di.unimi.it
- 243-118-statico.agra.unimi.it
- 130-116-dhcp.agra.unimi.it
- 178-119-dhcp.agra.unimi.it
- 132-116-dhcp.agra.unimi.it
- 135-117-dhcp.agra.unimi.it
- 168-118-dhcp.agra.unimi.it
- 191-118-dhcp.agra.unimi.it
- nix-cache.ricerca.sesar.di.unimi.it

- 121-119-dhcp.agra.unimi.it
- 23-117-dhcp.agra.unimi.it
- 209-117-dhcp.agra.unimi.it
- 112-116-dhcp.agra.unimi.it
- 215-118-dhcp.agra.unimi.it
- 128-118-dhcp.agra.unimi.it
- 159-119-dhcp.agra.unimi.it
- bitwarden.ricerca.sesar.di.unimi.it
- 198-117-dhcp.agra.unimi.it
- 163-119-dhcp.agra.unimi.it
- 251-119-statico.agra.unimi.it
- 167-116-dhcp.agra.unimi.it
- mat.unimi.it
- prng.di.unimi.it
- santini.di.unimi.it
- 28-118-dhcp.agra.unimi.it
- 159-117-dhcp.agra.unimi.it
- 126-118-dhcp.agra.unimi.it
- eng.scienzegiuridiche.unimi.it
- 165-118-dhcp.agra.unimi.it
- s3.ricerca.sesar.di.unimi.it
- chromabio.di.unimi.it
- 163-117-dhcp.agra.unimi.it
- 189-119-dhcp.agra.unimi.it
- benessereanimale.unimi.it
- harmopicta.unimi.it
- 149-116-dhcp.agra.unimi.it
- minio.ricerca.sesar.di.unimi.it
- 241-118-statico.agra.unimi.it
- core.harbor.ricerca.sesar.di.unimi.it
- dialects.changes.lim.di.unimi.it
- 153-116-dhcp.agra.unimi.it
- 188-119-dhcp.agra.unimi.it
- clavier2023.unimi.it
- registry.eduvirt.di.unimi.it
- unistem.unimi.it

- 152-116-dhcp.agra.unimi.it
- rnakgview.anacleto.di.unimi.it
- lonati.di.unimi.it
- micromesh.di.unimi.it
- 185-117-dhcp.agra.unimi.it
- wikirank-2024.di.unimi.it
- lsr.di.unimi.it
- 112-119-dhcp.agra.unimi.it
- grafana.cloud.di.unimi.it
- 25-118-dhcp.agra.unimi.it
- voip.unimi.it
- wifi.unimi.it
- 171-117-dhcp.agra.unimi.it
- wikirank-2015.di.unimi.it
- 203-117-dhcp.agra.unimi.it
- 149-118-dhcp.agra.unimi.it
- 116-118-dhcp.agra.unimi.it
- appuntamenti.servicemanagement.unimi.it
- sebinaopac.divsi.unimi.it
- ste.cdl.unimi.it
- 132-118-dhcp.agra.unimi.it
- 253-117-statico.agra.unimi.it
- 107-117-dhcp.agra.unimi.it
- 210-116-dhcp.agra.unimi.it
- 179-118-dhcp.agra.unimi.it
- 237-116-statico.agra.unimi.it
- 204-116-dhcp.agra.unimi.it
- authentik.ricerca.sesar.di.unimi.it
- webradio.divsi.unimi.it
- 175-117-dhcp.agra.unimi.it
- 199-117-dhcp.agra.unimi.it
- 166-117-dhcp.agra.unimi.it
- 115-119-dhcp.agra.unimi.it
- tecnocivismo.di.unimi.it
- master-barzaghib-novnc.laser.di.unimi.it
- pms.di.unimi.it

- 157-119-dhcp.agra.unimi.it
- 172-118-dhcp.agra.unimi.it
- auth.di.unimi.it
- criar.unimi.it
- 139-119-dhcp.agra.unimi.it
- 14-117-statico.agra.unimi.it
- 142-117-dhcp.agra.unimi.it
- 184-117-dhcp.agra.unimi.it
- 102-117-dhcp.agra.unimi.it
- mdamiani.di.unimi.it
- lifesciences.unimi.it
- 146-119-dhcp.agra.unimi.it
- 197-116-dhcp.agra.unimi.it
- apps.unimi.it
- logstest.studenti.di.unimi.it
- sp-ex-pwn-1.laser.di.unimi.it
- 173-117-dhcp.agra.unimi.it
- sebinaweb.divsi.unimi.it
- 155-116-dhcp.agra.unimi.it
- 159-116-dhcp.agra.unimi.it
- nanoworkshop2021.fisica.unimi.it
- prigioniero.di.unimi.it
- mass.cdl.unimi.it
- 108-119-dhcp.agra.unimi.it
- 149-117-dhcp.agra.unimi.it
- eng.esp.unimi.it
- tutoraggio.di.unimi.it
- 158-118-dhcp.agra.unimi.it
- 173-119-dhcp.agra.unimi.it
- 198-118-dhcp.agra.unimi.it
- 154-117-dhcp.agra.unimi.it
- spettacolo.fisica.unimi.it
- sp-ex-pwn-2.laser.di.unimi.it
- 188-118-dhcp.agra.unimi.it
- 202-119-dhcp.agra.unimi.it
- 171-118-dhcp.agra.unimi.it

- 12-117-statico.agra.unimi.it
- 28-119-dhcp.agra.unimi.it
- 140-117-dhcp.agra.unimi.it
- unimia.unimi.it
- promoplurilinguismo.unimi.it
- 104-116-dhcp.agra.unimi.it
- master-pigonia-novnc.laser.di.unimi.it
- 177-116-dhcp.agra.unimi.it
- counter.ricerca.sesar.di.unimi.it
- opac.unimi.it
- master-loritod-novnc.laser.di.unimi.it
- 29-118-dhcp.agra.unimi.it
- 111-119-dhcp.agra.unimi.it
- 149-119-dhcp.agra.unimi.it
- 186-117-dhcp.agra.unimi.it
- caronte-k1nd4sus.laser.di.unimi.it
- 136-119-dhcp.agra.unimi.it
- sp-ex-pwn-1-dhf84ba.laser.di.unimi.it
- 151-119-dhcp.agra.unimi.it
- studente.unimi.it
- 212-116-dhcp.agra.unimi.it
- wikirank-2023.di.unimi.it
- giornalismo.unimi.it
- infermieristica.cdl.unimi.it
- phdapi.cloudtest.di.unimi.it
- security.dico.unimi.it
- 26-119-dhcp.agra.unimi.it
- cewqo20.fisica.unimi.it
- ns.unimi.it
- 102-119-dhcp.agra.unimi.it
- dialettialcinema.changes.unimi.it
- 215-116-dhcp.agra.unimi.it
- 156-118-dhcp.agra.unimi.it
- 164-119-dhcp.agra.unimi.it
- phdold.di.unimi.it
- 31-117-dhcp.agra.unimi.it

- dse.cdl.unimi.it
- 242-118-statico.agra.unimi.it
- grafana.laser.di.unimi.it
- luci.unimi.it
- bitwarden.di.unimi.it
- 240-118-statico.agra.unimi.it
- accounts.di.unimi.it
- marra.di.unimi.it
- 136-117-dhcp.agra.unimi.it
- cewqo23.fisica.unimi.it
- masterdsebf.di.unimi.it
- 184-118-dhcp.agra.unimi.it
- minimat.ariel.ctu.unimi.it
- 162-117-dhcp.agra.unimi.it
- razzelombarde.unimi.it
- sansone.crema.unimi.it
- 183-119-dhcp.agra.unimi.it
- 179-116-dhcp.agra.unimi.it
- disaa-tirocini-tesi.unimi.it
- 160-119-dhcp.agra.unimi.it
- dbs.unimi.it
- prog2.di.unimi.it
- 206-119-dhcp.agra.unimi.it
- ssrionline.unimi.it
- boccignone.di.unimi.it
- 191-119-dhcp.agra.unimi.it
- climvib.unimi.it
- master-frassonea-novnc.laser.di.unimi.it
- .riviste.unimi.it
- 178-118-dhcp.agra.unimi.it
- secregistry.cloud.di.unimi.it
- 15-117-statico.agra.unimi.it
- 185-116-dhcp.agra.unimi.it
- 197-119-dhcp.agra.unimi.it
- 167-118-dhcp.agra.unimi.it
- master-galbuseral-novnc.laser.di.unimi.it

- 179-119-dhcp.agra.unimi.it
- assistenzasanitaria.cdl.unimi.it
- master-vivianim-novnc.laser.di.unimi.it
- 109-119-dhcp.agra.unimi.it
- mhr.cdl.unimi.it
- 246-119-statico.agra.unimi.it
- audioplugins.lim.di.unimi.it
- 136-116-dhcp.agra.unimi.it
- 11-117-statico.agra.unimi.it
- wikirank-2021.di.unimi.it
- datascience.unimi.it
- 212-119-dhcp.agra.unimi.it
- newsfeedapi.di.unimi.it
- registry.di.unimi.it
- welcome.di.unimi.it
- 105-117-dhcp.agra.unimi.it
- tirocinitestapi.di.unimi.it
- 202-118-dhcp.agra.unimi.it
- osservatoriodisabilita.unimi.it
- cla-slam.unimi.it
- old.agraria.unimi.it
- 232-116-statico.agra.unimi.it
- adminer.studenti.di.unimi.it
- 118-116-dhcp.agra.unimi.it
- homes.dsi.unimi.it
- 17-117-dhcp.agra.unimi.it
- ais-lab.di.unimi.it
- spark.bde.ricerca.sesar.di.unimi.it
- eng.matematica.unimi.it
- li2lin.ariel.ctu.unimi.it
- 246-118-statico.agra.unimi.it
- 213-117-dhcp.agra.unimi.it
- germoplasma.sesar.di.unimi.it
- 16-116-dhcp.agra.unimi.it
- 187-119-dhcp.agra.unimi.it
- influxdb.laser.di.unimi.it

- dapsco.unimi.it
- dept.unimi.it
- 176-119-dhcp.agra.unimi.it
- 161-118-dhcp.agra.unimi.it
- bitwardentest.di.unimi.it
- afferenti.fisica.unimi.it
- datascience.di.unimi.it
- 241-116-statico.agra.unimi.it
- 125-116-dhcp.agra.unimi.it
- 114-118-dhcp.agra.unimi.it
- 186-116-dhcp.agra.unimi.it
- 208-116-dhcp.agra.unimi.it
- insdbdemo.fisica.unimi.it
- 193-119-dhcp.agra.unimi.it
- 111-116-dhcp.agra.unimi.it
- islc.unimi.it
- 153-117-dhcp.agra.unimi.it
- 114-116-dhcp.agra.unimi.it
- 110-119-dhcp.agra.unimi.it
- presenze.unimi.it
- maven.adapt-lab.di.unimi.it
- 252-118-statico.agra.unimi.it
- lanzarotti.di.unimi.it
- 174-116-dhcp.agra.unimi.it
- phppgadmintest.studenti.di.unimi.it
- 162-116-dhcp.agra.unimi.it
- neworientamento.di.unimi.it
- 168-117-dhcp.agra.unimi.it
- redirect.laser.di.unimi.it
- 185-119-dhcp.agra.unimi.it
- cct.islab.di.unimi.it
- 252-119-statico.agra.unimi.it
- 33-117-dhcp.agra.unimi.it
- 254-117-statico.agra.unimi.it
- vailati.unimi.it
- 201-118-dhcp.agra.unimi.it

- 20-116-dhcp.agra.unimi.it
- 205-116-dhcp.agra.unimi.it
- cross.unimi.it
- traefik.cloud.di.unimi.it
- 107-118-dhcp.agra.unimi.it
- 13-116-statico.agra.unimi.it
- 206-116-dhcp.agra.unimi.it
- tales.islab.di.unimi.it
- timelapse.unimi.it
- 133-116-dhcp.agra.unimi.it
- fmportal.divsi.unimi.it
- 188-116-dhcp.agra.unimi.it
- 105-116-dhcp.agra.unimi.it
- security.di.unimi.it
- webmail.laser.di.unimi.it
- 195-119-dhcp.agra.unimi.it
- 187-116-dhcp.agra.unimi.it
- 23-116-dhcp.agra.unimi.it
- tim.ricerca.sesar.di.unimi.it
- argo.islab.di.unimi.it
- lama4j.di.unimi.it
- 102-116-dhcp.agra.unimi.it
- 21-117-dhcp.agra.unimi.it
- pupunimi.unimi.it
- 238-118-statico.agra.unimi.it

4 URLs found

Below is the list of URLs found:

- www.mat.unimi.it
- www.centrorusso.unimi.it
- vbellandipwm.ariel.ctu.unimi.it
- ricesmart.unimi.it
- timelapse.unimi.it
- minerva.unimi.it
- fastutil.di.unimi.it
- www.unimi.it
- cas.unimi.it
- elearning.unimi.it
- sites.unimi.it
- www.convegnodipchi.unimi.it
- elearning.unimi.it
- auth.unimi.it
- authentik.ricerca.sesar.di.unimi.it
- ines.unimi.it
- gatus.ricerca.sesar.di.unimi.it
- algofeed.unimi.it
- harmopicta.unimi.it
- anomalie.unimi.it
- marchi.ricerca.di.unimi.it
- glossarioinclusione.unimi.it
- www.unimi.it
- matematica.unimi.it
- wizardunicloud.unimi.it
- adminer.studenti.di.unimi.it
- cas.unimi.it
- security.di.unimi.it
- sites.unimi.it
- accountstest.di.unimi.it
- orari-be.divsi.unimi.it
- elearning.unimi.it
- tutoraggio.di.unimi.it
- ecare.unimi.it

- postlaurea.myariel.unimi.it
- wikirank-2020.di.unimi.it
- reda.unimi.it
- authentik.ricerca.sesar.di.unimi.it
- convegnodipchi.unimi.it
- delletto.fisica.unimi.it
- prenotazione-new.di.unimi.it
- rnakgview.anacleto.di.unimi.it
- wikirank-2023.di.unimi.it
- www.aislab.di.unimi.it
- gpu.di.unimi.it
- filibusta.crema.unimi.it
- mediacomm.unimi.it
- rustdesk.di.unimi.it
- wikirank-2017.di.unimi.it
- unistem.unimi.it
- fisica.unimi.it
- audioplugins.lim.di.unimi.it
- pong.di.unimi.it
- sp-ex-pwn-1-dhf84ba.laser.di.unimi.it
- www.vaccarilab.unimi.it
- textgen.ricerca.sesar.di.unimi.it
- auth.di.unimi.it
- www.unimi.it
- accounts.di.unimi.it
- lam.cdl.unimi.it
- bibliotecamattioli.unimi.it

5 Domain Related to URLs Found

5.1 Domain: accounts.di.unimi.it

- accounts.di.unimi.it

5.2 Domain: accountstest.di.unimi.it

- accountstest.di.unimi.it

5.3 Domain: adminer.studenti.di.unimi.it

- adminer.studenti.di.unimi.it

5.4 Domain: algofeed.unimi.it

- algofeed.unimi.it

5.5 Domain: anomalie.unimi.it

- anomalie.unimi.it

5.6 Domain: ariel.unimi.it

- postlaurea.myariel.unimi.it

5.7 Domain: audioplugins.lim.di.unimi.it

- audioplugins.lim.di.unimi.it

5.8 Domain: auth.di.unimi.it

- auth.di.unimi.it

5.9 Domain: auth.unimi.it

- auth.unimi.it

5.10 Domain: authentik.ricerca.sesar.di.unimi.it

- authentik.ricerca.sesar.di.unimi.it
- authentik.ricerca.sesar.di.unimi.it

5.11 Domain: bibliotecamattioli.unimi.it

- bibliotecamattioli.unimi.it

5.12 Domain: cas.unimi.it

- cas.unimi.it
- cas.unimi.it

5.13 Domain: convegnodipchi.unimi.it

- www.convegnodipchi.unimi.it
- convegnodipchi.unimi.it

5.14 Domain: delletto.fisica.unimi.it

- delletto.fisica.unimi.it

5.15 Domain: di.unimi.it

- fastutil.di.unimi.it
- authentik.ricerca.sesar.di.unimi.it
- gatus.ricerca.sesar.di.unimi.it
- marchi.ricerca.di.unimi.it
- adminer.studenti.di.unimi.it
- security.di.unimi.it
- accountstest.di.unimi.it
- tutoraggio.di.unimi.it
- wikirank-2020.di.unimi.it
- authentik.ricerca.sesar.di.unimi.it
- prenotazione-new.di.unimi.it
- rnakgview.anacleto.di.unimi.it
- wikirank-2023.di.unimi.it
- www.aislab.di.unimi.it
- gpu.di.unimi.it
- rustdesk.di.unimi.it
- wikirank-2017.di.unimi.it
- audioplugins.lim.di.unimi.it
- pong.di.unimi.it
- sp-ex-pwn-1-dhf84ba.laser.di.unimi.it
- textgen.ricerca.sesar.di.unimi.it
- auth.di.unimi.it
- accounts.di.unimi.it

5.16 Domain: ecare.unimi.it

- ecare.unimi.it

5.17 Domain: elearning.unimi.it

- elearning.unimi.it
- elearning.unimi.it
- elearning.unimi.it

5.18 Domain: fastutil.di.unimi.it

- fastutil.di.unimi.it

5.19 Domain: filibusta.crema.unimi.it

- filibusta.crema.unimi.it

5.20 Domain: fisica.unimi.it

- delletto.fisica.unimi.it
- fisica.unimi.it

5.21 Domain: gatus.ricerca.sesar.di.unimi.it

- gatus.ricerca.sesar.di.unimi.it

5.22 Domain: glossarioinclusione.unimi.it

- glossarioinclusione.unimi.it

5.23 Domain: gpu.di.unimi.it

- gpu.di.unimi.it

5.24 Domain: grafana.ricerca.sesar.di.unimi.it

- authentik.ricerca.sesar.di.unimi.it

5.25 Domain: harmopicta.unimi.it

- harmopicta.unimi.it

5.26 Domain: ines.unimi.it

- ines.unimi.it

5.27 Domain: lam.cdl.unimi.it

- lam.cdl.unimi.it

5.28 Domain: laser.di.unimi.it

- sp-ex-pwn-1-dhf84ba.laser.di.unimi.it

5.29 Domain: marchi.ricerca.di.unimi.it

- marchi.ricerca.di.unimi.it

5.30 Domain: mat.unimi.it

- www.mat.unimi.it

5.31 Domain: matematica.unimi.it

- matematica.unimi.it

5.32 Domain: mediacomm.unimi.it

- mediacomm.unimi.it

5.33 Domain: minerva.unimi.it

- minerva.unimi.it

5.34　Domain: myariel.unimi.it

- postlaurea.myariel.unimi.it

5.35　Domain: orari-be.divsi.unimi.it

- orari-be.divsi.unimi.it

5.36　Domain: pong.di.unimi.it

- pong.di.unimi.it

5.37　Domain: postlaurea.myariel.unimi.it

- postlaurea.myariel.unimi.it

5.38　Domain: postlaureaonline.unimi.it

- elearning.unimi.it

5.39　Domain: prenotazione-new.di.unimi.it

- prenotazione-new.di.unimi.it

5.40　Domain: reda.unimi.it

- reda.unimi.it

5.41　Domain: registrazione.unimi.it

- cas.unimi.it

5.42　Domain: ricesmart.unimi.it

- ricesmart.unimi.it

5.43　Domain: rnakgview.anacleto.di.unimi.it

- rnakgview.anacleto.di.unimi.it

5.44　Domain: rustdesk.di.unimi.it

- rustdesk.di.unimi.it

5.45　Domain: security.di.unimi.it

- security.di.unimi.it

5.46　Domain: sesar.di.unimi.it

- authentik.ricerca.sesar.di.unimi.it
- gatus.ricerca.sesar.di.unimi.it
- authentik.ricerca.sesar.di.unimi.it
- textgen.ricerca.sesar.di.unimi.it

5.47   Domain: sites.unimi.it

- sites.unimi.it
- sites.unimi.it

5.48   Domain: sp-ex-pwn-1-dhf84ba.laser.di.unimi.it

- sp-ex-pwn-1-dhf84ba.laser.di.unimi.it

5.49   Domain: textgen.ricerca.sesar.di.unimi.it

- textgen.ricerca.sesar.di.unimi.it

5.50   Domain: timelapse.unimi.it

- timelapse.unimi.it

5.51   Domain: tutoraggio.di.unimi.it

- tutoraggio.di.unimi.it

5.52   Domain: unistem.unimi.it

- unistem.unimi.it

5.53   Domain: vbellandipwm.ariel.ctu.unimi.it

- vbellandipwm.ariel.ctu.unimi.it

5.54   Domain: wikirank-2017.di.unimi.it

- wikirank-2017.di.unimi.it

5.55   Domain: wikirank-2020.di.unimi.it

- wikirank-2020.di.unimi.it

5.56   Domain: wikirank-2023.di.unimi.it

- wikirank-2023.di.unimi.it

5.57   Domain: wizardunicloud.unimi.it

- wizardunicloud.unimi.it

6 Emails found

Below is the list of Emails found:

- alessandro.leone1@unimi.it
- vweb@unimi.it
- francesca.elli@unimi.it
- ilenia.rossetti@unimi.it
- anna.moroni@unimi.it
- international.students@unimi.it
- ester.luconi@unimi.it
- giorgio.croci@unimi.it
- ermes.movedi@unimi.it
- andrea.barbuti@unimi.it
- giuseppe.marano@unimi.it
- daniele.passarella@unimi.it
- culthum@unimi.it
- redazione.milanoup@unimi.it
- carati@mat.unimi.it
- caterina.laporta@unimi.it
- enrico.sangiovanni@unimi.it
- giulia.fiore@unimi.it
- unicloud@unimi.it
- dario.tamascelli@unimi.it
- redbiolab@unimi.it
- francesco.fortunato@unimi.it
- luca.sacchi@unimi.it
- francesco.auxilia@unimi.it
- dmp@unimi.it
- openscience@unimi.it
- placement.aziende@unimi.it
- maria.gianni@unimi.it
- anna.cariboni@unimi.it
- arnaudmartino.capuzzo@studenti.unimi.it
- matteo.audano@unimi.it
- nome.cognome@unimi.it
- sara.dellatorre@unimi.it

- roberto.oleari@unimi.it
- nome.cognome@studenti.unimi.it
- enza.dauria@unimi.it
- unimibox@unimi.it
- agostino.riva@unimi.it
- giangiacomo.beretta@unimi.it
- stefano.aliberti@unimi.it
- antiplagio@unimi.it
- bd.help@unimi.it
- unitech@unimi.it
- esamiceli@unimi.it
- fabio.parazzini@unimi.it
- riviste@unimi.it
- elena.canavesi@unimi.it
- monica.marzagalli@unimi.it
- vincenzo.marra@unimi.it
- galgani@mat.unimi.it
- studiurp@unimi.it
- giuseppe.banderali@unimi.it
- competenzelinguistiche.slam@unimi.it
- francesco.blasi@unimi.it
- name.surname@unimi.it
- gianluca.lopez@unimi.it
- francesca.calabrese@unimi.it
- rdm@unimi.it
- stage@unimi.it
- irina.figini@unimi.it
- app@unimi.it
- votazioni@unimi.it
- elvira.verduci@unimi.it
- rocco.rinaldo@unimi.it
- marianna.porzio@unimi.it
- livio.luzi@unimi.it
- dataverse@unimi.it
- stefania.corti@unimi.it
- international.agreements@unimi.it

- paolo.brambilla1@unimi.it

- dirse@unimi.it

- formazionelinguistica.slam@unimi.it

- chiara.dilorenzo@unimi.it

- marco.sartorio@unimi.it

- italian.courses@unimi.it

- davide.coduto@studenti.unimi.it

- susanna.esposito@unimi.it

- piercarlo.sarziputtini@unimi.it

- name.surname@studenti.unimi.it

- angelica.bonfanti@unimi.it

- andreina.bordoni@unimi.it

7 Resolved Hosts

Below is a list of resolved hosts with their corresponding IP addresses:

- **10-116-statico.agra.unimi.it** : 159.149.116.10
- **10-117-statico.agra.unimi.it** : 159.149.117.10
- **10-118-statico.agra.unimi.it** : 159.149.118.10
- **10-119-statico.agra.unimi.it** : 159.149.119.10
- **100-116-dhcp.agra.unimi.it** : 159.149.116.100
- **100-117-dhcp.agra.unimi.it** : 159.149.117.100
- **100-118-dhcp.agra.unimi.it** : 159.149.118.100
- **100-119-dhcp.agra.unimi.it** : 159.149.119.100
- **101-116-dhcp.agra.unimi.it** : 159.149.116.101
- **101-117-dhcp.agra.unimi.it** : 159.149.117.101
- **101-118-dhcp.agra.unimi.it** : 159.149.118.101
- **101-119-dhcp.agra.unimi.it** : 159.149.119.101
- **102-116-dhcp.agra.unimi.it** : 159.149.116.102
- **102-117-dhcp.agra.unimi.it** : 159.149.117.102
- **102-118-dhcp.agra.unimi.it** : 159.149.118.102
- **102-119-dhcp.agra.unimi.it** : 159.149.119.102
- **103-116-dhcp.agra.unimi.it** : 159.149.116.103
- **103-117-dhcp.agra.unimi.it** : 159.149.117.103
- **103-118-dhcp.agra.unimi.it** : 159.149.118.103
- **103-119-dhcp.agra.unimi.it** : 159.149.119.103
- **104-116-dhcp.agra.unimi.it** : 159.149.116.104
- **104-117-dhcp.agra.unimi.it** : 159.149.117.104
- **104-118-dhcp.agra.unimi.it** : 159.149.118.104
- **104-119-dhcp.agra.unimi.it** : 159.149.119.104
- **105-116-dhcp.agra.unimi.it** : 159.149.116.105
- **105-117-dhcp.agra.unimi.it** : 159.149.117.105
- **105-118-dhcp.agra.unimi.it** : 159.149.118.105
- **105-119-dhcp.agra.unimi.it** : 159.149.119.105
- **106-116-dhcp.agra.unimi.it** : 159.149.116.106
- **106-117-dhcp.agra.unimi.it** : 159.149.117.106
- **106-118-dhcp.agra.unimi.it** : 159.149.118.106
- **106-119-dhcp.agra.unimi.it** : 159.149.119.106
- **107-116-dhcp.agra.unimi.it** : 159.149.116.107

- **107-117-dhcp.agra.unimi.it** : 159.149.117.107
- **107-118-dhcp.agra.unimi.it** : 159.149.118.107
- **107-119-dhcp.agra.unimi.it** : 159.149.119.107
- **108-116-dhcp.agra.unimi.it** : 159.149.116.108
- **108-117-dhcp.agra.unimi.it** : 159.149.117.108
- **108-118-dhcp.agra.unimi.it** : 159.149.118.108
- **108-119-dhcp.agra.unimi.it** : 159.149.119.108
- **109-116-dhcp.agra.unimi.it** : 159.149.116.109
- **109-117-dhcp.agra.unimi.it** : 159.149.117.109
- **109-118-dhcp.agra.unimi.it** : 159.149.118.109
- **109-119-dhcp.agra.unimi.it** : 159.149.119.109
- **11-116-statico.agra.unimi.it** : 159.149.116.11
- **11-117-statico.agra.unimi.it** : 159.149.117.11
- **11-118-statico.agra.unimi.it** : 159.149.118.11
- **11-119-statico.agra.unimi.it** : 159.149.119.11
- **110-116-dhcp.agra.unimi.it** : 159.149.116.110
- **110-117-dhcp.agra.unimi.it** : 159.149.117.110
- **110-118-dhcp.agra.unimi.it** : 159.149.118.110
- **110-119-dhcp.agra.unimi.it** : 159.149.119.110
- **111-116-dhcp.agra.unimi.it** : 159.149.116.111
- **111-117-dhcp.agra.unimi.it** : 159.149.117.111
- **111-118-dhcp.agra.unimi.it** : 159.149.118.111
- **111-119-dhcp.agra.unimi.it** : 159.149.119.111
- **112-116-dhcp.agra.unimi.it** : 159.149.116.112
- **112-117-dhcp.agra.unimi.it** : 159.149.117.112
- **112-118-dhcp.agra.unimi.it** : 159.149.118.112
- **112-119-dhcp.agra.unimi.it** : 159.149.119.112
- **113-116-dhcp.agra.unimi.it** : 159.149.116.113
- **113-117-dhcp.agra.unimi.it** : 159.149.117.113
- **113-118-dhcp.agra.unimi.it** : 159.149.118.113
- **113-119-dhcp.agra.unimi.it** : 159.149.119.113
- **114-116-dhcp.agra.unimi.it** : 159.149.116.114
- **114-117-dhcp.agra.unimi.it** : 159.149.117.114
- **114-118-dhcp.agra.unimi.it** : 159.149.118.114
- **114-119-dhcp.agra.unimi.it** : 159.149.119.114
- **115-116-dhcp.agra.unimi.it** : 159.149.116.115

- **115-117-dhcp.agra.unimi.it** : 159.149.117.115
- **115-118-dhcp.agra.unimi.it** : 159.149.118.115
- **115-119-dhcp.agra.unimi.it** : 159.149.119.115
- **116-116-dhcp.agra.unimi.it** : 159.149.116.116
- **116-117-dhcp.agra.unimi.it** : 159.149.117.116
- **116-118-dhcp.agra.unimi.it** : 159.149.118.116
- **116-119-dhcp.agra.unimi.it** : 159.149.119.116
- **117-116-dhcp.agra.unimi.it** : 159.149.116.117
- **117-117-dhcp.agra.unimi.it** : 159.149.117.117
- **117-118-dhcp.agra.unimi.it** : 159.149.118.117
- **117-119-dhcp.agra.unimi.it** : 159.149.119.117
- **118-116-dhcp.agra.unimi.it** : 159.149.116.118
- **118-117-dhcp.agra.unimi.it** : 159.149.117.118
- **118-118-dhcp.agra.unimi.it** : 159.149.118.118
- **118-119-dhcp.agra.unimi.it** : 159.149.119.118
- **119-116-dhcp.agra.unimi.it** : 159.149.116.119
- **119-117-dhcp.agra.unimi.it** : 159.149.117.119
- **119-118-dhcp.agra.unimi.it** : 159.149.118.119
- **119-119-dhcp.agra.unimi.it** : 159.149.119.119
- **12-116-statico.agra.unimi.it** : 159.149.116.12
- **12-117-statico.agra.unimi.it** : 159.149.117.12
- **12-118-statico.agra.unimi.it** : 159.149.118.12
- **12-119-statico.agra.unimi.it** : 159.149.119.12
- **120-116-dhcp.agra.unimi.it** : 159.149.116.120
- **120-117-dhcp.agra.unimi.it** : 159.149.117.120
- **120-118-dhcp.agra.unimi.it** : 159.149.118.120
- **120-119-dhcp.agra.unimi.it** : 159.149.119.120
- **121-116-dhcp.agra.unimi.it** : 159.149.116.121
- **121-117-dhcp.agra.unimi.it** : 159.149.117.121
- **121-118-dhcp.agra.unimi.it** : 159.149.118.121
- **121-119-dhcp.agra.unimi.it** : 159.149.119.121
- **122-116-dhcp.agra.unimi.it** : 159.149.116.122
- **122-117-dhcp.agra.unimi.it** : 159.149.117.122
- **122-118-dhcp.agra.unimi.it** : 159.149.118.122
- **122-119-dhcp.agra.unimi.it** : 159.149.119.122
- **123-116-dhcp.agra.unimi.it** : 159.149.116.123

- **123-117-dhcp.agra.unimi.it** : 159.149.117.123
- **123-118-dhcp.agra.unimi.it** : 159.149.118.123
- **123-119-dhcp.agra.unimi.it** : 159.149.119.123
- **124-116-dhcp.agra.unimi.it** : 159.149.116.124
- **124-117-dhcp.agra.unimi.it** : 159.149.117.124
- **124-118-dhcp.agra.unimi.it** : 159.149.118.124
- **124-119-dhcp.agra.unimi.it** : 159.149.119.124
- **125-116-dhcp.agra.unimi.it** : 159.149.116.125
- **125-117-dhcp.agra.unimi.it** : 159.149.117.125
- **125-118-dhcp.agra.unimi.it** : 159.149.118.125
- **125-119-dhcp.agra.unimi.it** : 159.149.119.125
- **126-116-dhcp.agra.unimi.it** : 159.149.116.126
- **126-117-dhcp.agra.unimi.it** : 159.149.117.126
- **126-118-dhcp.agra.unimi.it** : 159.149.118.126
- **126-119-dhcp.agra.unimi.it** : 159.149.119.126
- **127-116-dhcp.agra.unimi.it** : 159.149.116.127
- **127-117-dhcp.agra.unimi.it** : 159.149.117.127
- **127-118-dhcp.agra.unimi.it** : 159.149.118.127
- **127-119-dhcp.agra.unimi.it** : 159.149.119.127
- **128-116-dhcp.agra.unimi.it** : 159.149.116.128
- **128-117-dhcp.agra.unimi.it** : 159.149.117.128
- **128-118-dhcp.agra.unimi.it** : 159.149.118.128
- **128-119-dhcp.agra.unimi.it** : 159.149.119.128
- **129-116-dhcp.agra.unimi.it** : 159.149.116.129
- **129-117-dhcp.agra.unimi.it** : 159.149.117.129
- **129-118-dhcp.agra.unimi.it** : 159.149.118.129
- **129-119-dhcp.agra.unimi.it** : 159.149.119.129
- **13-116-statico.agra.unimi.it** : 159.149.116.13
- **13-117-statico.agra.unimi.it** : 159.149.117.13
- **13-119-statico.agra.unimi.it** : 159.149.119.13
- **130-116-dhcp.agra.unimi.it** : 159.149.116.130
- **130-117-dhcp.agra.unimi.it** : 159.149.117.130
- **130-118-dhcp.agra.unimi.it** : 159.149.118.130
- **130-119-dhcp.agra.unimi.it** : 159.149.119.130
- **131-116-dhcp.agra.unimi.it** : 159.149.116.131
- **131-117-dhcp.agra.unimi.it** : 159.149.117.131

- **131-118-dhcp.agra.unimi.it** : 159.149.118.131
- **131-119-dhcp.agra.unimi.it** : 159.149.119.131
- **132-116-dhcp.agra.unimi.it** : 159.149.116.132
- **132-117-dhcp.agra.unimi.it** : 159.149.117.132
- **132-118-dhcp.agra.unimi.it** : 159.149.118.132
- **132-119-dhcp.agra.unimi.it** : 159.149.119.132
- **133-116-dhcp.agra.unimi.it** : 159.149.116.133
- **133-117-dhcp.agra.unimi.it** : 159.149.117.133
- **133-118-dhcp.agra.unimi.it** : 159.149.118.133
- **133-119-dhcp.agra.unimi.it** : 159.149.119.133
- **134-116-dhcp.agra.unimi.it** : 159.149.116.134
- **134-117-dhcp.agra.unimi.it** : 159.149.117.134
- **134-118-dhcp.agra.unimi.it** : 159.149.118.134
- **134-119-dhcp.agra.unimi.it** : 159.149.119.134
- **135-116-dhcp.agra.unimi.it** : 159.149.116.135
- **135-117-dhcp.agra.unimi.it** : 159.149.117.135
- **135-118-dhcp.agra.unimi.it** : 159.149.118.135
- **135-119-dhcp.agra.unimi.it** : 159.149.119.135
- **136-116-dhcp.agra.unimi.it** : 159.149.116.136
- **136-117-dhcp.agra.unimi.it** : 159.149.117.136
- **136-118-dhcp.agra.unimi.it** : 159.149.118.136
- **136-119-dhcp.agra.unimi.it** : 159.149.119.136
- **137-116-dhcp.agra.unimi.it** : 159.149.116.137
- **137-117-dhcp.agra.unimi.it** : 159.149.117.137
- **137-118-dhcp.agra.unimi.it** : 159.149.118.137
- **137-119-dhcp.agra.unimi.it** : 159.149.119.137
- **138-116-dhcp.agra.unimi.it** : 159.149.116.138
- **138-117-dhcp.agra.unimi.it** : 159.149.117.138
- **138-118-dhcp.agra.unimi.it** : 159.149.118.138
- **138-119-dhcp.agra.unimi.it** : 159.149.119.138
- **139-116-dhcp.agra.unimi.it** : 159.149.116.139
- **139-117-dhcp.agra.unimi.it** : 159.149.117.139
- **139-118-dhcp.agra.unimi.it** : 159.149.118.139
- **139-119-dhcp.agra.unimi.it** : 159.149.119.139
- **14-116-statico.agra.unimi.it** : 159.149.116.14
- **14-117-statico.agra.unimi.it** : 159.149.117.14

- **14-119-statico.agra.unimi.it** : 159.149.119.14
- **140-116-dhcp.agra.unimi.it** : 159.149.116.140
- **140-117-dhcp.agra.unimi.it** : 159.149.117.140
- **140-118-dhcp.agra.unimi.it** : 159.149.118.140
- **140-119-dhcp.agra.unimi.it** : 159.149.119.140
- **141-116-dhcp.agra.unimi.it** : 159.149.116.141
- **141-117-dhcp.agra.unimi.it** : 159.149.117.141
- **141-118-dhcp.agra.unimi.it** : 159.149.118.141
- **141-119-dhcp.agra.unimi.it** : 159.149.119.141
- **142-116-dhcp.agra.unimi.it** : 159.149.116.142
- **142-117-dhcp.agra.unimi.it** : 159.149.117.142
- **142-118-dhcp.agra.unimi.it** : 159.149.118.142
- **142-119-dhcp.agra.unimi.it** : 159.149.119.142
- **143-116-dhcp.agra.unimi.it** : 159.149.116.143
- **143-117-dhcp.agra.unimi.it** : 159.149.117.143
- **143-118-dhcp.agra.unimi.it** : 159.149.118.143
- **143-119-dhcp.agra.unimi.it** : 159.149.119.143
- **144-116-dhcp.agra.unimi.it** : 159.149.116.144
- **144-117-dhcp.agra.unimi.it** : 159.149.117.144
- **144-118-dhcp.agra.unimi.it** : 159.149.118.144
- **144-119-dhcp.agra.unimi.it** : 159.149.119.144
- **145-116-dhcp.agra.unimi.it** : 159.149.116.145
- **145-117-dhcp.agra.unimi.it** : 159.149.117.145
- **145-118-dhcp.agra.unimi.it** : 159.149.118.145
- **145-119-dhcp.agra.unimi.it** : 159.149.119.145
- **146-116-dhcp.agra.unimi.it** : 159.149.116.146
- **146-117-dhcp.agra.unimi.it** : 159.149.117.146
- **146-119-dhcp.agra.unimi.it** : 159.149.119.146
- **147-116-dhcp.agra.unimi.it** : 159.149.116.147
- **147-117-dhcp.agra.unimi.it** : 159.149.117.147
- **147-118-dhcp.agra.unimi.it** : 159.149.118.147
- **147-119-dhcp.agra.unimi.it** : 159.149.119.147
- **148-116-dhcp.agra.unimi.it** : 159.149.116.148
- **148-117-dhcp.agra.unimi.it** : 159.149.117.148
- **148-118-dhcp.agra.unimi.it** : 159.149.118.148
- **148-119-dhcp.agra.unimi.it** : 159.149.119.148

- **149-116-dhcp.agra.unimi.it** : 159.149.116.149
- **149-117-dhcp.agra.unimi.it** : 159.149.117.149
- **149-118-dhcp.agra.unimi.it** : 159.149.118.149
- **149-119-dhcp.agra.unimi.it** : 159.149.119.149
- **15-116-statico.agra.unimi.it** : 159.149.116.15
- **15-117-statico.agra.unimi.it** : 159.149.117.15
- **15-119-statico.agra.unimi.it** : 159.149.119.15
- **150-116-dhcp.agra.unimi.it** : 159.149.116.150
- **150-117-dhcp.agra.unimi.it** : 159.149.117.150
- **150-118-dhcp.agra.unimi.it** : 159.149.118.150
- **150-119-dhcp.agra.unimi.it** : 159.149.119.150
- **151-116-dhcp.agra.unimi.it** : 159.149.116.151
- **151-117-dhcp.agra.unimi.it** : 159.149.117.151
- **151-118-dhcp.agra.unimi.it** : 159.149.118.151
- **151-119-dhcp.agra.unimi.it** : 159.149.119.151
- **152-116-dhcp.agra.unimi.it** : 159.149.116.152
- **152-117-dhcp.agra.unimi.it** : 159.149.117.152
- **152-118-dhcp.agra.unimi.it** : 159.149.118.152
- **152-119-dhcp.agra.unimi.it** : 159.149.119.152
- **153-116-dhcp.agra.unimi.it** : 159.149.116.153
- **153-117-dhcp.agra.unimi.it** : 159.149.117.153
- **153-118-dhcp.agra.unimi.it** : 159.149.118.153
- **153-119-dhcp.agra.unimi.it** : 159.149.119.153
- **154-116-dhcp.agra.unimi.it** : 159.149.116.154
- **154-117-dhcp.agra.unimi.it** : 159.149.117.154
- **154-118-dhcp.agra.unimi.it** : 159.149.118.154
- **154-119-dhcp.agra.unimi.it** : 159.149.119.154
- **155-116-dhcp.agra.unimi.it** : 159.149.116.155
- **155-117-dhcp.agra.unimi.it** : 159.149.117.155
- **155-118-dhcp.agra.unimi.it** : 159.149.118.155
- **155-119-dhcp.agra.unimi.it** : 159.149.119.155
- **156-116-dhcp.agra.unimi.it** : 159.149.116.156
- **156-117-dhcp.agra.unimi.it** : 159.149.117.156
- **156-118-dhcp.agra.unimi.it** : 159.149.118.156
- **156-119-dhcp.agra.unimi.it** : 159.149.119.156
- **157-116-dhcp.agra.unimi.it** : 159.149.116.157

- **157-117-dhcp.agra.unimi.it** : 159.149.117.157
- **157-118-dhcp.agra.unimi.it** : 159.149.118.157
- **157-119-dhcp.agra.unimi.it** : 159.149.119.157
- **158-116-dhcp.agra.unimi.it** : 159.149.116.158
- **158-117-dhcp.agra.unimi.it** : 159.149.117.158
- **158-118-dhcp.agra.unimi.it** : 159.149.118.158
- **158-119-dhcp.agra.unimi.it** : 159.149.119.158
- **159-116-dhcp.agra.unimi.it** : 159.149.116.159
- **159-117-dhcp.agra.unimi.it** : 159.149.117.159
- **159-118-dhcp.agra.unimi.it** : 159.149.118.159
- **159-119-dhcp.agra.unimi.it** : 159.149.119.159
- **16-116-dhcp.agra.unimi.it** : 159.149.116.16
- **16-117-dhcp.agra.unimi.it** : 159.149.117.16
- **16-118-dhcp.agra.unimi.it** : 159.149.118.16
- **16-119-dhcp.agra.unimi.it** : 159.149.119.16
- **160-116-dhcp.agra.unimi.it** : 159.149.116.160
- **160-117-dhcp.agra.unimi.it** : 159.149.117.160
- **160-118-dhcp.agra.unimi.it** : 159.149.118.160
- **160-119-dhcp.agra.unimi.it** : 159.149.119.160
- **161-116-dhcp.agra.unimi.it** : 159.149.116.161
- **161-117-dhcp.agra.unimi.it** : 159.149.117.161
- **161-118-dhcp.agra.unimi.it** : 159.149.118.161
- **161-119-dhcp.agra.unimi.it** : 159.149.119.161
- **162-116-dhcp.agra.unimi.it** : 159.149.116.162
- **162-117-dhcp.agra.unimi.it** : 159.149.117.162
- **162-118-dhcp.agra.unimi.it** : 159.149.118.162
- **162-119-dhcp.agra.unimi.it** : 159.149.119.162
- **163-116-dhcp.agra.unimi.it** : 159.149.116.163
- **163-117-dhcp.agra.unimi.it** : 159.149.117.163
- **163-118-dhcp.agra.unimi.it** : 159.149.118.163
- **163-119-dhcp.agra.unimi.it** : 159.149.119.163
- **164-116-dhcp.agra.unimi.it** : 159.149.116.164
- **164-117-dhcp.agra.unimi.it** : 159.149.117.164
- **164-118-dhcp.agra.unimi.it** : 159.149.118.164
- **164-119-dhcp.agra.unimi.it** : 159.149.119.164
- **165-116-dhcp.agra.unimi.it** : 159.149.116.165

- **165-117-dhcp.agra.unimi.it** : 159.149.117.165
- **165-118-dhcp.agra.unimi.it** : 159.149.118.165
- **165-119-dhcp.agra.unimi.it** : 159.149.119.165
- **166-116-dhcp.agra.unimi.it** : 159.149.116.166
- **166-117-dhcp.agra.unimi.it** : 159.149.117.166
- **166-118-dhcp.agra.unimi.it** : 159.149.118.166
- **166-119-dhcp.agra.unimi.it** : 159.149.119.166
- **167-116-dhcp.agra.unimi.it** : 159.149.116.167
- **167-117-dhcp.agra.unimi.it** : 159.149.117.167
- **167-118-dhcp.agra.unimi.it** : 159.149.118.167
- **167-119-dhcp.agra.unimi.it** : 159.149.119.167
- **168-116-dhcp.agra.unimi.it** : 159.149.116.168
- **168-117-dhcp.agra.unimi.it** : 159.149.117.168
- **168-118-dhcp.agra.unimi.it** : 159.149.118.168
- **168-119-dhcp.agra.unimi.it** : 159.149.119.168
- **169-116-dhcp.agra.unimi.it** : 159.149.116.169
- **169-117-dhcp.agra.unimi.it** : 159.149.117.169
- **169-118-dhcp.agra.unimi.it** : 159.149.118.169
- **169-119-dhcp.agra.unimi.it** : 159.149.119.169
- **17-116-dhcp.agra.unimi.it** : 159.149.116.17
- **17-117-dhcp.agra.unimi.it** : 159.149.117.17
- **17-118-dhcp.agra.unimi.it** : 159.149.118.17
- **170-116-dhcp.agra.unimi.it** : 159.149.116.170
- **170-117-dhcp.agra.unimi.it** : 159.149.117.170
- **170-118-dhcp.agra.unimi.it** : 159.149.118.170
- **170-119-dhcp.agra.unimi.it** : 159.149.119.170
- **171-116-dhcp.agra.unimi.it** : 159.149.116.171
- **171-117-dhcp.agra.unimi.it** : 159.149.117.171
- **171-118-dhcp.agra.unimi.it** : 159.149.118.171
- **171-119-dhcp.agra.unimi.it** : 159.149.119.171
- **172-116-dhcp.agra.unimi.it** : 159.149.116.172
- **172-117-dhcp.agra.unimi.it** : 159.149.117.172
- **172-118-dhcp.agra.unimi.it** : 159.149.118.172
- **172-119-dhcp.agra.unimi.it** : 159.149.119.172
- **173-116-dhcp.agra.unimi.it** : 159.149.116.173
- **173-117-dhcp.agra.unimi.it** : 159.149.117.173

- **173-118-dhcp.agra.unimi.it** : 159.149.118.173
- **173-119-dhcp.agra.unimi.it** : 159.149.119.173
- **174-116-dhcp.agra.unimi.it** : 159.149.116.174
- **174-117-dhcp.agra.unimi.it** : 159.149.117.174
- **174-118-dhcp.agra.unimi.it** : 159.149.118.174
- **174-119-dhcp.agra.unimi.it** : 159.149.119.174
- **175-116-dhcp.agra.unimi.it** : 159.149.116.175
- **175-117-dhcp.agra.unimi.it** : 159.149.117.175
- **175-118-dhcp.agra.unimi.it** : 159.149.118.175
- **175-119-dhcp.agra.unimi.it** : 159.149.119.175
- **176-116-dhcp.agra.unimi.it** : 159.149.116.176
- **176-117-dhcp.agra.unimi.it** : 159.149.117.176
- **176-118-dhcp.agra.unimi.it** : 159.149.118.176
- **176-119-dhcp.agra.unimi.it** : 159.149.119.176
- **177-116-dhcp.agra.unimi.it** : 159.149.116.177
- **177-117-dhcp.agra.unimi.it** : 159.149.117.177
- **177-118-dhcp.agra.unimi.it** : 159.149.118.177
- **177-119-dhcp.agra.unimi.it** : 159.149.119.177
- **178-116-dhcp.agra.unimi.it** : 159.149.116.178
- **178-117-dhcp.agra.unimi.it** : 159.149.117.178
- **178-118-dhcp.agra.unimi.it** : 159.149.118.178
- **178-119-dhcp.agra.unimi.it** : 159.149.119.178
- **179-116-dhcp.agra.unimi.it** : 159.149.116.179
- **179-117-dhcp.agra.unimi.it** : 159.149.117.179
- **179-118-dhcp.agra.unimi.it** : 159.149.118.179
- **179-119-dhcp.agra.unimi.it** : 159.149.119.179
- **18-116-dhcp.agra.unimi.it** : 159.149.116.18
- **18-117-dhcp.agra.unimi.it** : 159.149.117.18
- **18-118-dhcp.agra.unimi.it** : 159.149.118.18
- **18-119-dhcp.agra.unimi.it** : 159.149.119.18
- **180-116-dhcp.agra.unimi.it** : 159.149.116.180
- **180-117-dhcp.agra.unimi.it** : 159.149.117.180
- **180-118-dhcp.agra.unimi.it** : 159.149.118.180
- **180-119-dhcp.agra.unimi.it** : 159.149.119.180
- **181-116-dhcp.agra.unimi.it** : 159.149.116.181
- **181-117-dhcp.agra.unimi.it** : 159.149.117.181

- **181-118-dhcp.agra.unimi.it** : 159.149.118.181
- **182-116-dhcp.agra.unimi.it** : 159.149.116.182
- **182-117-dhcp.agra.unimi.it** : 159.149.117.182
- **182-118-dhcp.agra.unimi.it** : 159.149.118.182
- **182-119-dhcp.agra.unimi.it** : 159.149.119.182
- **183-116-dhcp.agra.unimi.it** : 159.149.116.183
- **183-117-dhcp.agra.unimi.it** : 159.149.117.183
- **183-118-dhcp.agra.unimi.it** : 159.149.118.183
- **183-119-dhcp.agra.unimi.it** : 159.149.119.183
- **184-116-dhcp.agra.unimi.it** : 159.149.116.184
- **184-117-dhcp.agra.unimi.it** : 159.149.117.184
- **184-118-dhcp.agra.unimi.it** : 159.149.118.184
- **184-119-dhcp.agra.unimi.it** : 159.149.119.184
- **185-116-dhcp.agra.unimi.it** : 159.149.116.185
- **185-117-dhcp.agra.unimi.it** : 159.149.117.185
- **185-118-dhcp.agra.unimi.it** : 159.149.118.185
- **185-119-dhcp.agra.unimi.it** : 159.149.119.185
- **186-116-dhcp.agra.unimi.it** : 159.149.116.186
- **186-117-dhcp.agra.unimi.it** : 159.149.117.186
- **186-118-dhcp.agra.unimi.it** : 159.149.118.186
- **186-119-dhcp.agra.unimi.it** : 159.149.119.186
- **187-116-dhcp.agra.unimi.it** : 159.149.116.187
- **187-117-dhcp.agra.unimi.it** : 159.149.117.187
- **187-118-dhcp.agra.unimi.it** : 159.149.118.187
- **187-119-dhcp.agra.unimi.it** : 159.149.119.187
- **188-116-dhcp.agra.unimi.it** : 159.149.116.188
- **188-117-dhcp.agra.unimi.it** : 159.149.117.188
- **188-118-dhcp.agra.unimi.it** : 159.149.118.188
- **188-119-dhcp.agra.unimi.it** : 159.149.119.188
- **189-116-dhcp.agra.unimi.it** : 159.149.116.189
- **189-117-dhcp.agra.unimi.it** : 159.149.117.189
- **189-118-dhcp.agra.unimi.it** : 159.149.118.189
- **189-119-dhcp.agra.unimi.it** : 159.149.119.189
- **19-116-dhcp.agra.unimi.it** : 159.149.116.19
- **19-117-dhcp.agra.unimi.it** : 159.149.117.19
- **19-118-dhcp.agra.unimi.it** : 159.149.118.19

- **19-119-dhcp.agra.unimi.it** : 159.149.119.19
- **190-116-dhcp.agra.unimi.it** : 159.149.116.190
- **190-117-dhcp.agra.unimi.it** : 159.149.117.190
- **190-118-dhcp.agra.unimi.it** : 159.149.118.190
- **190-119-dhcp.agra.unimi.it** : 159.149.119.190
- **191-116-dhcp.agra.unimi.it** : 159.149.116.191
- **191-117-dhcp.agra.unimi.it** : 159.149.117.191
- **191-118-dhcp.agra.unimi.it** : 159.149.118.191
- **191-119-dhcp.agra.unimi.it** : 159.149.119.191
- **192-116-dhcp.agra.unimi.it** : 159.149.116.192
- **192-117-dhcp.agra.unimi.it** : 159.149.117.192
- **192-118-dhcp.agra.unimi.it** : 159.149.118.192
- **192-119-dhcp.agra.unimi.it** : 159.149.119.192
- **193-116-dhcp.agra.unimi.it** : 159.149.116.193
- **193-117-dhcp.agra.unimi.it** : 159.149.117.193
- **193-118-dhcp.agra.unimi.it** : 159.149.118.193
- **193-119-dhcp.agra.unimi.it** : 159.149.119.193
- **194-116-dhcp.agra.unimi.it** : 159.149.116.194
- **194-117-dhcp.agra.unimi.it** : 159.149.117.194
- **194-118-dhcp.agra.unimi.it** : 159.149.118.194
- **194-119-dhcp.agra.unimi.it** : 159.149.119.194
- **195-116-dhcp.agra.unimi.it** : 159.149.116.195
- **195-117-dhcp.agra.unimi.it** : 159.149.117.195
- **195-118-dhcp.agra.unimi.it** : 159.149.118.195
- **195-119-dhcp.agra.unimi.it** : 159.149.119.195
- **196-116-dhcp.agra.unimi.it** : 159.149.116.196
- **196-117-dhcp.agra.unimi.it** : 159.149.117.196
- **196-118-dhcp.agra.unimi.it** : 159.149.118.196
- **196-119-dhcp.agra.unimi.it** : 159.149.119.196
- **197-116-dhcp.agra.unimi.it** : 159.149.116.197
- **197-117-dhcp.agra.unimi.it** : 159.149.117.197
- **197-118-dhcp.agra.unimi.it** : 159.149.118.197
- **197-119-dhcp.agra.unimi.it** : 159.149.119.197
- **198-116-dhcp.agra.unimi.it** : 159.149.116.198
- **198-117-dhcp.agra.unimi.it** : 159.149.117.198
- **198-118-dhcp.agra.unimi.it** : 159.149.118.198

- **198-119-dhcp.agra.unimi.it** : 159.149.119.198
- **199-116-dhcp.agra.unimi.it** : 159.149.116.199
- **199-117-dhcp.agra.unimi.it** : 159.149.117.199
- **199-118-dhcp.agra.unimi.it** : 159.149.118.199
- **199-119-dhcp.agra.unimi.it** : 159.149.119.199
- **20-116-dhcp.agra.unimi.it** : 159.149.116.20
- **20-117-dhcp.agra.unimi.it** : 159.149.117.20
- **20-118-dhcp.agra.unimi.it** : 159.149.118.20
- **20-119-dhcp.agra.unimi.it** : 159.149.119.20
- **200-116-dhcp.agra.unimi.it** : 159.149.116.200
- **200-117-dhcp.agra.unimi.it** : 159.149.117.200
- **200-118-dhcp.agra.unimi.it** : 159.149.118.200
- **200-119-dhcp.agra.unimi.it** : 159.149.119.200
- **201-116-dhcp.agra.unimi.it** : 159.149.116.201
- **201-117-dhcp.agra.unimi.it** : 159.149.117.201
- **201-118-dhcp.agra.unimi.it** : 159.149.118.201
- **201-119-dhcp.agra.unimi.it** : 159.149.119.201
- **202-116-dhcp.agra.unimi.it** : 159.149.116.202
- **202-117-dhcp.agra.unimi.it** : 159.149.117.202
- **202-118-dhcp.agra.unimi.it** : 159.149.118.202
- **202-119-dhcp.agra.unimi.it** : 159.149.119.202
- **203-116-dhcp.agra.unimi.it** : 159.149.116.203
- **203-117-dhcp.agra.unimi.it** : 159.149.117.203
- **203-118-dhcp.agra.unimi.it** : 159.149.118.203
- **203-119-dhcp.agra.unimi.it** : 159.149.119.203
- **204-116-dhcp.agra.unimi.it** : 159.149.116.204
- **204-117-dhcp.agra.unimi.it** : 159.149.117.204
- **204-118-dhcp.agra.unimi.it** : 159.149.118.204
- **204-119-dhcp.agra.unimi.it** : 159.149.119.204
- **205-116-dhcp.agra.unimi.it** : 159.149.116.205
- **205-117-dhcp.agra.unimi.it** : 159.149.117.205
- **205-118-dhcp.agra.unimi.it** : 159.149.118.205
- **205-119-dhcp.agra.unimi.it** : 159.149.119.205
- **206-116-dhcp.agra.unimi.it** : 159.149.116.206
- **206-117-dhcp.agra.unimi.it** : 159.149.117.206
- **206-119-dhcp.agra.unimi.it** : 159.149.119.206

- **207-116-dhcp.agra.unimi.it** : 159.149.116.207
- **207-117-dhcp.agra.unimi.it** : 159.149.117.207
- **207-118-dhcp.agra.unimi.it** : 159.149.118.207
- **207-119-dhcp.agra.unimi.it** : 159.149.119.207
- **208-116-dhcp.agra.unimi.it** : 159.149.116.208
- **208-117-dhcp.agra.unimi.it** : 159.149.117.208
- **208-118-dhcp.agra.unimi.it** : 159.149.118.208
- **208-119-dhcp.agra.unimi.it** : 159.149.119.208
- **209-116-dhcp.agra.unimi.it** : 159.149.116.209
- **209-117-dhcp.agra.unimi.it** : 159.149.117.209
- **209-118-dhcp.agra.unimi.it** : 159.149.118.209
- **209-119-dhcp.agra.unimi.it** : 159.149.119.209
- **21-116-dhcp.agra.unimi.it** : 159.149.116.21
- **21-117-dhcp.agra.unimi.it** : 159.149.117.21
- **21-118-dhcp.agra.unimi.it** : 159.149.118.21
- **21-119-dhcp.agra.unimi.it** : 159.149.119.21
- **210-116-dhcp.agra.unimi.it** : 159.149.116.210
- **210-117-dhcp.agra.unimi.it** : 159.149.117.210
- **210-118-dhcp.agra.unimi.it** : 159.149.118.210
- **210-119-dhcp.agra.unimi.it** : 159.149.119.210
- **211-116-dhcp.agra.unimi.it** : 159.149.116.211
- **211-117-dhcp.agra.unimi.it** : 159.149.117.211
- **211-118-dhcp.agra.unimi.it** : 159.149.118.211
- **212-116-dhcp.agra.unimi.it** : 159.149.116.212
- **212-117-dhcp.agra.unimi.it** : 159.149.117.212
- **212-118-dhcp.agra.unimi.it** : 159.149.118.212
- **212-119-dhcp.agra.unimi.it** : 159.149.119.212
- **213-116-dhcp.agra.unimi.it** : 159.149.116.213
- **213-117-dhcp.agra.unimi.it** : 159.149.117.213
- **213-118-dhcp.agra.unimi.it** : 159.149.118.213
- **213-119-dhcp.agra.unimi.it** : 159.149.119.213
- **214-116-dhcp.agra.unimi.it** : 159.149.116.214
- **214-117-dhcp.agra.unimi.it** : 159.149.117.214
- **214-118-dhcp.agra.unimi.it** : 159.149.118.214
- **214-119-dhcp.agra.unimi.it** : 159.149.119.214
- **215-116-dhcp.agra.unimi.it** : 159.149.116.215

- **215-117-dhcp.agra.unimi.it** : 159.149.117.215
- **215-118-dhcp.agra.unimi.it** : 159.149.118.215
- **215-119-dhcp.agra.unimi.it** : 159.149.119.215
- **22-116-dhcp.agra.unimi.it** : 159.149.116.22
- **22-118-dhcp.agra.unimi.it** : 159.149.118.22
- **23-116-dhcp.agra.unimi.it** : 159.149.116.23
- **23-117-dhcp.agra.unimi.it** : 159.149.117.23
- **23-118-dhcp.agra.unimi.it** : 159.149.118.23
- **232-116-statico.agra.unimi.it** : 159.149.116.232
- **234-116-statico.agra.unimi.it** : 159.149.116.234
- **235-116-statico.agra.unimi.it** : 159.149.116.235
- **236-116-statico.agra.unimi.it** : 159.149.116.236
- **236-118-statico.agra.unimi.it** : 159.149.118.236
- **237-116-statico.agra.unimi.it** : 159.149.116.237
- **237-118-statico.agra.unimi.it** : 159.149.118.237
- **238-116-statico.agra.unimi.it** : 159.149.116.238
- **238-118-statico.agra.unimi.it** : 159.149.118.238
- **239-118-statico.agra.unimi.it** : 159.149.118.239
- **24-116-dhcp.agra.unimi.it** : 159.149.116.24
- **24-117-dhcp.agra.unimi.it** : 159.149.117.24
- **24-118-dhcp.agra.unimi.it** : 159.149.118.24
- **24-119-dhcp.agra.unimi.it** : 159.149.119.24
- **240-116-statico.agra.unimi.it** : 159.149.116.240
- **240-118-statico.agra.unimi.it** : 159.149.118.240
- **241-118-statico.agra.unimi.it** : 159.149.118.241
- **242-118-statico.agra.unimi.it** : 159.149.118.242
- **243-116-statico.agra.unimi.it** : 159.149.116.243
- **243-118-statico.agra.unimi.it** : 159.149.118.243
- **244-116-statico.agra.unimi.it** : 159.149.116.244
- **246-118-statico.agra.unimi.it** : 159.149.118.246
- **246-119-statico.agra.unimi.it** : 159.149.119.246
- **247-117-statico.agra.unimi.it** : 159.149.117.247
- **247-118-statico.agra.unimi.it** : 159.149.118.247
- **247-119-statico.agra.unimi.it** : 159.149.119.247
- **248-117-statico.agra.unimi.it** : 159.149.117.248
- **248-118-statico.agra.unimi.it** : 159.149.118.248

- **248-119-statico.agra.unimi.it** : 159.149.119.248
- **249-118-statico.agra.unimi.it** : 159.149.118.249
- **249-119-statico.agra.unimi.it** : 159.149.119.249
- **25-116-dhcp.agra.unimi.it** : 159.149.116.25
- **25-117-dhcp.agra.unimi.it** : 159.149.117.25
- **25-118-dhcp.agra.unimi.it** : 159.149.118.25
- **25-119-dhcp.agra.unimi.it** : 159.149.119.25
- **250-117-statico.agra.unimi.it** : 159.149.117.250
- **250-118-statico.agra.unimi.it** : 159.149.118.250
- **251-117-statico.agra.unimi.it** : 159.149.117.251
- **251-118-statico.agra.unimi.it** : 159.149.118.251
- **251-119-statico.agra.unimi.it** : 159.149.119.251
- **252-117-statico.agra.unimi.it** : 159.149.117.252
- **252-118-statico.agra.unimi.it** : 159.149.118.252
- **252-119-statico.agra.unimi.it** : 159.149.119.252
- **253-117-statico.agra.unimi.it** : 159.149.117.253
- **253-118-statico.agra.unimi.it** : 159.149.118.253
- **253-119-statico.agra.unimi.it** : 159.149.119.253
- **254-117-statico.agra.unimi.it** : 159.149.117.254
- **254-119-statico.agra.unimi.it** : 159.149.119.254
- **26-117-dhcp.agra.unimi.it** : 159.149.117.26
- **26-119-dhcp.agra.unimi.it** : 159.149.119.26
- **27-116-dhcp.agra.unimi.it** : 159.149.116.27
- **27-117-dhcp.agra.unimi.it** : 159.149.117.27
- **27-118-dhcp.agra.unimi.it** : 159.149.118.27
- **27-119-dhcp.agra.unimi.it** : 159.149.119.27
- **28-116-dhcp.agra.unimi.it** : 159.149.116.28
- **28-117-dhcp.agra.unimi.it** : 159.149.117.28
- **28-118-dhcp.agra.unimi.it** : 159.149.118.28
- **28-119-dhcp.agra.unimi.it** : 159.149.119.28
- **29-116-dhcp.agra.unimi.it** : 159.149.116.29
- **29-117-dhcp.agra.unimi.it** : 159.149.117.29
- **29-118-dhcp.agra.unimi.it** : 159.149.118.29
- **29-119-dhcp.agra.unimi.it** : 159.149.119.29
- **30-117-dhcp.agra.unimi.it** : 159.149.117.30
- **30-118-dhcp.agra.unimi.it** : 159.149.118.30

- **31-116-dhcp.agra.unimi.it** : 159.149.116.31
- **31-117-dhcp.agra.unimi.it** : 159.149.117.31
- **31-118-dhcp.agra.unimi.it** : 159.149.118.31
- **31-119-dhcp.agra.unimi.it** : 159.149.119.31
- **32-116-dhcp.agra.unimi.it** : 159.149.116.32
- **32-117-dhcp.agra.unimi.it** : 159.149.117.32
- **32-118-dhcp.agra.unimi.it** : 159.149.118.32
- **32-119-dhcp.agra.unimi.it** : 159.149.119.32
- **33-117-dhcp.agra.unimi.it** : 159.149.117.33
- **33-118-dhcp.agra.unimi.it** : 159.149.118.33
- **33-119-dhcp.agra.unimi.it** : 159.149.119.33
- **34-116-dhcp.agra.unimi.it** : 159.149.116.34
- **34-119-dhcp.agra.unimi.it** : 159.149.119.34
- **Studente.unimi.it** : 159.149.53.239
- **accounts.di.unimi.it** : 159.149.130.182
- **accountstest.di.unimi.it** : 159.149.130.178
- **adapt-lab.di.unimi.it** : 159.149.129.224
- **adapt-lab.ricerca.di.unimi.it** : 159.149.129.224
- **adipascaledds.ariel.ctu.unimi.it** : 159.149.15.42
- **adminer.studenti.di.unimi.it** : 159.149.130.182
- **afferenti.fisica.unimi.it** : 159.149.45.8
- **air.unimi.it** : 130.186.28.54
- **ais-lab.di.unimi.it** : 159.149.130.139
- **alertmanager.cloud.di.unimi.it** : 159.149.142.185
- **algofeed.unimi.it** : 159.149.53.246
- **alos.di.unimi.it** : 159.149.130.139
- **an-icon.unimi.it** : 159.149.53.132
- **anomalie.unimi.it** : 159.149.53.246
- **anticorruzione.ariel.ctu.unimi.it** : 159.149.15.42
- **apegeo.unimi.it** : 159.149.53.241
- **api.accounts.di.unimi.it** : 159.149.130.182
- **api.minio.ricerca.sesar.di.unimi.it** : 159.149.147.136
- **apps.unimi.it** : 159.149.53.221
- **appuntamenti.servicemanagement.unimi.it** : 159.149.53.196
- **aqm4.fisica.unimi.it** : 193.205.78.171
- **archive4j.di.unimi.it** : 159.149.136.4

- **argo.islab.di.unimi.it** : 159.149.147.194
- **argocd.ricerca.sesar.di.unimi.it** : 159.149.147.136
- **ariel.unimi.it** : 159.149.15.43
- **asardellapd.ariel.ctu.unimi.it** : 159.149.15.42
- **assistenzasanitaria.cdl.unimi.it** : 130.186.7.246
- **astro.fisica.unimi.it** : 193.205.78.171
- **audioplugins.lim.di.unimi.it** : 159.149.133.149
- **auth.di.unimi.it** : 159.149.130.182
- **auth.unimi.it** : 159.149.105.179
- **authentik.ricerca.sesar.di.unimi.it** : 159.149.147.136
- **autoconfig.laser.di.unimi.it** : 159.149.145.136
- **ayw2023.di.unimi.it** : 159.149.130.139
- **bacheca2lv.fisica.unimi.it** : 159.149.45.32
- **basilico.di.unimi.it** : 159.149.130.139
- **beccaria.unimi.it** : 159.149.53.164
- **bellettini.di.unimi.it** : 159.149.130.139
- **benessereanimale.unimi.it** : 159.149.53.246
- **bibliotecamattioli.unimi.it** : 159.149.53.132
- **bioms2013.di.unimi.it** : 159.149.130.139
- **biosciences.unimi.it** : 159.149.53.164
- **bioscienze.unimi.it** : 159.149.53.164
- **bioscienzebio.unimi.it** : 159.149.53.241
- **biotecnologiemediche.cdl.unimi.it** : 130.186.7.246
- **bitwarden.di.unimi.it** : 159.149.130.182
- **bitwarden.ricerca.sesar.di.unimi.it** : 159.149.147.136
- **bitwardentest.di.unimi.it** : 159.149.130.178
- **boccignone.di.unimi.it** : 159.149.130.139
- **bollatilab.unimi.it** : 159.149.53.246
- **borghese.di.unimi.it** : 159.149.130.139
- **broker.cloudtest.di.unimi.it** : 159.149.130.178
- **calamperetest.di.unimi.it** : 159.149.130.178
- **calamperetestapi.di.unimi.it** : 159.149.130.178
- **cas.unimi.it** : 159.149.53.217
- **cazzola.di.unimi.it** : 159.149.130.139
- **cct.islab.di.unimi.it** : 159.149.147.194
- **centenario.unimi.it** : 159.149.53.132

- **cewqo20.fisica.unimi.it** : 193.205.78.171
- **cewqo23.fisica.unimi.it** : 193.205.78.171
- **cgil.unimi.it** : 159.149.53.132
- **changes.lim.di.unimi.it** : 159.149.133.149
- **changes.unimi.it** : 159.149.133.149
- **chimica.unimi.it** : 159.149.53.164
- **chromabio.di.unimi.it** : 159.149.130.182
- **ciccio.fisica.unimi.it** : 193.205.78.171
- **cimaina2.fisica.unimi.it** : 193.205.78.171
- **cimeamilano.unimi.it** : 159.149.53.241
- **ciriani.di.unimi.it** : 159.149.130.139
- **ciss11.unimi.it** : 159.149.53.246
- **cla-slam.unimi.it** : 159.149.15.70
- **clavier2023.unimi.it** : 159.149.53.246
- **climvib.unimi.it** : 159.149.53.246
- **cloud.di.unimi.it** : 159.149.142.185
- **coding.lim.di.unimi.it** : 159.149.133.149
- **colorist.di.unimi.it** : 159.149.133.208
- **com.cdl.unimi.it** : 130.186.7.246
- **commiati.di.unimi.it** : 159.149.130.182
- **console.s3.ricerca.sesar.di.unimi.it** : 159.149.147.136
- **contrabass.fisica.unimi.it** : 193.205.78.171
- **convegnodipchi.unimi.it** : 159.149.53.241
- **cookiepolicy.di.unimi.it** : 159.149.130.182
- **cooml.di.unimi.it** : 159.149.129.213
- **corbellasummerschool.unimi.it** : 159.149.53.241
- **core.harbor.ricerca.sesar.di.unimi.it** : 159.149.147.136
- **counter.ricerca.sesar.di.unimi.it** : 159.149.147.136
- **criar.unimi.it** : 159.149.53.246
- **cross.unimi.it** : 159.149.53.132
- **crypto.club.di.unimi.it** : 159.149.147.114
- **ctf.cdl.unimi.it** : 130.186.7.246
- **culthum.unimi.it** : 159.149.53.246
- **cusmibio-prenota.unimi.it** : 159.149.53.132
- **czds.unimi.it** : 159.149.53.241
- **dairysmart.unimi.it** : 159.149.53.132

- **dantona.di.unimi.it** : 159.149.130.139
- **dapsco.unimi.it** : 159.149.53.132
- **dashboard.laser.di.unimi.it** : 159.149.145.130
- **dataloading.bapherd.ricerca.sesar.di.unimi.it** : 159.149.147.136
- **datascience.di.unimi.it** : 159.149.130.182
- **datascience.unimi.it** : 159.149.130.182
- **dataverse.unimi.it** : 18.200.39.12
- **dbs.unimi.it** : 159.149.53.164
- **dcfs2017.di.unimi.it** : 185.199.110.153
- **delletto.fisica.unimi.it** : 159.149.47.101
- **dept.unimi.it** : 159.149.53.164
- **di.unimi.it** : 159.149.53.164
- **dialects.changes.lim.di.unimi.it** : 159.149.133.149
- **dialects.changes.unimi.it** : 159.149.133.149
- **dialettialcinema.changes.unimi.it** : 159.149.133.149
- **diart.fisica.unimi.it** : 193.205.78.171
- **digit-manzoni.divsi.unimi.it** : 159.149.53.215
- **disaa-tirocini-tesi.unimi.it** : 159.149.53.241
- **discco.unimi.it** : 159.149.53.164
- **dottorato.di.unimi.it** : 159.149.130.182
- **dpm2016.di.unimi.it** : 159.149.130.139
- **dse.cdl.unimi.it** : 130.186.7.246
- **dsiutils.di.unimi.it** : 159.149.136.4
- **dsrctracker.islab.di.unimi.it** : 159.149.147.194
- **dwtest.di.unimi.it** : 159.149.130.178
- **easystaff.divsi.unimi.it** : 159.149.53.241
- **ecare.unimi.it** : 159.149.53.132
- **econ.cdl.unimi.it** : 130.186.7.246
- **eesms2009.di.unimi.it** : 159.149.130.139
- **eesms2010.di.unimi.it** : 159.149.130.139
- **elearning.unimi.it** : 159.149.15.26
- **eng.beccaria.unimi.it** : 159.149.53.164
- **eng.dbs.unimi.it** : 159.149.53.164
- **eng.dept.unimi.it** : 159.149.53.164
- **eng.discco.unimi.it** : 159.149.53.164
- **eng.esp.unimi.it** : 159.149.53.164

- **eng.matematica.unimi.it** : 159.149.53.164
- **eng.scienzegiuridiche.unimi.it** : 159.149.53.164
- **environsci.unimi.it** : 159.149.53.241
- **epaganirec.ariel.ctu.unimi.it** : 159.149.15.42
- **ercshare.unimi.it** : 159.149.53.246
- **erogatore.unimi.it** : 130.186.7.246
- **esamimoodle.unimi.it** : 159.149.15.69
- **escapes.unimi.it** : 159.149.53.132
- **esp.unimi.it** : 159.149.53.164
- **etruscologia.di.unimi.it** : 159.149.130.182
- **etruscologia.unimi.it** : 159.149.130.182
- **ext.unimi.it** : 159.149.53.246
- **farmacia.cdl.unimi.it** : 130.186.7.246
- **farmacognosia.unimi.it** : 159.149.53.246
- **fastutil.di.unimi.it** : 159.149.136.4
- **fca-namirial.unimi.it** : 159.149.53.236
- **filibusta.crema.unimi.it** : 159.149.70.151
- **fisica.unimi.it** : 159.149.53.164
- **fmpc.ariel.ctu.unimi.it** : 159.149.15.42
- **fmportal.divsi.unimi.it** : 159.149.53.247
- **frontend.serenade.ewlab.di.unimi.it** : 159.149.145.95
- **fsdattackerserver.laser.di.unimi.it** : 159.149.145.130
- **fuellab.unimi.it** : 159.149.53.246
- **gatus.ricerca.sesar.di.unimi.it** : 159.149.147.136
- **genovese.di.unimi.it** : 159.149.130.139
- **geocareers.unimi.it** : 159.149.53.241
- **germoplasma.sesar.di.unimi.it** : 159.149.130.90
- **germoplasma.unimi.it** : 159.149.130.90
- **germoplasmatest.sesar.di.unimi.it** : 159.149.130.90
- **ggobors.ariel.ctu.unimi.it** : 159.149.15.42
- **giornalismo.unimi.it** : 159.149.53.246
- **glitter.di.unimi.it** : 159.149.129.248
- **glossarioinclusione.unimi.it** : 159.149.53.132
- **gpu.di.unimi.it** : 159.149.130.139
- **grafana.cloud.di.unimi.it** : 159.149.142.185
- **grafana.ricerca.sesar.di.unimi.it** : 159.149.147.136

- **grew.di.unimi.it** : 159.149.130.182
- **h2020.fisica.unimi.it** : 159.149.47.62
- **harbor.ricerca.sesar.di.unimi.it** : 159.149.147.136
- **harmopicta.unimi.it** : 159.149.53.246
- **hdfs.ricerca.sesar.di.unimi.it** : 159.149.147.136
- **helpdesk.divsi.unimi.it** : 159.149.53.27
- **helpdesk.unimi.it** : 159.149.53.27
- **hesabu.fisica.unimi.it** : 159.149.47.56
- **hue.bapherd.ricerca.sesar.di.unimi.it** : 159.149.147.136
- **humanhall.unimi.it** : 159.149.53.132
- **ibp2025.unimi.it** : 159.149.53.132
- **icona.crc.unimi.it** : 159.149.53.246
- **iebil.di.unimi.it** : 159.149.130.139
- **ims.cdl.unimi.it** : 130.186.7.246
- **incase.di.unimi.it** : 159.149.130.182
- **incontriarea.di.unimi.it** : 159.149.130.182
- **ines.unimi.it** : 159.149.53.246
- **infermieristica.cdl.unimi.it** : 130.186.7.246
- **infocom.di.unimi.it** : 159.149.130.139
- **informastudenti.unimi.it** : 159.149.53.130
- **insdbdemo.fisica.unimi.it** : 159.149.47.225
- **instrumentaloptics.fisica.unimi.it** : 193.205.78.171
- **intranet.di.unimi.it** : 159.149.130.182
- **intranet.divsi.unimi.it** : 159.149.53.244
- **ioi.di.unimi.it** : 159.149.136.4
- **iqis2019.fisica.unimi.it** : 193.205.78.171
- **islc.unimi.it** : 159.149.53.132
- **istitutoconfucio.unimi.it** : 159.149.53.132
- **jhub.ricerca.sesar.di.unimi.it** : 159.149.147.136
- **kas.gitlab.ricerca.sesar.di.unimi.it** : 159.149.147.136
- **kb.di.unimi.it** : 159.149.130.182
- **labanof.unimi.it** : 159.149.53.241
- **laila.di.unimi.it** : 159.149.130.182
- **lam.cdl.unimi.it** : 130.186.7.246
- **lama4j.di.unimi.it** : 159.149.136.4
- **lanzarotti.di.unimi.it** : 159.149.130.139

- **laser.di.unimi.it** : 159.149.145.130
- **law.di.unimi.it** : 159.149.130.139
- **legato.lim.di.unimi.it** : 159.149.133.149
- **let.di.unimi.it** : 3.70.101.28
- **lettere.cdl.unimi.it** : 130.186.7.246
- **li2lin.ariel.ctu.unimi.it** : 159.149.15.42
- **libri.unimi.it** : 34.252.50.82
- **lifemega.unimi.it** : 159.149.53.132
- **lifesciences.unimi.it** : 159.149.53.164
- **lin.cdl.unimi.it** : 130.186.7.246
- **livinglab.di.unimi.it** : 159.149.130.182
- **llmsd.cdl.unimi.it** : 130.186.7.246
- **logbookveterinaria.unimi.it** : 159.149.53.241
- **logstest.studenti.di.unimi.it** : 159.149.130.178
- **lonati.di.unimi.it** : 159.149.130.139
- **longhorn.ricerca.sesar.di.unimi.it** : 159.149.147.136
- **lsr.di.unimi.it** : 159.149.136.4
- **luci.unimi.it** : 159.149.53.132
- **mail.laser.di.unimi.it** : 159.149.145.136
- **mailergw-db-test.di.unimi.it** : 159.149.130.178
- **mailergw-db.di.unimi.it** : 159.149.130.182
- **mailergw-test.di.unimi.it** : 159.149.130.178
- **mailergw.di.unimi.it** : 159.149.130.182
- **marchi.ricerca.di.unimi.it** : 159.149.129.213
- **marra.di.unimi.it** : 159.149.130.139
- **mass.cdl.unimi.it** : 130.186.7.246
- **masterdsebf.di.unimi.it** : 159.149.130.139
- **masterdsebf.unimi.it** : 159.149.130.139
- **matematica-lm.cdl.unimi.it** : 130.186.7.246
- **matematica.unimi.it** : 159.149.53.164
- **materia.fisica.unimi.it** : 159.149.45.149
- **mathup2425.mat.unimi.it** : 159.149.30.18
- **maven.adapt-lab.di.unimi.it** : 159.149.129.224
- **mdamiani.di.unimi.it** : 159.149.130.182
- **mediazione-k21.cdl.unimi.it** : 130.186.7.246
- **mediazione.cdl.unimi.it** : 130.186.7.246

- **mermaid.unimi.it** : 159.149.53.246
- **mg4j.di.unimi.it** : 159.149.136.4
- **mhr.cdl.unimi.it** : 130.186.7.246
- **micromesh.di.unimi.it** : 159.149.130.139
- **midimonitor.lim.di.unimi.it** : 159.149.133.149
- **minatore.divtlc.unimi.it** : 159.149.104.154
- **minerva.unimi.it** : 216.147.214.138
- **minimat.ariel.ctu.unimi.it** : 159.149.15.42
- **minio.bapherd.ricerca.sesar.di.unimi.it** : 159.149.147.136
- **minio.ricerca.sesar.di.unimi.it** : 159.149.147.136
- **mjessoulacws.ariel.ctu.unimi.it** : 159.149.15.42
- **ml4pm.di.unimi.it** : 159.149.130.139
- **ml4pm2022.di.unimi.it** : 159.149.130.139
- **ml4pm2023.di.unimi.it** : 159.149.130.139
- **mpradali.ariel.ctu.unimi.it** : 159.149.15.42
- **multimech.fisica.unimi.it** : 193.205.78.171
- **musicblockly.lim.di.unimi.it** : 159.149.133.149
- **musicstudio.lim.di.unimi.it** : 159.149.133.149
- **myariel.unimi.it** : 159.149.53.100
- **myc3place.di.unimi.it** : 159.149.130.182
- **nanoworkshop2021.fisica.unimi.it** : 193.205.78.171
- **ne.di.unimi.it** : 159.149.136.4
- **neurofisiopatologia.cdl.unimi.it** : 130.186.7.246
- **newdottorato.di.unimi.it** : 159.149.130.182
- **neworientamento.di.unimi.it** : 159.149.130.182
- **newsfeed.di.unimi.it** : 159.149.130.182
- **newsfeedapi.di.unimi.it** : 159.149.130.182
- **newsfeedtest.di.unimi.it** : 159.149.130.178
- **newsfeedtestapi.di.unimi.it** : 159.149.130.178
- **newsmail.islab.di.unimi.it** : 159.149.147.194
- **nextcloud.laser.di.unimi.it** : 159.149.145.130
- **nix-cache.ricerca.sesar.di.unimi.it** : 159.149.147.136
- **ns.unimi.it** : 159.149.10.1
- **old.agraria.unimi.it** : 159.149.53.241
- **oldweb.laser.di.unimi.it** : 159.149.145.240
- **oncolab.unimi.it** : 159.149.53.132

- **opac.unimi.it** : 159.149.53.144
- **openscience.unimi.it** : 159.149.53.132
- **oracleserver.srv.di.unimi.it** : 159.149.129.229
- **oramigis.unimi.it** : 159.149.53.241
- **orari-be.divsi.unimi.it** : 18.184.101.234
- **orientamento.di.unimi.it** : 159.149.130.182
- **orienteantico.unimi.it** : 159.149.53.132
- **osservatoriodisabilita.unimi.it** : 159.149.53.246
- **patrimonioold.di.unimi.it** : 159.149.130.182
- **pcg.di.unimi.it** : 159.149.136.4
- **phabtest.divsi.unimi.it** : 159.149.53.16
- **phanlab.unimi.it** : 159.149.53.246
- **phd.cloudtest.di.unimi.it** : 159.149.130.178
- **phd.fisica.unimi.it** : 159.149.45.149
- **phdapi.cloudtest.di.unimi.it** : 159.149.130.178
- **phddb.cloudtest.di.unimi.it** : 159.149.130.178
- **phdlog.cloudtest.di.unimi.it** : 159.149.130.178
- **phdold.di.unimi.it** : 159.149.130.178
- **phppgadmintest.studenti.di.unimi.it** : 159.149.130.178
- **piuri.di.unimi.it** : 159.149.130.139
- **play4physio.di.unimi.it** : 159.149.145.84
- **pls.fisica.unimi.it** : 193.205.78.171
- **pms.di.unimi.it** : 159.149.130.182
- **podologia.cdl.unimi.it** : 130.186.7.246
- **pong.di.unimi.it** : 159.149.130.110
- **portainer.eduvirt.di.unimi.it** : 159.149.130.187
- **portainer.laser.di.unimi.it** : 159.149.145.130
- **postlaurea.myariel.unimi.it** : 159.149.15.70
- **postlaureaonline.unimi.it** : 159.149.15.70
- **prenotabiblio.sba.unimi.it** : 35.156.221.86
- **prenotazione-new.di.unimi.it** : 159.149.130.182
- **presenze.unimi.it** : 159.149.53.34
- **prestito.cloudtest.di.unimi.it** : 159.149.130.178
- **prestitoapi.cloudtest.di.unimi.it** : 159.149.130.178
- **prestitodb.cloudtest.di.unimi.it** : 159.149.130.178
- **prigioniero.di.unimi.it** : 18.192.231.252

- **prinhealing.unimi.it** : 159.149.53.246
- **prng.di.unimi.it** : 159.149.136.4
- **prog2.di.unimi.it** : 3.70.101.28
- **progettocalvatone.unimi.it** : 159.149.53.241
- **progettopalmira.unimi.it** : 159.149.53.241
- **prometheus.cloud.di.unimi.it** : 159.149.142.185
- **promoplurilinguismo.unimi.it** : 159.149.53.132
- **pseudorandom.di.unimi.it** : 159.149.136.4
- **ptab.slam.unimi.it** : 159.149.53.241
- **pwncollege-si.laser.di.unimi.it** : 159.149.145.228
- **pwncollege.laser.di.unimi.it** : 159.149.145.162
- **qbio.cdl.unimi.it** : 130.186.7.246
- **qtech2.fisica.unimi.it** : 159.149.47.22
- **qureco.fisica.unimi.it** : 193.205.78.171
- **random.di.unimi.it** : 159.149.136.4
- **ranger.bapherd.ricerca.sesar.di.unimi.it** : 159.149.147.136
- **raton.anacleto.di.unimi.it** : 159.149.147.186
- **razzelombarde.unimi.it** : 159.149.53.132
- **reception.cloudtest.di.unimi.it** : 159.149.130.178
- **reda.unimi.it** : 159.149.53.246
- **redirect.laser.di.unimi.it** : 159.149.145.130
- **registrazione.unimi.it** : 159.149.53.221
- **registry.cloud.di.unimi.it** : 159.149.142.185
- **registry.di.unimi.it** : 159.149.130.182
- **registry.eduvirt.di.unimi.it** : 159.149.130.187
- **rel.cdl.unimi.it** : 130.186.7.246
- **ricercamix.unimi.it** : 159.149.53.132
- **ricesmart.unimi.it** : 159.149.53.246
- **riviste.unimi.it** : 34.252.50.82
- **rng.di.unimi.it** : 159.149.136.4
- **rproject.economia.unimi.it** : 159.149.53.241
- **rsu.unimi.it** : 159.149.53.132
- **rustdesk.di.unimi.it** : 159.149.130.178
- **s3.ricerca.sesar.di.unimi.it** : 159.149.147.136
- **samarati.di.unimi.it** : 159.149.130.139
- **sansone.crema.unimi.it** : 159.149.70.95

- **santini.di.unimi.it** : 3.70.101.28

- **scienzegiuridiche.unimi.it** : 159.149.53.164

- **scienzeumanistichecomunicazione.cdl.unimi.it** : 130.186.7.246

- **scuolasisa.unimi.it** : 159.149.53.132

- **sebinaopac.divsi.unimi.it** : 159.149.53.252

- **sebinaweb.divsi.unimi.it** : 159.149.53.252

- **seclab.dti.unimi.it** : 159.149.70.130

- **secregistry.cloud.di.unimi.it** : 159.149.142.185

- **securemail.unimi.it** : 159.149.10.101

- **security.di.unimi.it** : 159.149.145.130

- **servizi.di.unimi.it** : 159.149.130.182

- **sesar.di.unimi.it** : 159.149.130.182

- **shrinkai.di.unimi.it** : 159.149.136.4

- **siem.laser.di.unimi.it** : 159.149.145.130

- **sites.unimi.it** : 159.149.53.51

- **skynet.unimi.it** : 159.149.53.132

- **sliver.docenti.di.unimi.it** : 159.149.136.4

- **smartbear-it.di.unimi.it** : 159.149.130.182

- **smartbear.di.unimi.it** : 159.149.130.182

- **smartpen.aislab.di.unimi.it** : 159.149.133.61

- **smtp.unimi.it** : 159.149.10.89

- **smtpbridge.unimi.it** : 159.149.10.20

- **socialcampus.di.unimi.it** : 159.149.130.182

- **spa.cdl.unimi.it** : 130.186.7.246

- **spark.bde.ricerca.sesar.di.unimi.it** : 159.149.147.136

- **spaziofilosofico.filosofia.unimi.it** : 159.149.53.132

- **spdp.di.unimi.it** : 159.149.130.139

- **spettacolo.fisica.unimi.it** : 193.205.78.171

- **spoc.unimi.it** : 159.149.53.196

- **srv-moodle-4.ctu.unimi.it** : 159.149.15.70

- **ssrionline.unimi.it** : 159.149.15.70

- **ste.cdl.unimi.it** : 130.186.7.246

- **striptest.fisica.unimi.it** : 159.149.47.77

- **studente.divsi.unimi.it** : 159.149.53.239

- **studente.unimi.it** : 159.149.53.239

- **studenti.unimi.it** : 159.149.53.242

- **studentitest.di.unimi.it** : 159.149.130.178
- **sunfloat.unimi.it** : 159.149.53.241
- **superset.bapherd.ricerca.sesar.di.unimi.it** : 159.149.147.136
- **sux.di.unimi.it** : 159.149.136.4
- **sux4j.di.unimi.it** : 159.149.136.4
- **tales.islab.di.unimi.it** : 159.149.147.194
- **teaching.basilico.di.unimi.it** : 159.149.130.182
- **tecnocivismo.di.unimi.it** : 159.149.130.182
- **textgen.ricerca.sesar.di.unimi.it** : 159.149.147.136
- **thor.di.unimi.it** : 159.149.130.182
- **tim.ricerca.sesar.di.unimi.it** : 159.149.147.136
- **timelapse.unimi.it** : 159.149.53.246
- **tirocini.di.unimi.it** : 159.149.130.182
- **tirociniapi.di.unimi.it** : 159.149.130.182
- **tirocinitest.di.unimi.it** : 159.149.130.178
- **tirocinitestapi.di.unimi.it** : 159.149.130.178
- **tracesofmobility.unimi.it** : 78.47.83.247
- **traefik-mirco.laser.di.unimi.it** : 159.149.145.216
- **traefik.cloud.di.unimi.it** : 159.149.142.185
- **traefik.laser.di.unimi.it** : 159.149.145.130
- **traefikllama.laser.di.unimi.it** : 159.149.145.148
- **trino.bapherd.ricerca.sesar.di.unimi.it** : 159.149.147.136
- **trm.cdl.unimi.it** : 130.186.7.246
- **tutoraggio.di.unimi.it** : 159.149.129.249
- **unimia.unimi.it** : 159.149.53.172
- **unimix3.unimi.it** : 159.149.10.83
- **unistem.unimi.it** : 159.149.53.132
- **unitech.unimi.it** : 159.149.53.196
- **unsee.cloud.di.unimi.it** : 159.149.142.185
- **upload.di.unimi.it** : 159.149.130.182
- **uploadapi.di.unimi.it** : 159.149.130.182
- **uploadold.di.unimi.it** : 159.149.130.178
- **users.mat.unimi.it** : 159.149.30.3
- **vailati.unimi.it** : 159.149.53.132
- **valchiavenna.unimi.it** : 159.149.53.132
- **vaultwarden.laser.di.unimi.it** : 159.149.145.130

- **vaultwarden.ricerca.sesar.di.unimi.it** : 159.149.147.136
- **vbellandipwm.ariel.ctu.unimi.it** : 159.149.15.42
- **veterinaria.cdl.unimi.it** : 130.186.7.246
- **videoconf.unimi.it** : 159.149.106.180
- **vigna.di.unimi.it** : 159.149.136.4
- **visconti.di.unimi.it** : 159.149.130.139
- **viticolturaenologia.cdl.unimi.it** : 130.186.7.246
- **vpn.unimi.it** : 159.149.104.138
- **web.laser.di.unimi.it** : 159.149.145.130
- **webdbtest.studenti.di.unimi.it** : 159.149.130.178
- **webdbtestapi.studenti.di.unimi.it** : 159.149.130.178
- **webdev.ewlab.di.unimi.it** : 159.149.145.2
- **webgraph.di.unimi.it** : 159.149.136.4
- **webmail.laser.di.unimi.it** : 159.149.145.136
- **webradio.divsi.unimi.it** : 159.149.53.209
- **welcome.di.unimi.it** : 159.149.130.182
- **whoami.cloud.di.unimi.it** : 159.149.142.185
- **whoami.cloudstaff.di.unimi.it** : 159.149.130.182
- **wikirank-2015.di.unimi.it** : 159.149.136.4
- **wikirank-2016.di.unimi.it** : 159.149.136.4
- **wikirank-2017.di.unimi.it** : 159.149.136.4
- **wikirank-2018.di.unimi.it** : 159.149.136.4
- **wikirank-2019.di.unimi.it** : 159.149.136.4
- **wikirank-2020.di.unimi.it** : 159.149.136.4
- **wikirank-2021.di.unimi.it** : 159.149.136.4
- **wikirank-2022.di.unimi.it** : 159.149.136.4
- **wikirank-2023.di.unimi.it** : 159.149.136.4
- **wikirank-2024.di.unimi.it** : 159.149.136.4
- **wikirank.di.unimi.it** : 159.149.136.4
- **wireguard.laser.di.unimi.it** : 159.149.145.130
- **wizardunicloud.unimi.it** : 159.149.53.241
- **work.unimi.it** : 159.149.53.221
- **wp-temp.fisica.unimi.it** : 193.205.78.171
- **wp-temp2.fisica.unimi.it** : 193.205.78.171
- **xoroshiro.di.unimi.it** : 159.149.136.4
- **xorshift.di.unimi.it** : 159.149.136.4
- **xoshiro.di.unimi.it** : 159.149.136.4

8   Server Mail found

Below is the list of Mail Server found:

- 52.101.68.8
- 52.101.68.29
- 52.101.68.27
- unimi-it.mail.protection.outlook.com.
- 52.101.73.12

9 Pie Chart of Vulnerabilities

Pie chart showing the distribution of vulnerabilities for the domain `unimi.it`:
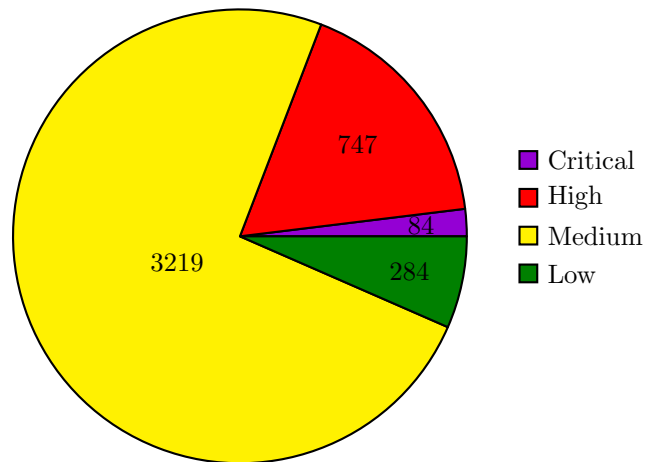
10 Vulnerability Summary per IP

The table below shows the number of critical, high, medium, and low vulnerabilities for each IP, ordered by the number of vulnerabilities (first by critical, then high, medium, and low):

IP Address	Critical	High	Medium	Low
159.149.53.209	11	103	220	10
159.149.53.16	5	31	231	21
159.149.130.110	5	30	144	9
159.149.133.208	5	26	110	7
159.149.133.149	5	24	177	18
159.149.53.224	4	28	184	16
193.205.78.171	4	27	105	6
159.149.53.172	4	26	112	6
159.149.53.221	4	26	112	6
159.149.53.140	4	22	164	16
159.149.53.215	4	22	164	16
159.149.53.27	4	14	94	12
159.149.130.178	3	8	35	2
159.149.15.22	2	66	211	23
159.149.53.164	2	16	63	5
159.149.53.217	2	13	56	3
159.149.53.191	2	11	82	8
159.149.119.18	1	13	81	7
159.149.205.26	1	11	60	5
159.149.136.4	1	7	26	4
159.149.130.139	1	7	18	5
159.149.145.2	1	4	16	1
159.149.47.69	1	4	16	1
159.149.53.242	1	1	4	0
159.149.53.244	1	1	4	0
185.221.216.115	1	0	11	2
159.149.147.136	1	0	11	2
159.149.130.182	1	0	7	0
92.42.111.202	1	0	6	1
159.149.145.130	1	0	3	0
159.149.129.213	1	0	1	0
159.149.15.69	0	25	79	7
159.149.133.61	0	22	100	8
18.200.39.12	0	22	94	8
159.149.130.90	0	20	70	6
159.149.129.249	0	19	47	6
159.149.15.70	0	13	32	4
35.185.199.199	0	13	31	4
34.252.50.82	0	12	30	4
159.149.129.248	0	12	30	4
159.149.30.3	0	11	47	4
159.149.129.224	0	6	24	4
159.149.147.114	0	6	15	2
159.149.45.8	0	6	14	4
159.149.30.18	0	6	14	4
159.149.147.194	0	4	10	0
159.149.53.100	0	3	8	1
159.149.45.32	0	3	7	2
159.149.53.132	0	2	2	0

IP Address	Critical	High	Medium	Low
159.149.53.246	0	1	1	0
159.149.15.42	0	0	12	0
159.149.47.56	0	0	7	0
159.149.15.43	0	0	4	0
159.149.47.62	0	0	4	0
159.149.53.196	0	0	2	0
159.149.47.77	0	0	2	0
159.149.53.239	0	0	2	0
159.149.145.84	0	0	2	0
159.149.53.90	0	0	1	0
18.192.231.252	0	0	0	0
159.149.145.162	0	0	0	0
159.149.147.186	0	0	0	0
159.149.47.22	0	0	0	0
159.149.53.247	0	0	0	0
159.149.106.180	0	0	0	0
88.99.2.212	0	0	0	0
159.149.53.34	0	0	0	0
159.149.53.130	0	0	0	0
50.18.215.94	0	0	0	0
52.101.73.12	0	0	0	0
104.18.11.29	0	0	0	0
159.149.145.216	0	0	0	0
159.149.10.1	0	0	0	0
50.18.142.31	0	0	0	0
104.18.10.29	0	0	0	0
159.149.129.169	0	0	0	0
52.101.68.29	0	0	0	0
159.149.129.229	0	0	0	0
159.149.145.136	0	0	0	0
78.47.83.247	0	0	0	0
2606:4700::6812:b	0	0	0	0
159.149.53.51	0	0	0	0
172.64.151.32	0	0	0	0
2606:4700::6812:a	0	0	0	0
52.101.68.27	0	0	0	0
159.149.145.148	0	0	0	0
159.149.47.225	0	0	0	0
216.147.214.138	0	0	0	0
35.156.221.86	0	0	0	0
52.59.135.101	0	0	0	0
130.186.7.246	0	0	0	0
159.149.105.179	0	0	0	0
159.149.53.252	0	0	0	0
3.126.205.183	0	0	0	0
159.149.145.228	0	0	0	0
130.186.28.54	0	0	0	0
159.149.145.95	0	0	0	0
159.149.116.206	0	0	0	0
3.70.101.28	0	0	0	0
159.149.10.20	0	0	0	0
104.18.36.224	0	0	0	0
52.101.68.8	0	0	0	0
159.149.145.164	0	0	0	0
159.149.53.241	0	0	0	0

IP Address	Critical	High	Medium	Low
159.149.145.161	0	0	0	0
159.149.53.144	0	0	0	0
159.149.133.37	0	0	0	0
185.199.110.153	0	0	0	0
159.149.104.138	0	0	0	0
159.149.116.203	0	0	0	0
18.184.101.234	0	0	0	0

Table 1: Number of vulnerabilities per IP, sorted by severity.

11 Shodan Results for IP Addresses

Below is the detailed report of vulnerabilities and services for each IP address:

11.1 IP Address: 159.149.53.209

- Organization: UNI-Milano
- Operating System: N/A
- Critical Vulnerabilities: 11
- High Vulnerabilities: 103
- Medium Vulnerabilities: 220
- Low Vulnerabilities: 10
- Total Vulnerabilities: 344

Services Running on IP Address

- Service: Apache httpd
    - Port: 80
    - Version: 2.2.15
    - Location: http://radiostatale.it/
- Service: N/A
    - Port: 10000
    - Version: N/A
    - Location:

Vulnerabilities Found

- Vulnerability: CVE-2018-10549
    - CVSS Score: 6.8
    - Description: An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. exif_read_data in ext/exif/exif.c has an out-of-bounds read for crafted JPEG data because exif_iif_add_value mishandles the case of a MakerNote that lacks a final '\{}0' character.
- Vulnerability: CVE-2018-10548
    - CVSS Score: 5
    - Description: An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. ext/ldap/ldap.c allows remote LDAP servers to cause a denial of service (NULL pointer dereference and application crash) because of mishandling of the ldap_get_dn return value.
- Vulnerability: CVE-2018-10545
    - CVSS Score: 1.9
    - Description: An issue was discovered in PHP before 5.6.35, 7.0.x before 7.0.29, 7.1.x before 7.1.16, and 7.2.x before 7.2.4. Dumpable FPM child processes allow bypassing opcache access controls because fpm_unix.c makes a PR_SET_DUMPABLE prctl call, allowing one user (in a multiuser environment) to obtain sensitive information from the process memory of a second user's PHP applications by running gcore on the PID of the PHP-FPM worker process.

- Vulnerability: CVE-2018-10547

  – CVSS Score: 4.3
  – Description: An issue was discovered in ext/phar/phar_object.c in PHP before
    5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before
    7.2.5. There is Reflected XSS on the PHAR 403 and 404 error
    pages via request data of a request for a .phar file. NOTE: this
    vulnerability exists because of an incomplete fix for CVE-2018-5712.

- Vulnerability: CVE-2018-10546

  – CVSS Score: 5
  – Description: An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30,
    7.1.x before 7.1.17, and 7.2.x before 7.2.5. An infinite loop exists
    in ext/iconv/iconv.c because the iconv stream filter does not reject
    invalid multibyte sequences.

- Vulnerability: CVE-2015-0231

  – CVSS Score: 7.5
  – Description: Use-after-free vulnerability in the process_nested_data function
    in ext/standard/var_unserializer.re in PHP before 5.4.37, 5.5.x
    before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to
    execute arbitrary code via a crafted unserialize call that leverages
    improper handling of duplicate numerical keys within the serialized
    properties of an object. NOTE: this vulnerability exists because of
    an incomplete fix for CVE-2014-8142.

- Vulnerability: CVE-2015-0232

  – CVSS Score: 6.8
  – Description: The exif_process_unicode function in ext/exif/exif.c in PHP before
    5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote
    attackers to execute arbitrary code or cause a denial of service
    (uninitialized pointer free and application crash) via crafted EXIF
    data in a JPEG image.

- Vulnerability: CVE-2019-9638

  – CVSS Score: 5
  – Description: An issue was discovered in the EXIF component in PHP before
    7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is
    an uninitialized read in exif_process_IFD_in_MAKERNOTE because of
    mishandling the maker_note->offset relationship to value_len.

- Vulnerability: CVE-2017-7679

  – CVSS Score: 7.5
  – Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime
    can read one byte past the end of a buffer when sending a malicious
    Content-Type response header.

- Vulnerability: CVE-2016-3171

  – CVSS Score: 6.8
  – Description: Drupal 6.x before 6.38, when used with PHP before 5.4.45, 5.5.x
    before 5.5.29, or 5.6.x before 5.6.13, might allow remote attackers
    to execute arbitrary code via vectors related to session data
    truncation.

- Vulnerability: CVE-2016-5773

  – CVSS Score: 7.5

- Description: php_zip.c in the zip extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and application crash) via crafted serialized data containing a ZipArchive object.

- Vulnerability: CVE-2016-5772

  - CVSS Score: 7.5
  - Description: Double free vulnerability in the php_wddx_process_data function in wddx.c in the WDDX extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via crafted XML data that is mishandled in a wddx_deserialize call.

- Vulnerability: CVE-2016-5771

  - CVSS Score: 7.5
  - Description: spl_array.c in the SPL extension in PHP before 5.5.37 and 5.6.x before 5.6.23 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and application crash) via crafted serialized data.

- Vulnerability: CVE-2016-5770

  - CVSS Score: 7.5
  - Description: Integer overflow in the SplFileObject::fread function in spl_directory.c in the SPL extension in PHP before 5.5.37 and 5.6.x before 5.6.23 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large integer argument, a related issue to CVE-2016-5096.

- Vulnerability: CVE-2018-20783

  - CVSS Score: 5
  - Description: In PHP before 5.6.39, 7.x before 7.0.33, 7.1.x before 7.1.25, and 7.2.x before 7.2.13, a buffer over-read in PHAR reading functions may allow an attacker to read allocated or unallocated memory past the actual data when trying to parse a .phar file. This is related to phar_parse_pharfile in ext/phar/phar.c.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2021-32786

  - CVSS Score: 5.8

- Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, `oidc_validate_redirect_url()` does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring `mod_auth_openidc` to only allow redirection whose destination matches a given regular expression.

- Vulnerability: CVE-2021-32785

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache (`OIDCCacheEncrypt off`, `OIDCSessionType server-cache`, `OIDCCacheType redis`), `mod_auth_openidc` wrongly performed argument interpolation before passing Redis requests to `hiredis`, which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the `hiredis` API. As a workaround, this vulnerability can be mitigated by setting `OIDCCacheEncrypt` to `on`, as cache keys are cryptographically hashed before use when this option is enabled.

- Vulnerability: CVE-2016-4070

  - CVSS Score: 5
  - Description: Integer overflow in the php_raw_url_encode function in ext/standard/url.c in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 allows remote attackers to cause a denial of service (application crash) via a long string to the rawurlencode function. NOTE: the vendor says "Not sure if this qualifies as security issue (probably not).

- Vulnerability: CVE-2017-8923

  - CVSS Score: 7.5
  - Description: The zend_string_extend function in Zend/zend_string.h in PHP through 7.1.5 does not prevent changes to string objects that result in a negative length, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact by leveraging a script's use of .= with a long string.

- Vulnerability: CVE-2010-3710

  - CVSS Score: 4.3
  - Description: Stack consumption vulnerability in the filter_var function in PHP 5.2.x through 5.2.14 and 5.3.x through 5.3.3, when FILTER_VALIDATE_EMAIL mode is used, allows remote attackers to cause a denial of service (memory consumption and application crash) via a long e-mail address string.

- Vulnerability: CVE-2014-9427

  – CVSS Score: 7.5
  – Description: sapi/cgi/cgi_main.c in the CGI component in PHP through 5.4.36, 5.5.x
    through 5.5.20, and 5.6.x through 5.6.4, when mmap is used to read
    a .php file, does not properly consider the mapping's length during
    processing of an invalid file that begins with a # character and
    lacks a newline character, which causes an out-of-bounds read and
    might (1) allow remote attackers to obtain sensitive information from
    php-cgi process memory by leveraging the ability to upload a .php
    file or (2) trigger unexpected code execution if a valid PHP script
    is present in memory locations adjacent to the mapping.

- Vulnerability: CVE-2016-6174

  – CVSS Score: 6.8
  – Description: applications/core/modules/front/system/content.php in Invision Power
    Services IPS Community Suite (aka Invision Power Board, IPB, or
    Power Board) before 4.1.13, when used with PHP before 5.4.24 or 5.5.x
    before 5.5.8, allows remote attackers to execute arbitrary code via
    the content_class parameter.

- Vulnerability: CVE-2018-5712

  – CVSS Score: 4.3
  – Description: An issue was discovered in PHP before 5.6.33, 7.0.x before 7.0.27,
    7.1.x before 7.1.13, and 7.2.x before 7.2.1. There is Reflected XSS
    on the PHAR 404 error page via the URI of a request for a .phar file.

- Vulnerability: CVE-2018-5711

  – CVSS Score: 4.3
  – Description: gd_gif_in.c in the GD Graphics Library (aka libgd), as used in PHP
    before 5.6.33, 7.0.x before 7.0.27, 7.1.x before 7.1.13, and 7.2.x
    before 7.2.1, has an integer signedness error that leads to an
    infinite loop via a crafted GIF file, as demonstrated by a call to
    the imagecreatefromgif or imagecreatefromstring PHP function. This
    is related to GetCode_ and gdImageCreateFromGifCtx.

- Vulnerability: CVE-2014-2020

  – CVSS Score: 5
  – Description: ext/gd/gd.c in PHP 5.5.x before 5.5.9 does not check data types,
    which might allow remote attackers to obtain sensitive information by
    using a (1) string or (2) array data type in place of a numeric data
    type, as demonstrated by an imagecrop function call with a string for
    the x dimension value, a different vulnerability than CVE-2013-7226.

- Vulnerability: CVE-2016-9137

  – CVSS Score: 7.5
  – Description: Use-after-free vulnerability in the CURLFile implementation in
    ext/curl/curl_file.c in PHP before 5.6.27 and 7.x before 7.0.12
    allows remote attackers to cause a denial of service or possibly
    have unspecified other impact via crafted serialized data that is
    mishandled during __wakeup processing.

- Vulnerability: CVE-2010-3436

  – CVSS Score: 5
  – Description: fopen_wrappers.c in PHP 5.3.x through 5.3.3 might allow remote
    attackers to bypass open_basedir restrictions via vectors related
    to the length of a filename.

- Vulnerability: CVE-2015-6831

    - CVSS Score: 7.5
    - Description: Multiple use-after-free vulnerabilities in SPL in PHP before 5.4.44,
                   5.5.x before 5.5.28, and 5.6.x before 5.6.12 allow remote attackers
                   to execute arbitrary code via vectors involving (1) ArrayObject, (2)
                   SplObjectStorage, and (3) SplDoublyLinkedList, which are mishandled
                   during unserialization.

- Vulnerability: CVE-2015-6832

    - CVSS Score: 7.5
    - Description: Use-after-free vulnerability in the SPL unserialize implementation
                   in ext/spl/spl_array.c in PHP before 5.4.44, 5.5.x before 5.5.28, and
                   5.6.x before 5.6.12 allows remote attackers to execute arbitrary code
                   via crafted serialized data that triggers misuse of an array field.

- Vulnerability: CVE-2015-6833

    - CVSS Score: 5
    - Description: Directory traversal vulnerability in the PharData class in PHP before
                   5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 allows remote
                   attackers to write to arbitrary files via a .. (dot dot) in a ZIP
                   archive entry that is mishandled during an extractTo call.

- Vulnerability: CVE-2015-6834

    - CVSS Score: 7.5
    - Description: Multiple use-after-free vulnerabilities in PHP before 5.4.45,
                   5.5.x before 5.5.29, and 5.6.x before 5.6.13 allow remote
                   attackers to execute arbitrary code via vectors related to (1)
                   the Serializable interface, (2) the SplObjectStorage class, and
                   (3) the SplDoublyLinkedList class, which are mishandled during
                   unserialization.

- Vulnerability: CVE-2015-6835

    - CVSS Score: 7.5
    - Description: The session deserializer in PHP before 5.4.45, 5.5.x before 5.5.29,
                   and 5.6.x before 5.6.13 mishandles multiple php_var_unserialize calls,
                   which allow remote attackers to execute arbitrary code or cause a
                   denial of service (use-after-free) via crafted session content.

- Vulnerability: CVE-2015-6836

    - CVSS Score: 7.5
    - Description: The SoapClient __call method in ext/soap/soap.c in PHP before 5.4.45,
                   5.5.x before 5.5.29, and 5.6.x before 5.6.13 does not properly manage
                   headers, which allows remote attackers to execute arbitrary code
                   via crafted serialized data that triggers a "type confusion" in the
                   serialize_function_call function.

- Vulnerability: CVE-2015-6837

    - CVSS Score: 5
    - Description: The xsl_ext_function_php function in ext/xsl/xsltprocessor.c in PHP
                   before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13, when
                   libxml2 before 2.9.2 is used, does not consider the possibility of a
                   NULL valuePop return value before proceeding with a free operation
                   during initial error checking, which allows remote attackers to
                   cause a denial of service (NULL pointer dereference and application
                   crash) via a crafted XML document, a different vulnerability than
                   CVE-2015-6838.

- Vulnerability: CVE-2015-6838
  - CVSS Score: 5
  - Description: The xsl_ext_function_php function in ext/xsl/xsltprocessor.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13, when libxml2 before 2.9.2 is used, does not consider the possibility of a NULL valuePop return value before proceeding with a free operation after the principal argument loop, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted XML document, a different vulnerability than CVE-2015-6837.
- Vulnerability: CVE-2018-19520
  - CVSS Score: 6.5
  - Description: An issue was discovered in SDCMS 1.6 with PHP 5.x. app/admin/controller/themecontroller.php uses a check_bad function in an attempt to block certain PHP functions such as eval, but does not prevent use of preg_replace 'e' calls, allowing users to execute arbitrary code by leveraging access to admin template management.
- Vulnerability: CVE-2016-7478
  - CVSS Score: 5
  - Description: Zend/zend_exceptions.c in PHP, possibly 5.x before 5.6.28 and 7.x before 7.0.13, allows remote attackers to cause a denial of service (infinite loop) via a crafted Exception object in serialized data, a related issue to CVE-2015-8876.
- Vulnerability: CVE-2017-7890
  - CVSS Score: 4.3
  - Description: The GIF decoding function gdImageCreateFromGifCtx in gd_gif_in.c in the GD Graphics Library (aka libgd), as used in PHP before 5.6.31 and 7.x before 7.1.7, does not zero colorMap arrays before use. A specially crafted GIF image could use the uninitialized tables to read ~700 bytes from the top of the stack, potentially disclosing sensitive information.
- Vulnerability: CVE-2014-0207
  - CVSS Score: 4.3
  - Description: The cdf_read_short_sector function in cdf.c in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, allows remote attackers to cause a denial of service (assertion failure and application exit) via a crafted CDF file.
- Vulnerability: CVE-2018-17082
  - CVSS Score: 4.3
  - Description: The Apache2 component in PHP before 5.6.38, 7.0.x before 7.0.32, 7.1.x before 7.1.22, and 7.2.x before 7.2.10 allows XSS via the body of a "Transfer-Encoding: chunked" request, because the bucket brigade is mishandled in the php_handler function in sapi/apache2handler/sapi_apache2.c.
- Vulnerability: CVE-2013-5704
  - CVSS Score: 5
  - Description: The mod_headers module in the Apache HTTP Server 2.2.22 allows remote attackers to bypass "RequestHeader unset" directives by placing a header in the trailer portion of data sent with chunked transfer coding. NOTE: the vendor states "this is not a security issue in httpd as such."

- Vulnerability: CVE-2016-1903

  - CVSS Score: 6.4
  - Description: The gdImageRotateInterpolated function in ext/gd/libgd/gd_interpolation.c in PHP before 5.5.31, 5.6.x before 5.6.17, and 7.x before 7.0.2 allows remote attackers to obtain sensitive information or cause a denial of service (out-of-bounds read and application crash) via a large bgd_color argument to the imagerotate function.

- Vulnerability: CVE-2013-7456

  - CVSS Score: 6.8
  - Description: gd_interpolation.c in the GD Graphics Library (aka libgd) before 2.1.1, as used in PHP before 5.5.36, 5.6.x before 5.6.22, and 7.x before 7.0.7, allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted image that is mishandled by the imagescale function.

- Vulnerability: CVE-2013-7327

  - CVSS Score: 6.8
  - Description: The gdImageCrop function in ext/gd/gd.c in PHP 5.5.x before 5.5.9 does not check return values, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via invalid imagecrop arguments that lead to use of a NULL pointer as a return value, a different vulnerability than CVE-2013-7226.

- Vulnerability: CVE-2013-1635

  - CVSS Score: 7.5
  - Description: ext/soap/soap.c in PHP before 5.3.22 and 5.4.x before 5.4.13 does not validate the relationship between the soap.wsdl_cache_dir directive and the open_basedir directive, which allows remote attackers to bypass intended access restrictions by triggering the creation of cached SOAP WSDL files in an arbitrary directory.

- Vulnerability: CVE-2017-12868

  - CVSS Score: 7.5
  - Description: The secureCompare method in lib/SimpleSAML/Utils/Crypto.php in SimpleSAMLphp 1.14.13 and earlier, when used with PHP before 5.6, allows attackers to conduct session fixation attacks or possibly bypass authentication by leveraging missing character conversions before an XOR operation.

- Vulnerability: CVE-2018-14883

  - CVSS Score: 5
  - Description: An issue was discovered in PHP before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8. An Integer Overflow leads to a heap-based buffer over-read in exif_thumbnail_extract of exif.c.

- Vulnerability: CVE-2010-1452

  - CVSS Score: 5
  - Description: The (1) mod_cache and (2) mod_dav modules in the Apache HTTP Server 2.2.x before 2.2.16 allow remote attackers to cause a denial of service (process crash) via a request that lacks a path.

- Vulnerability: CVE-2011-1153

- CVSS Score: 7.5
- Description: Multiple format string vulnerabilities in phar_object.c in the phar extension in PHP 5.3.5 and earlier allow context-dependent attackers to obtain sensitive information from process memory, cause a denial of service (memory corruption), or possibly execute arbitrary code via format string specifiers in an argument to a class method, leading to an incorrect zend_throw_exception_ex call.

- Vulnerability: CVE-2014-8142

  - CVSS Score: 7.5
  - Description: Use-after-free vulnerability in the process_nested_data function in ext/standard/var_unserializer.re in PHP before 5.4.36, 5.5.x before 5.5.20, and 5.6.x before 5.6.4 allows remote attackers to execute arbitrary code via a crafted unserialize call that leverages improper handling of duplicate keys within the serialized properties of an object, a different vulnerability than CVE-2004-1019.

- Vulnerability: CVE-2017-7963

  - CVSS Score: 5
  - Description: The GNU Multiple Precision Arithmetic Library (GMP) interfaces for PHP through 7.1.4 allow attackers to cause a denial of service (memory consumption and application crash) via operations on long strings. NOTE: the vendor disputes this, stating "There is no security issue here, because GMP safely aborts in case of an OOM condition. The only attack vector here is denial of service. However, if you allow attacker-controlled, unbounded allocations you have a DoS vector regardless of GMP's OOM behavior.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- Vulnerability: CVE-2014-3587

  - CVSS Score: 4.3
  - Description: Integer overflow in the cdf_read_property_info function in cdf.c in file through 5.19, as used in the Fileinfo component in PHP before 5.4.32 and 5.5.x before 5.5.16, allows remote attackers to cause a denial of service (application crash) via a crafted CDF file. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1571.

- Vulnerability: CVE-2015-1351

  - CVSS Score: 7.5
  - Description: Use-after-free vulnerability in the _zend_shared_memdup function in zend_shared_alloc.c in the OPcache extension in PHP through 5.6.7 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.

- Vulnerability: CVE-2015-1352

  - CVSS Score: 5
  - Description: The build_tablename function in pgsql.c in the PostgreSQL (aka pgsql) extension in PHP through 5.6.7 does not validate token extraction for table names, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted name.

- Vulnerability: CVE-2010-1623
  - CVSS Score: 5
  - Description: Memory leak in the apr_brigade_split_line function in buckets/apr_brigade.c in the Apache Portable Runtime Utility library (aka APR-util) before 1.3.10, as used in the mod_reqtimeout module in the Apache HTTP Server and other software, allows remote attackers to cause a denial of service (memory consumption) via unspecified vectors related to the destruction of an APR bucket.

- Vulnerability: CVE-2011-3368
  - CVSS Score: 5
  - Description: The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21 does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an initial @ (at sign) character.

- Vulnerability: CVE-2012-4558
  - CVSS Score: 4.3
  - Description: Multiple cross-site scripting (XSS) vulnerabilities in the balancer_handler function in the manager interface in mod_proxy_balancer.c in the mod_proxy_balancer module in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via a crafted string.

- Vulnerability: CVE-2016-10161
  - CVSS Score: 5
  - Description: The object_common1 function in ext/standard/var_unserializer.c in PHP before 5.6.30, 7.0.x before 7.0.15, and 7.1.x before 7.1.1 allows remote attackers to cause a denial of service (buffer over-read and application crash) via crafted serialized data that is mishandled in a finish_nested_data call.

- Vulnerability: CVE-2022-22721
  - CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2012-4557
  - CVSS Score: 5
  - Description: The mod_proxy_ajp module in the Apache HTTP Server 2.2.12 through 2.2.21 places a worker node into an error state upon detection of a long request-processing time, which allows remote attackers to cause a denial of service (worker consumption) via an expensive request.

- Vulnerability: CVE-2010-4697
  - CVSS Score: 6.8
  - Description: Use-after-free vulnerability in the Zend engine in PHP before 5.2.15 and 5.3.x before 5.3.4 might allow context-dependent attackers to cause a denial of service (heap memory corruption) or have unspecified other impact via vectors related to use of __set, __get, __isset, and __unset methods on objects accessed by a reference.

- Vulnerability: CVE-2017-9226

  - CVSS Score: 7.5
  - Description: An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A heap out-of-bounds write or read occurs in next_state_val() during regular expression compilation. Octal numbers larger than 0xff are not handled correctly in fetch_token() and fetch_token_in_cc(). A malformed regular expression containing an octal number in the form of '\{}700' would produce an invalid code point value larger than 0xff in next_state_val(), resulting in an out-of-bounds write memory corruption.

- Vulnerability: CVE-2010-4698

  - CVSS Score: 5
  - Description: Stack-based buffer overflow in the GD extension in PHP before 5.2.15 and 5.3.x before 5.3.4 allows context-dependent attackers to cause a denial of service (application crash) via a large number of anti-aliasing steps in an argument to the imagepstext function.

- Vulnerability: CVE-2017-9224

  - CVSS Score: 7.5
  - Description: An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A stack out-of-bounds read occurs in match_at() during regular expression searching. A logical error involving order of validation and access in match_at() could result in an out-of-bounds read from a stack buffer.

- Vulnerability: CVE-2014-3981

  - CVSS Score: 3.3
  - Description: acinclude.m4, as used in the configure script in PHP 5.5.13 and earlier, allows local users to overwrite arbitrary files via a symlink attack on the /tmp/phpglibccheck file.

- Vulnerability: CVE-2016-6288

  - CVSS Score: 7.5
  - Description: The php_url_parse_ex function in ext/standard/url.c in PHP before 5.5.38 allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via vectors involving the smart_str data type.

- Vulnerability: CVE-2016-6289

  - CVSS Score: 6.8
  - Description: Integer overflow in the virtual_file_ex function in TSRM/tsrm_virtual_cwd.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a crafted extract operation on a ZIP archive.

- Vulnerability: CVE-2014-3478

  - CVSS Score: 5
  - Description: Buffer overflow in the mconvert function in softmagic.c in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, allows remote attackers to cause a denial of service (application crash) via a crafted Pascal string in a FILE_PSTRING conversion.

- Vulnerability: CVE-2018-1301

  - CVSS Score: 4.3
  - Description: A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.

- Vulnerability: CVE-2018-1302

  - CVSS Score: 4.3
  - Description: When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.

- Vulnerability: CVE-2018-1303

  - CVSS Score: 5
  - Description: A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache. The vulnerability is considered as low risk since mod_cache_socache is not widely used, mod_cache_disk is not concerned by this vulnerability.

- Vulnerability: CVE-2013-6712

  - CVSS Score: 5
  - Description: The scan function in ext/date/lib/parse_iso_intervals.c in PHP through 5.5.6 does not properly restrict creation of DateInterval objects, which might allow remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted interval specification.

- Vulnerability: CVE-2015-6497

  - CVSS Score: 6.5
  - Description: The create function in app/code/core/Mage/Catalog/Model/Product/Api/V2.php in Magento Community Edition (CE) before 1.9.2.1 and Enterprise Edition (EE) before 1.14.2.1, when used with PHP before 5.4.24 or 5.5.8, allows remote authenticated users to execute arbitrary PHP code via the productData parameter to index.php/api/v2_soap.

- Vulnerability: CVE-2014-3670

  - CVSS Score: 6.8
  - Description: The exif_ifd_make_value function in exif.c in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the exif_thumbnail function.

- Vulnerability: CVE-2019-9641

  - CVSS Score: 7.5

- Description: An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_TIFF.

- Vulnerability: CVE-2011-4317

  - CVSS Score: 4.3
  - Description: The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an @ (at sign) character and a : (colon) character in invalid positions. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-3368.

- Vulnerability: CVE-2014-0236

  - CVSS Score: 5
  - Description: file before 5.18, as used in the Fileinfo component in PHP before 5.6.0, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a zero root_storage value in a CDF file, related to cdf.c and readcdf.c.

- Vulnerability: CVE-2014-2270

  - CVSS Score: 4.3
  - Description: softmagic.c in file before 5.17 and libmagic allows context-dependent attackers to cause a denial of service (out-of-bounds memory access and crash) via crafted offsets in the softmagic of a PE executable.

- Vulnerability: CVE-2014-4721

  - CVSS Score: 2.6
  - Description: The phpinfo implementation in ext/standard/info.c in PHP before 5.4.30 and 5.5.x before 5.5.14 does not ensure use of the string data type for the PHP_AUTH_PW, PHP_AUTH_TYPE, PHP_AUTH_USER, and PHP_SELF variables, which might allow context-dependent attackers to obtain sensitive information from process memory by using the integer data type with crafted values, related to a "type confusion" vulnerability, as demonstrated by reading a private SSL key in an Apache HTTP Server web-hosting environment with mod_ssl and a PHP 5.3.x mod_php.

- Vulnerability: CVE-2016-4537

  - CVSS Score: 7.5
  - Description: The bcpowmod function in ext/bcmath/bcmath.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 accepts a negative integer for the scale argument, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted call.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2016-4538
  - CVSS Score: 7.5
  - Description: The bcpowmod function in ext/bcmath/bcmath.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 modifies certain data structures without considering whether they are copies of the _zero_, _one_, or _two_ global variable, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted call.
- Vulnerability: CVE-2016-4539
  - CVSS Score: 7.5
  - Description: The xml_parse_into_struct function in ext/xml/xml.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 allows remote attackers to cause a denial of service (buffer under-read and segmentation fault) or possibly have unspecified other impact via crafted XML data in the second argument, leading to a parser level of zero.
- Vulnerability: CVE-2020-11579
  - CVSS Score: 5
  - Description: An issue was discovered in Chadha PHPKB 9.0 Enterprise Edition. installer/test-connection.php (part of the installation process) allows a remote unauthenticated attacker to disclose local files on hosts running PHP before 7.2.16, or on hosts where the MySQL ALLOW LOCAL DATA INFILE option is enabled.
- Vulnerability: CVE-2012-3526
  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.
- Vulnerability: CVE-2015-4644
  - CVSS Score: 5
  - Description: The php_pgsql_meta_data function in pgsql.c in the PostgreSQL (aka pgsql) extension in PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 does not validate token extraction for table names, which might allow remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted name. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-1352.
- Vulnerability: CVE-2012-2386
  - CVSS Score: 7.5
  - Description: Integer overflow in the phar_parse_tarfile function in tar.c in the phar extension in PHP before 5.3.14 and 5.4.x before 5.4.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted tar file that triggers a heap-based buffer overflow.
- Vulnerability: CVE-2015-4643
  - CVSS Score: 7.5

- Description: Integer overflow in the ftp_genlist function in ext/ftp/ftp.c in PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 allows remote FTP servers to execute arbitrary code via a long reply to a LIST command, leading to a heap-based buffer overflow. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-4022.

- Vulnerability: CVE-2015-4642

  - CVSS Score: 10

  - Description: The escapeshellarg function in ext/standard/exec.c in PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 on Windows allows remote attackers to execute arbitrary OS commands via a crafted string to an application that accepts command-line arguments for a call to the PHP system function.

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1

  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3

  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2023-45802

  - CVSS Score: N/A

  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2014-5459

  - CVSS Score: 3.6

  - Description: The PEAR_REST class in REST.php in PEAR in PHP through 5.6.0 allows local users to write to arbitrary files via a symlink attack on a (1) rest.cachefile or (2) rest.cacheid file in /tmp/pear/cache/, related to the retrieveCacheFirst and useLocalCache functions.

- Vulnerability: CVE-2010-4645

  - CVSS Score: 5

- Description: strtod.c, as used in the zend_strtod function in PHP 5.2 before 5.2.17 and 5.3 before 5.3.5, and other products, allows context-dependent attackers to cause a denial of service (infinite loop) via a certain floating-point value in scientific notation, which is not properly handled in x87 FPU registers, as demonstrated using 2.2250738585072011e-308.

- **Vulnerability:** CVE-2014-0118

  - CVSS Score: 4.3
  - Description: The deflate_in_filter function in mod_deflate.c in the mod_deflate module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.

- **Vulnerability:** CVE-2015-8874

  - CVSS Score: 5
  - Description: Stack consumption vulnerability in GD in PHP before 5.6.12 allows remote attackers to cause a denial of service via a crafted imagefilltoborder call.

- **Vulnerability:** CVE-2022-28330

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- **Vulnerability:** CVE-2009-3720

  - CVSS Score: 5
  - Description: The updatePosition function in lib/xmltok_impl.c in libexpat in Expat 2.0.1, as used in Python, PyXML, w3c-libwww, and other software, allows context-dependent attackers to cause a denial of service (application crash) via an XML document with crafted UTF-8 sequences that trigger a buffer over-read, a different vulnerability than CVE-2009-2625.

- **Vulnerability:** CVE-2012-2311

  - CVSS Score: 7.5
  - Description: sapi/cgi/cgi_main.c in PHP before 5.3.13 and 5.4.x before 5.4.3, when configured as a CGI script (aka php-cgi), does not properly handle query strings that contain a %3D sequence but no = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1823.

- **Vulnerability:** CVE-2014-2497

  - CVSS Score: 4.3
  - Description: The gdImageCreateFromXpm function in gdxpm.c in libgd, as used in PHP 5.4.26 and earlier, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted color table in an XPM file.

- **Vulnerability:** CVE-2014-0185

  - CVSS Score: 7.2

- Description: sapi/fpm/fpm/fpm_unix.c in the FastCGI Process Manager (FPM) in PHP before 5.4.28 and 5.5.x before 5.5.12 uses 0666 permissions for the UNIX socket, which allows local users to gain privileges via a crafted FastCGI client.

- Vulnerability: CVE-2016-8670

  - CVSS Score: 7.5
  - Description: Integer signedness error in the dynamicGetbuf function in gd_io_dp.c in the GD Graphics Library (aka libgd) through 2.2.3, as used in PHP before 5.6.28 and 7.x before 7.0.13, allows remote attackers to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a crafted imagecreatefromstring call.

- Vulnerability: CVE-2011-3182

  - CVSS Score: 5
  - Description: PHP before 5.3.7 does not properly check the return values of the malloc, calloc, and realloc library functions, which allows context-dependent attackers to cause a denial of service (NULL pointer dereference and application crash) or trigger a buffer overflow by leveraging the ability to provide an arbitrary value for a function argument, related to (1) ext/curl/interface.c, (2) ext/date/lib/parse_date.c, (3) ext/date/lib/parse_iso_intervals.c, (4) ext/date/lib/parse_tz.c, (5) ext/date/lib/timelib.c, (6) ext/pdo_odbc/pdo_odbc.c, (7) ext/reflection/php_reflection.c, (8) ext/soap/php_sdl.c, (9) ext/xmlrpc/libxmlrpc/base64.c, (10) TSRM/tsrm_win32.c, and (11) the strtotime function.

- Vulnerability: CVE-2006-7243

  - CVSS Score: 5
  - Description: PHP before 5.3.4 accepts the \{}0 character in a pathname, which might allow context-dependent attackers to bypass intended access restrictions by placing a safe file extension after this character, as demonstrated by .php\{}0.jpg at the end of the argument to the file_exists function.

- Vulnerability: CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2016-5766

  - CVSS Score: 6.8
  - Description: Integer overflow in the _gd2GetHeader function in gd_gd2.c in the GD Graphics Library (aka libgd) before 2.2.3, as used in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8, allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via crafted chunk dimensions in an image.

- Vulnerability: CVE-2016-5767

  - CVSS Score: 6.8
  - Description: Integer overflow in the gdImageCreate function in gd.c in the GD Graphics Library (aka libgd) before 2.0.34RC1, as used in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8, allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted image dimensions.

- Vulnerability: CVE-2016-5768

  – CVSS Score: 7.5
  – Description: Double free vulnerability in the _php_mb_regex_ereg_replace_exec function in php_mbregex.c in the mbstring extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) by leveraging a callback exception.

- Vulnerability: CVE-2016-5769

  – CVSS Score: 7.5
  – Description: Multiple integer overflows in mcrypt.c in the mcrypt extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 allow remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted length value, related to the (1) mcrypt_generic and (2) mdecrypt_generic functions.

- Vulnerability: CVE-2012-2143

  – CVSS Score: 4.3
  – Description: The crypt_des (aka DES-based crypt) function in FreeBSD before 9.0-RELEASE-p2, as used in PHP, PostgreSQL, and other products, does not process the complete cleartext password if this password contains a 0x80 character, which makes it easier for context-dependent attackers to obtain access via an authentication attempt with an initial substring of the intended password, as demonstrated by a Unicode password.

- Vulnerability: CVE-2012-1171

  – CVSS Score: 5
  – Description: The libxml RSHUTDOWN function in PHP 5.x allows remote attackers to bypass the open_basedir protection mechanism and read arbitrary files via vectors involving a stream_close method call during use of a custom stream wrapper.

- Vulnerability: CVE-2012-1172

  – CVSS Score: 5.8
  – Description: The file-upload implementation in rfc1867.c in PHP before 5.4.0 does not properly handle invalid [(open square bracket) characters in name values, which makes it easier for remote attackers to cause a denial of service (malformed $_FILES indexes) or conduct directory traversal attacks during multi-file uploads by leveraging a script that lacks its own filename restrictions.

- Vulnerability: CVE-2019-9639

  – CVSS Score: 5
  – Description: An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_MAKERNOTE because of mishandling the data_len variable.

- Vulnerability: CVE-2010-3709

  – CVSS Score: 4.3
  – Description: The ZipArchive::getArchiveComment function in PHP 5.2.x through 5.2.14 and 5.3.x through 5.3.3 allows context-dependent attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted ZIP archive.

- Vulnerability: CVE-2013-2220

  – CVSS Score: 7.5
  – Description: Buffer overflow in the radius_get_vendor_attr function in the Radius extension before 1.2.7 for PHP allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a large Vendor Specific Attributes (VSA) length value.

- Vulnerability: CVE-2019-9637

  – CVSS Score: 5
  – Description: An issue was discovered in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. Due to the way rename() across filesystems is implemented, it is possible that file being renamed is briefly available with wrong permissions while the rename is ongoing, thus enabling unauthorized users to access the data.

- Vulnerability: CVE-2012-4360

  – CVSS Score: 4.3
  – Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2018-7584

  – CVSS Score: 7.5
  – Description: In PHP through 5.6.33, 7.0.x before 7.0.28, 7.1.x through 7.1.14, and 7.2.x through 7.2.2, there is a stack-based buffer under-read while parsing an HTTP response in the php_stream_url_wrap_http_ex function in ext/standard/http_fopen_wrapper.c. This subsequently results in copying a large string.

- Vulnerability: CVE-2015-4601

  – CVSS Score: 10
  – Description: PHP before 5.6.7 might allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an unexpected data type, related to "type confusion" issues in (1) ext/soap/php_encoding.c, (2) ext/soap/php_http.c, and (3) ext/soap/soap.c, a different issue than CVE-2015-4600.

- Vulnerability: CVE-2015-4600

  – CVSS Score: 10
  – Description: The SoapClient implementation in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an unexpected data type, related to "type confusion" issues in the (1) SoapClient::__getLastRequest, (2) SoapClient::__getLastResponse, (3) SoapClient::__getLastRequestHeaders, (4) SoapClient::__getLastResponseHeaders, (5) SoapClient::__getCookies, and (6) SoapClient::__setCookie methods.

- Vulnerability: CVE-2015-4603

  – CVSS Score: 10
  – Description: The exception::getTraceAsString function in Zend/zend_exceptions.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to execute arbitrary code via an unexpected data type, related to a "type confusion" issue.

- Vulnerability: CVE-2015-4602
  - CVSS Score: 10
  - Description: The __PHP_Incomplete_Class function in ext/standard/incomplete_class.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an unexpected data type, related to a "type confusion" issue.
- Vulnerability: CVE-2015-4605
  - CVSS Score: 5
  - Description: The mcopy function in softmagic.c in file 5.x, as used in the Fileinfo component in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8, does not properly restrict a certain offset value, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted string that is mishandled by a "Python script text executable" rule.
- Vulnerability: CVE-2015-4604
  - CVSS Score: 5
  - Description: The mget function in softmagic.c in file 5.x, as used in the Fileinfo component in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8, does not properly maintain a certain pointer relationship, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted string that is mishandled by a "Python script text executable" rule.
- Vulnerability: CVE-2011-4718
  - CVSS Score: 6.8
  - Description: Session fixation vulnerability in the Sessions subsystem in PHP before 5.5.2 allows remote attackers to hijack web sessions by specifying a session ID.
- Vulnerability: CVE-2014-9912
  - CVSS Score: 7.5
  - Description: The get_icu_disp_value_src_php function in ext/intl/locale/locale_methods.c in PHP before 5.3.29, 5.4.x before 5.4.30, and 5.5.x before 5.5.14 does not properly restrict calls to the ICU uresbund.cpp component, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a locale_get_display_name call with a long first argument.
- Vulnerability: CVE-2014-0237
  - CVSS Score: 5
  - Description: The cdf_unpack_summary_info function in cdf.c in the Fileinfo component in PHP before 5.4.29 and 5.5.x before 5.5.13 allows remote attackers to cause a denial of service (performance degradation) by triggering many file_printf calls.
- Vulnerability: CVE-2016-5093
  - CVSS Score: 7.5
  - Description: The get_icu_value_internal function in ext/intl/locale/locale_methods.c in PHP before 5.5.36, 5.6.x before 5.6.22, and 7.x before 7.0.7 does not ensure the presence of a '\{}0' character, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted locale_get_primary_language call.

- Vulnerability: CVE-2016-5096
  - CVSS Score: 7.5
  - Description: Integer overflow in the fread function in ext/standard/file.c in PHP before 5.5.36 and 5.6.x before 5.6.22 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large integer in the second argument.

- Vulnerability: CVE-2011-0419
  - CVSS Score: 4.3
  - Description: Stack consumption vulnerability in the fnmatch implementation in apr_fnmatch.c in the Apache Portable Runtime (APR) library before 1.4.3 and the Apache HTTP Server before 2.2.18, and in fnmatch.c in libc in NetBSD 5.1, OpenBSD 4.8, FreeBSD, Apple Mac OS X 10.6, Oracle Solaris 10, and Android, allows context-dependent attackers to cause a denial of service (CPU and memory consumption) via *? sequences in the first argument, as demonstrated by attacks against mod_autoindex in httpd.

- Vulnerability: CVE-2014-0231
  - CVSS Score: 5
  - Description: The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.

- Vulnerability: CVE-2016-5095
  - CVSS Score: 7.5
  - Description: Integer overflow in the php_escape_html_entities_ex function in ext/standard/html.c in PHP before 5.5.36 and 5.6.x before 5.6.22 allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering a large output string from a FILTER_SANITIZE_FULL_SPECIAL_CHARS filter_var call. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-5094.

- Vulnerability: CVE-2016-4543
  - CVSS Score: 7.5
  - Description: The exif_process_IFD_in_JPEG function in ext/exif/exif.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 does not validate IFD sizes, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted header data.

- Vulnerability: CVE-2016-4542
  - CVSS Score: 7.5
  - Description: The exif_process_IFD_TAG function in ext/exif/exif.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 does not properly construct spprintf arguments, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted header data.

- Vulnerability: CVE-2016-4541
  - CVSS Score: 7.5
  - Description: The grapheme_strpos function in ext/intl/grapheme/grapheme_string.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a negative offset.

- Vulnerability: CVE-2016-4540

  - CVSS Score: 7.5
  - Description: The grapheme_stripos function in ext/intl/grapheme/grapheme_string.c
                  in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6
                  allows remote attackers to cause a denial of service (out-of-bounds
                  read) or possibly have unspecified other impact via a negative
                  offset.

- Vulnerability: CVE-2014-0238

  - CVSS Score: 5
  - Description: The cdf_read_property_info function in cdf.c in the Fileinfo component
                  in PHP before 5.4.29 and 5.5.x before 5.5.13 allows remote attackers
                  to cause a denial of service (infinite loop or out-of-bounds memory
                  access) via a vector that (1) has zero length or (2) is too long.

- Vulnerability: CVE-2016-5399

  - CVSS Score: 6.8
  - Description: The bzread function in ext/bz2/bz2.c in PHP before 5.5.38, 5.6.x
                  before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause
                  a denial of service (out-of-bounds write) or execute arbitrary code
                  via a crafted bz2 archive.

- Vulnerability: CVE-2016-3167

  - CVSS Score: 6.4
  - Description: Open redirect vulnerability in the drupal_goto function in Drupal 6.x
                  before 6.38, when used with PHP before 5.4.7, allows remote attackers
                  to redirect users to arbitrary web sites and conduct phishing attacks
                  via a double-encoded URL in the "destination" parameter.

- Vulnerability: CVE-2021-39275

  - CVSS Score: 7.5
  - Description: ap_escape_quotes() may write beyond the end of a buffer when given
                  malicious input. No included modules pass untrusted data to these
                  functions, but third-party / external modules may. This issue
                  affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2011-2483

  - CVSS Score: 5
  - Description: crypt_blowfish before 1.1, as used in PHP before 5.3.7 on certain
                  platforms, PostgreSQL before 8.4.9, and other products, does
                  not properly handle 8-bit characters, which makes it easier for
                  context-dependent attackers to determine a cleartext password by
                  leveraging knowledge of a password hash.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server
                  allows remote attackers to cause a denial of service (NULL pointer
                  dereference, process crash, and disk consumption) via a POST request
                  with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2013-4635

  - CVSS Score: 5

– Description: Integer overflow in the SdnToJewish function in jewish.c in the Calendar component in PHP before 5.3.26 and 5.4.x before 5.4.16 allows context-dependent attackers to cause a denial of service (application hang) via a large argument to the jdtojewish function.

- Vulnerability: CVE-2015-4116

  – CVSS Score: 7.5
  – Description: Use-after-free vulnerability in the spl_ptr_heap_insert function in ext/spl/spl_heap.c in PHP before 5.5.27 and 5.6.x before 5.6.11 allows remote attackers to execute arbitrary code by triggering a failed SplMinHeap::compare operation.

- Vulnerability: CVE-2015-8865

  – CVSS Score: 7.5
  – Description: The file_check_mem function in funcs.c in file before 5.23, as used in the Fileinfo component in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5, mishandles continuation-level jumps, which allows context-dependent attackers to cause a denial of service (buffer overflow and application crash) or possibly execute arbitrary code via a crafted magic file.

- Vulnerability: CVE-2014-9705

  – CVSS Score: 7.5
  – Description: Heap-based buffer overflow in the enchant_broker_request_dict function in ext/enchant/enchant.c in PHP before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6 allows remote attackers to execute arbitrary code via vectors that trigger creation of multiple dictionaries.

- Vulnerability: CVE-2016-10712

  – CVSS Score: 5
  – Description: In PHP before 5.5.32, 5.6.x before 5.6.18, and 7.x before 7.0.3, all of the return values of stream_get_meta_data can be controlled if the input can be controlled (e.g., during file uploads). For example, a "$uri = stream_get_meta_data(fopen($file, "r"))['uri']" call mishandles the case where $file is data:text/plain;uri=eviluri, -- in other words, metadata can be set by an attacker.

- Vulnerability: CVE-2015-5589

  – CVSS Score: 10
  – Description: The phar_convert_to_other function in ext/phar/phar_object.c in PHP before 5.4.43, 5.5.x before 5.5.27, and 5.6.x before 5.6.11 does not validate a file pointer before a close operation, which allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via a crafted TAR archive that is mishandled in a Phar::convertToData call.

- Vulnerability: CVE-2011-1148

  – CVSS Score: 7.5
  – Description: Use-after-free vulnerability in the substr_replace function in PHP 5.3.6 and earlier allows context-dependent attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact by using the same variable for multiple arguments.

- Vulnerability: CVE-2015-4599

  – CVSS Score: 10

– Description: The SoapFault::__toString method in ext/soap/soap.c in PHP before
5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote
attackers to obtain sensitive information, cause a denial of service
(application crash), or possibly execute arbitrary code via an
unexpected data type, related to a "type confusion" issue.

• Vulnerability: CVE-2011-0708

  – CVSS Score: 4.3
  – Description: exif.c in the Exif extension in PHP before 5.3.6 on 64-bit platforms
performs an incorrect cast, which allows remote attackers to cause
a denial of service (application crash) via an image with a crafted
Image File Directory (IFD) that triggers a buffer over-read.

• Vulnerability: CVE-2015-4598

  – CVSS Score: 7.5
  – Description: PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10
does not ensure that pathnames lack %00 sequences, which might
allow remote attackers to read or write to arbitrary files via
crafted input to an application that calls (1) a DOMDocument save
method or (2) the GD imagepsloadfont function, as demonstrated by a
filename\{}0.html attack that bypasses an intended configuration in
which client users may write to only .html files.

• Vulnerability: CVE-2016-7132

  – CVSS Score: 5
  – Description: ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows
remote attackers to cause a denial of service (NULL pointer
dereference and application crash) or possibly have unspecified other
impact via an invalid wddxPacket XML document that is mishandled in
a wddx_deserialize call, as demonstrated by a stray element inside a
boolean element, leading to incorrect pop processing.

• Vulnerability: CVE-2016-7131

  – CVSS Score: 5
  – Description: ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows
remote attackers to cause a denial of service (NULL pointer
dereference and application crash) or possibly have unspecified other
impact via a malformed wddxPacket XML document that is mishandled
in a wddx_deserialize call, as demonstrated by a tag that lacks a <
(less than) character.

• Vulnerability: CVE-2016-7130

  – CVSS Score: 5
  – Description: The php_wddx_pop_element function in ext/wddx/wddx.c in PHP before
5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a
denial of service (NULL pointer dereference and application crash) or
possibly have unspecified other impact via an invalid base64 binary
value, as demonstrated by a wddx_deserialize call that mishandles a
binary element in a wddxPacket XML document.

• Vulnerability: CVE-2013-6438

  – CVSS Score: 5
  – Description: The dav_xml_get_cdata function in main/util.c in the mod_dav module
in the Apache HTTP Server before 2.4.8 does not properly remove
whitespace characters from CDATA sections, which allows remote
attackers to cause a denial of service (daemon crash) via a crafted
DAV WRITE request.

- Vulnerability: CVE-2015-4021

  – CVSS Score: 5
  – Description: The phar_parse_tarfile function in ext/phar/tar.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 does not verify that the first character of a filename is different from the \{}0 character, which allows remote attackers to cause a denial of service (integer underflow and memory corruption) via a crafted entry in a tar archive.

- Vulnerability: CVE-2015-4022

  – CVSS Score: 7.5
  – Description: Integer overflow in the ftp_genlist function in ext/ftp/ftp.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 allows remote FTP servers to execute arbitrary code via a long reply to a LIST command, leading to a heap-based buffer overflow.

- Vulnerability: CVE-2015-4025

  – CVSS Score: 7.5
  – Description: PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 truncates a pathname upon encountering a \{}x00 character in certain situations, which allows remote attackers to bypass intended extension restrictions and access files or directories with unexpected names via a crafted argument to (1) set_include_path, (2) tempnam, (3) rmdir, or (4) readlink. NOTE: this vulnerability exists because of an incomplete fix for CVE-2006-7243.

- Vulnerability: CVE-2015-4024

  – CVSS Score: 5
  – Description: Algorithmic complexity vulnerability in the multipart_buffer_headers function in main/rfc1867.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 allows remote attackers to cause a denial of service (CPU consumption) via crafted form data that triggers an improper order-of-growth outcome.

- Vulnerability: CVE-2015-4026

  – CVSS Score: 7.5
  – Description: The pcntl_exec implementation in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 truncates a pathname upon encountering a \{}x00 character, which might allow remote attackers to bypass intended extension restrictions and execute files with unexpected names via a crafted first argument. NOTE: this vulnerability exists because of an incomplete fix for CVE-2006-7243.

- Vulnerability: CVE-2016-10158

  – CVSS Score: 5
  – Description: The exif_convert_any_to_int function in ext/exif/exif.c in PHP before 5.6.30, 7.0.x before 7.0.15, and 7.1.x before 7.1.1 allows remote attackers to cause a denial of service (application crash) via crafted EXIF data that triggers an attempt to divide the minimum representable negative integer by -1.

- Vulnerability: CVE-2016-10159

  – CVSS Score: 5

- Description: Integer overflow in the phar_parse_pharfile function in ext/phar/phar.c in PHP before 5.6.30 and 7.0.x before 7.0.15 allows remote attackers to cause a denial of service (memory consumption or application crash) via a truncated manifest entry in a PHAR archive.

- Vulnerability: CVE-2016-8743

  - CVSS Score: 5
  - Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

- Vulnerability: CVE-2012-3365

  - CVSS Score: 5
  - Description: The SQLite functionality in PHP before 5.3.15 allows remote attackers to bypass the open_basedir protection mechanism via unspecified vectors.

- Vulnerability: CVE-2017-9067

  - CVSS Score: 4.4
  - Description: In MODX Revolution before 2.5.7, when PHP 5.3.3 is used, an attacker is able to include and execute arbitrary files on the web server due to insufficient validation of the action parameter to setup/index.php, aka directory traversal.

- Vulnerability: CVE-2014-3487

  - CVSS Score: 4.3
  - Description: The cdf_read_property_info function in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, does not properly validate a stream offset, which allows remote attackers to cause a denial of service (application crash) via a crafted CDF file.

- Vulnerability: CVE-2014-3480

  - CVSS Score: 4.3
  - Description: The cdf_count_chain function in cdf.c in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, does not properly validate sector-count data, which allows remote attackers to cause a denial of service (application crash) via a crafted CDF file.

- Vulnerability: CVE-2015-3329

  - CVSS Score: 7.5
  - Description: Multiple stack-based buffer overflows in the phar_set_inode function in phar_internal.h in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allow remote attackers to execute arbitrary code via a crafted length value in a (1) tar, (2) phar, or (3) ZIP archive.

- Vulnerability: CVE-2013-2110

  - CVSS Score: 5

      – Description: Heap-based buffer overflow in the php_quot_print_encode function in
                 ext/standard/quot_print.c in PHP before 5.3.26 and 5.4.x before
                 5.4.16 allows remote attackers to cause a denial of service
                 (application crash) or possibly have unspecified other impact via
                 a crafted argument to the quoted_printable_encode function.

- Vulnerability: CVE-2012-0031

  – CVSS Score: 4.6
  – Description: scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might
             allow local users to cause a denial of service (daemon crash during
             shutdown) or possibly have unspecified other impact by modifying a
             certain type field within a scoreboard shared memory segment, leading
             to an invalid call to the free function.

- Vulnerability: CVE-2017-9788

  – CVSS Score: 6.4
  – Description: In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value
             placeholder in [Proxy-]Authorization headers of type 'Digest' was
             not initialized or reset before or between successive key=value
             assignments by mod_auth_digest. Providing an initial key with no
             '=' assignment could reflect the stale value of uninitialized pool
             memory used by the prior request, leading to leakage of potentially
             confidential information, and a segfault in other cases resulting in
             denial of service.

- Vulnerability: CVE-2014-4049

  – CVSS Score: 5.1
  – Description: Heap-based buffer overflow in the php_parserr function in
             ext/standard/dns.c in PHP 5.6.0beta4 and earlier allows remote
             servers to cause a denial of service (crash) and possibly execute
             arbitrary code via a crafted DNS TXT record, related to the
             dns_get_record function.

- Vulnerability: CVE-2017-11142

  – CVSS Score: 7.8
  – Description: In PHP before 5.6.31, 7.x before 7.0.17, and 7.1.x before
             7.1.3, remote attackers could cause a CPU consumption denial
             of service attack by injecting long form variables, related to
             main/php_variables.c.

- Vulnerability: CVE-2016-9933

  – CVSS Score: 5
  – Description: Stack consumption vulnerability in the gdImageFillToBorder function
             in gd.c in the GD Graphics Library (aka libgd) before 2.2.2, as used
             in PHP before 5.6.28 and 7.x before 7.0.13, allows remote attackers
             to cause a denial of service (segmentation violation) via a crafted
             imagefilltoborder call that triggers use of a negative color value.

- Vulnerability: CVE-2011-1471

  – CVSS Score: 4.3
  – Description: Integer signedness error in zip_stream.c in the Zip extension in PHP
             before 5.3.6 allows context-dependent attackers to cause a denial of
             service (CPU consumption) via a malformed archive file that triggers
             errors in zip_fread function calls.

- Vulnerability: CVE-2011-1470

- CVSS Score: 4.3
- Description: The Zip extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via a ziparchive stream that is not properly handled by the stream_get_contents function.

- Vulnerability: CVE-2022-28615

  - CVSS Score: 6.4
  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- Vulnerability: CVE-2022-28614

  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

- Vulnerability: CVE-2017-7272

  - CVSS Score: 5.8
  - Description: PHP through 7.1.11 enables potential SSRF in applications that accept an fsockopen or pfsockopen hostname argument with an expectation that the port number is constrained. Because a :port syntax is recognized, fsockopen will use the port number that is specified in the hostname argument, instead of the port number in the second argument of the function.

- Vulnerability: CVE-2024-4577

  - CVSS Score: N/A
  - Description: In PHP versions8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in command line given toWin32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc.

- Vulnerability: CVE-2011-2202

  - CVSS Score: 6.4
  - Description: The rfc1867_post_handler function in main/rfc1867.c in PHP before 5.3.7 does not properly restrict filenames in multipart/form-data POST requests, which allows remote attackers to conduct absolute path traversal attacks, and possibly create or overwrite arbitrary files, via a crafted upload request, related to a "file path injection vulnerability."

- Vulnerability: CVE-2016-7418

  - CVSS Score: 5

– Description: The php_wddx_push_element function in ext/wddx/wddx.c in PHP before
    5.6.26 and 7.x before 7.0.11 allows remote attackers to cause a
    denial of service (invalid pointer access and out-of-bounds read)
    or possibly have unspecified other impact via an incorrect boolean
    element in a wddxPacket XML document, leading to mishandling in a
    wddx_deserialize call.

- Vulnerability: CVE-2016-7414

  – CVSS Score: 7.5
  – Description: The ZIP signature-verification feature in PHP before 5.6.26 and 7.x
    before 7.0.11 does not ensure that the uncompressed_filesize field
    is large enough, which allows remote attackers to cause a denial of
    service (out-of-bounds memory access) or possibly have unspecified
    other impact via a crafted PHAR archive, related to ext/phar/util.c
    and ext/phar/zip.c.

- Vulnerability: CVE-2016-7416

  – CVSS Score: 5
  – Description: ext/intl/msgformat/msgformat_format.c in PHP before 5.6.26 and 7.x
    before 7.0.11 does not properly restrict the locale length provided
    to the Locale class in the ICU library, which allows remote attackers
    to cause a denial of service (application crash) or possibly have
    unspecified other impact via a MessageFormatter::formatMessage call
    with a long first argument.

- Vulnerability: CVE-2016-7417

  – CVSS Score: 7.5
  – Description: ext/spl/spl_array.c in PHP before 5.6.26 and 7.x before 7.0.11
    proceeds with SplArray unserialization without validating a return
    value and data type, which allows remote attackers to cause a denial
    of service or possibly have unspecified other impact via crafted
    serialized data.

- Vulnerability: CVE-2016-7411

  – CVSS Score: 7.5
  – Description: ext/standard/var_unserializer.re in PHP before 5.6.26 mishandles
    object-deserialization failures, which allows remote attackers
    to cause a denial of service (memory corruption) or possibly have
    unspecified other impact via an unserialize call that references a
    partially constructed object.

- Vulnerability: CVE-2016-7412

  – CVSS Score: 6.8
  – Description: ext/mysqlnd/mysqlnd_wireprotocol.c in PHP before 5.6.26 and 7.x
    before 7.0.11 does not verify that a BIT field has the UNSIGNED_FLAG
    flag, which allows remote MySQL servers to cause a denial of service
    (heap-based buffer overflow) or possibly have unspecified other
    impact via crafted field metadata.

- Vulnerability: CVE-2016-7413

  – CVSS Score: 7.5
  – Description: Use-after-free vulnerability in the wddx_stack_destroy function in
    ext/wddx/wddx.c in PHP before 5.6.26 and 7.x before 7.0.11 allows
    remote attackers to cause a denial of service or possibly have
    unspecified other impact via a wddxPacket XML document that lacks
    an end-tag for a recordset field element, leading to mishandling in a
    wddx_deserialize call.

- Vulnerability: CVE-2011-0421

  – CVSS Score: 4.3
  – Description: The _zip_name_locate function in zip_name_locate.c in the
                   Zip extension in PHP before 5.3.6 does not properly handle
                   a ZIPARCHIVE::FL_UNCHANGED argument, which might allow
                   context-dependent attackers to cause a denial of service (NULL
                   pointer dereference) via an empty ZIP archive that is processed with
                   a (1) locateName or (2) statName operation.

- Vulnerability: CVE-2012-2688

  – CVSS Score: 10
  – Description: Unspecified vulnerability in the _php_stream_scandir function in the
                   stream implementation in PHP before 5.3.15 and 5.4.x before 5.4.5 has
                   unknown impact and remote attack vectors, related to an "overflow."

- Vulnerability: CVE-2010-4700

  – CVSS Score: 6.8
  – Description: The set_magic_quotes_runtime function in PHP 5.3.2 and 5.3.3, when
                   the MySQLi extension is used, does not properly interact with use
                   of the mysqli_fetch_assoc function, which might make it easier for
                   context-dependent attackers to conduct SQL injection attacks via
                   crafted input that had been properly handled in earlier PHP versions.

- Vulnerability: CVE-2012-2687

  – CVSS Score: 2.6
  – Description: Multiple cross-site scripting (XSS) vulnerabilities in the
                   make_variant_list function in mod_negotiation.c in the mod_negotiation
                   module in the Apache HTTP Server 2.4.x before 2.4.3, when the
                   MultiViews option is enabled, allow remote attackers to inject
                   arbitrary web script or HTML via a crafted filename that is not
                   properly handled during construction of a variant list.

- Vulnerability: CVE-2015-8994

  – CVSS Score: 6.8
  – Description: An issue was discovered in PHP 5.x and 7.x, when the configuration
                   uses apache2handler/mod_php or php-fpm with OpCache enabled. With
                   5.x after 5.6.28 or 7.x after 7.0.13, the issue is resolved in a
                   non-default configuration with the opcache.validate_permission=1
                   setting. The vulnerability details are as follows. In PHP SAPIs
                   where PHP interpreters share a common parent process, Zend OpCache
                   creates a shared memory object owned by the common parent during
                   initialization. Child PHP processes inherit the SHM descriptor,
                   using it to cache and retrieve compiled script bytecode ("opcode"
                   in PHP jargon). Cache keys vary depending on configuration,
                   but filename is a central key component, and compiled opcode can
                   generally be run if a script's filename is known or can be guessed.
                   Many common shared-hosting configurations change EUID in child
                   processes to enforce privilege separation among hosted users (for
                   example using mod_ruid2 for the Apache HTTP Server, or php-fpm user
                   settings). In these scenarios, the default Zend OpCache behavior
                   defeats script file permissions by sharing a single SHM cache
                   among all child PHP processes. PHP scripts often contain sensitive
                   information: Think of CMS configurations where reading or running
                   another user's script usually means gaining privileges to the CMS
                   database.

- Vulnerability: CVE-2011-3336

- CVSS Score: 7.8
- Description: regcomp in the BSD implementation of libc is vulnerable to denial of
  service due to stack exhaustion.

- Vulnerability: CVE-2015-2348

  - CVSS Score: 5
  - Description: The move_uploaded_file implementation in ext/standard/basic_functions.c
    in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7
    truncates a pathname upon encountering a \{}x00 character, which
    allows remote attackers to bypass intended extension restrictions
    and create files with unexpected names via a crafted second argument.
    NOTE: this vulnerability exists because of an incomplete fix for
    CVE-2006-7243.

- Vulnerability: CVE-2015-8838

  - CVSS Score: 4.3
  - Description: ext/mysqlnd/mysqlnd.c in PHP before 5.4.43, 5.5.x before 5.5.27,
    and 5.6.x before 5.6.11 uses a client SSL option to mean that SSL is
    optional, which allows man-in-the-middle attackers to spoof servers
    via a cleartext-downgrade attack, a related issue to CVE-2015-3152.

- Vulnerability: CVE-2015-8835

  - CVSS Score: 7.5
  - Description: The make_http_soap_request function in ext/soap/php_http.c in PHP
    before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 does
    not properly retrieve keys, which allows remote attackers to cause
    a denial of service (NULL pointer dereference, type confusion, and
    application crash) or possibly execute arbitrary code via crafted
    serialized data representing a numerically indexed _cookies array,
    related to the SoapClient::__call method in ext/soap/soap.c.

- Vulnerability: CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel
    4.3.4a, when the Apache HTTP Server is used, allows remote attackers
    to bypass authentication via directory traversal sequences in a URI
    that ends with the name of a publicly available page, as demonstrated
    by a "/...../" sequence and an account_manage.php/login.php final
    component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2012-1823

  - CVSS Score: 7.5
  - Description: sapi/cgi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when
    configured as a CGI script (aka php-cgi), does not properly handle
    query strings that lack an = (equals sign) character, which allows
    remote attackers to execute arbitrary code by placing command-line
    options in the query string, related to lack of skipping a certain
    php_getopt for the 'd' case.

- Vulnerability: CVE-2016-4975

  - CVSS Score: 4.3
  - Description: Possible CRLF injection allowing HTTP response splitting attacks for
    sites which use mod_userdir. This issue was mitigated by changes
    made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the
    "Location" or other outbound header key or value. Fixed in Apache
    HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP
    Server 2.2.32 (Affected 2.2.0-2.2.31).

- Vulnerability: CVE-2013-1824

  - CVSS Score: 4.3
  - Description: The SOAP parser in PHP before 5.3.22 and 5.4.x before 5.4.12 allows remote attackers to read arbitrary files via a SOAP WSDL file containing an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue in the soap_xmlParseFile and soap_xmlParseMemory functions.

- Vulnerability: CVE-2013-6420

  - CVSS Score: 7.5
  - Description: The asn1_time_to_time_t function in ext/openssl/openssl.c in PHP before 5.3.28, 5.4.x before 5.4.23, and 5.5.x before 5.5.7 does not properly parse (1) notBefore and (2) notAfter timestamps in X.509 certificates, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted certificate that is not properly handled by the openssl_x509_parse function.

- Vulnerability: CVE-2022-31628

  - CVSS Score: N/A
  - Description: In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the phar uncompressor code would recursively uncompress "quines" gzip files, resulting in an infinite loop.

- Vulnerability: CVE-2022-31629

  - CVSS Score: N/A
  - Description: In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the vulnerability enables network and same-site attackers to set a standard insecure cookie in the victim's browser which is treated as a '__Host-' or '__Secure-' cookie by PHP applications.

- Vulnerability: CVE-2015-2783

  - CVSS Score: 5.8
  - Description: ext/phar/phar.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to obtain sensitive information from process memory or cause a denial of service (buffer over-read and application crash) via a crafted length value in conjunction with crafted serialized data in a phar archive, related to the phar_parse_metadata and phar_parse_pharfile functions.

- Vulnerability: CVE-2015-2787

  - CVSS Score: 7.5
  - Description: Use-after-free vulnerability in the process_nested_data function in ext/standard/var_unserializer.re in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 allows remote attackers to execute arbitrary code via a crafted unserialize call that leverages use of the unset function within an __wakeup function, a related issue to CVE-2015-0231.

- Vulnerability: CVE-2011-3348

  - CVSS Score: 4.3
  - Description: The mod_proxy_ajp module in the Apache HTTP Server before 2.2.21, when used with mod_proxy_balancer in certain configurations, allows remote attackers to cause a denial of service (temporary "error state" in the backend server) via a malformed HTTP request.

- Vulnerability: CVE-2015-3411

  – CVSS Score: 6.4
  – Description: PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 does not ensure that pathnames lack %00 sequences, which might allow remote attackers to read or write to arbitrary files via crafted input to an application that calls (1) a DOMDocument load method, (2) the xmlwriter_open_uri function, (3) the finfo_file function, or (4) the hash_hmac_file function, as demonstrated by a filename\{}0.xml attack that bypasses an intended configuration in which client users may read only .xml files.

- Vulnerability: CVE-2016-9934

  – CVSS Score: 5
  – Description: ext/wddx/wddx.c in PHP before 5.6.28 and 7.x before 7.0.13 allows remote attackers to cause a denial of service (NULL pointer dereference) via crafted serialized data in a wddxPacket XML document, as demonstrated by a PDORow string.

- Vulnerability: CVE-2017-11143

  – CVSS Score: 5
  – Description: In PHP before 5.6.31, an invalid free in the WDDX deserialization of boolean parameters could be used by attackers able to inject XML for deserialization to crash the PHP interpreter, related to an invalid free for an empty boolean element in ext/wddx/wddx.c.

- Vulnerability: CVE-2015-3412

  – CVSS Score: 5
  – Description: PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 does not ensure that pathnames lack %00 sequences, which might allow remote attackers to read arbitrary files via crafted input to an application that calls the stream_resolve_include_path function in ext/standard/streamsfuncs.c, as demonstrated by a filename\{}0.extension attack that bypasses an intended configuration in which client users may read files with only one specific extension.

- Vulnerability: CVE-2017-11145

  – CVSS Score: 5
  – Description: In PHP before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7, an error in the date extension's timelib_meridian parsing code could be used by attackers able to supply date strings to leak information from the interpreter, related to ext/date/lib/parse_date.c out-of-bounds reads affecting the php_parse_date function. NOTE: the correct fix is in the e8b7698f5ee757ce2c8bd10a192a491a498f891c commit, not the bd77ac90d3bdf31ce2a5251ad92e9e75 gist.

- Vulnerability: CVE-2017-11144

  – CVSS Score: 5
  – Description: In PHP before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7, the openssl extension PEM sealing code did not check the return value of the OpenSSL sealing function, which could lead to a crash of the PHP interpreter, related to an interpretation conflict for a negative number in ext/openssl/openssl.c, and an OpenSSL documentation omission.

- Vulnerability: CVE-2017-11147

- CVSS Score: 6.4
- Description: In PHP before 5.6.30 and 7.x before 7.0.15, the PHAR archive handler could be used by attackers supplying malicious archive files to crash the PHP interpreter or potentially disclose information due to a buffer over-read in the phar_parse_pharfile function in ext/phar/phar.c.

- Vulnerability: CVE-2011-4415

  - CVSS Score: 1.2
  - Description: The ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, does not restrict the size of values of environment variables, which allows local users to cause a denial of service (memory consumption or NULL pointer dereference) via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, related to (1) the "len +=" statement and (2) the apr_pcalloc function call, a different vulnerability than CVE-2011-3607.

- Vulnerability: CVE-2011-1938

  - CVSS Score: 7.5
  - Description: Stack-based buffer overflow in the socket_connect function in ext/sockets/sockets.c in PHP 5.3.3 through 5.3.6 might allow context-dependent attackers to execute arbitrary code via a long pathname for a UNIX socket.

- Vulnerability: CVE-2011-1939

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in Zend Framework 1.10.x before 1.10.9 and 1.11.x before 1.11.6 when using non-ASCII-compatible encodings in conjunction PDO_MySql in PHP before 5.3.6.

- Vulnerability: CVE-2011-1398

  - CVSS Score: 4.3
  - Description: The sapi_header_op function in main/SAPI.c in PHP before 5.3.11 and 5.4.x before 5.4.0RC2 does not check for %0D sequences (aka carriage return characters), which allows remote attackers to bypass an HTTP response-splitting protection mechanism via a crafted URL, related to improper interaction between the PHP header function and certain browsers, as demonstrated by Internet Explorer and Google Chrome.

- Vulnerability: CVE-2014-4670

  - CVSS Score: 4.6
  - Description: Use-after-free vulnerability in ext/spl/spl_dllist.c in the SPL component in PHP through 5.5.14 allows context-dependent attackers to cause a denial of service or possibly have unspecified other impact via crafted iterator usage within applications in certain web-hosting environments.

- Vulnerability: CVE-2014-3515

  - CVSS Score: 7.5
  - Description: The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.

- Vulnerability: CVE-2011-3192

  – CVSS Score: 7.8
  – Description: The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.

- Vulnerability: CVE-2009-3560

  – CVSS Score: 5
  – Description: The big2_toUtf8 function in lib/xmltok.c in libexpat in Expat 2.0.1, as used in the XML-Twig module for Perl, allows context-dependent attackers to cause a denial of service (application crash) via an XML document with malformed UTF-8 sequences that trigger a buffer over-read, related to the doProlog function in lib/xmlparse.c, a different vulnerability than CVE-2009-2625 and CVE-2009-3720.

- Vulnerability: CVE-2022-29404

  – CVSS Score: 5
  – Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2016-3185

  – CVSS Score: 6.4
  – Description: The make_http_soap_request function in ext/soap/php_http.c in PHP before 5.4.44, 5.5.x before 5.5.28, 5.6.x before 5.6.12, and 7.x before 7.0.4 allows remote attackers to obtain sensitive information from process memory or cause a denial of service (type confusion and application crash) via crafted serialized _cookies data, related to the SoapClient::__call method in ext/soap/soap.c.

- Vulnerability: CVE-2007-3205

  – CVSS Score: 5
  – Description: The parse_str function in (1) PHP, (2) Hardened-PHP, and (3) Suhosin, when called without a second parameter, might allow remote attackers to overwrite arbitrary variables by specifying variable names and values in the string to be parsed. NOTE: it is not clear whether this is a design limitation of the function or a bug in PHP, although it is likely to be regarded as a bug in Hardened-PHP and Suhosin.

- Vulnerability: CVE-2011-3607

  – CVSS Score: 4.4
  – Description: Integer overflow in the ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, allows local users to gain privileges via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, leading to a heap-based buffer overflow.

- Vulnerability: CVE-2014-0226

  – CVSS Score: 6.8

- Description: Race condition in the mod_status module in the Apache HTTP Server
  before 2.4.10 allows remote attackers to cause a denial of
  service (heap-based buffer overflow), or possibly obtain sensitive
  credential information or execute arbitrary code, via a crafted
  request that triggers improper scoreboard handling within the
  status_handler function in modules/generators/mod_status.c and the
  lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

- Vulnerability: CVE-2006-20001

  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or
    write of a single zero byte, in a pool (heap) memory location beyond
    the header value sent. This could cause the process to crash.This
    issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2015-9253

  - CVSS Score: 6.8
  - Description: An issue was discovered in PHP 7.3.x before 7.3.0alpha3, 7.2.x before
    7.2.8, and before 7.1.20. The php-fpm master process restarts
    a child process in an endless loop when using program execution
    functions (e.g., passthru, exec, shell_exec, or system) with a
    non-blocking STDIN stream, causing this master process to consume
    100% of the CPU, and consume disk space with a large volume of error
    logs, as demonstrated by an attack by a customer of a shared-hosting
    facility.

- Vulnerability: CVE-2016-5387

  - CVSS Score: 6.8
  - Description: The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18
    and therefore does not protect applications from the presence of
    untrusted client data in the HTTP_PROXY environment variable, which
    might allow remote attackers to redirect an application's outbound
    HTTP traffic to an arbitrary proxy server via a crafted Proxy header
    in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states
    "This mitigation has been assigned the identifier CVE-2016-5387"; in
    other words, this is not a CVE ID for a vulnerability.

- Vulnerability: CVE-2019-6977

  - CVSS Score: 6.8
  - Description: gdImageColorMatch in gd_color_match.c in the GD Graphics Library (aka
    LibGD) 2.2.5, as used in the imagecolormatch function in PHP before
    5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before
    7.3.1, has a heap-based buffer overflow. This can be exploited by
    an attacker who is able to trigger imagecolormatch calls with crafted
    image data.

- Vulnerability: CVE-2015-8873

  - CVSS Score: 5
  - Description: Stack consumption vulnerability in Zend/zend_exceptions.c in PHP
    before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 allows
    remote attackers to cause a denial of service (segmentation fault)
    via recursive method calls.

- Vulnerability: CVE-2015-8877

  - CVSS Score: 5

- Description: The gdImageScaleTwoPass function in gd_interpolation.c in the GD
  Graphics Library (aka libgd) before 2.2.0, as used in PHP before
  5.6.12, uses inconsistent allocate and free approaches, which allows
  remote attackers to cause a denial of service (memory consumption)
  via a crafted call, as demonstrated by a call to the PHP imagescale
  function.

- Vulnerability: CVE-2015-5590

  - CVSS Score: 7.5
  - Description: Stack-based buffer overflow in the phar_fix_filepath function in
    ext/phar/phar.c in PHP before 5.4.43, 5.5.x before 5.5.27, and 5.6.x
    before 5.6.11 allows remote attackers to cause a denial of service or
    possibly have unspecified other impact via a large length value, as
    demonstrated by mishandling of an e-mail attachment by the imap PHP
    extension.

- Vulnerability: CVE-2015-8879

  - CVSS Score: 5
  - Description: The odbc_bindcols function in ext/odbc/php_odbc.c in PHP before 5.6.12
    mishandles driver behavior for SQL_WVARCHAR columns, which allows
    remote attackers to cause a denial of service (application crash) in
    opportunistic circumstances by leveraging use of the odbc_fetch_array
    function to access a certain type of Microsoft SQL Server table.

- Vulnerability: CVE-2014-9425

  - CVSS Score: 7.5
  - Description: Double free vulnerability in the zend_ts_hash_graceful_destroy
    function in zend_ts_hash.c in the Zend Engine in PHP through 5.5.20
    and 5.6.x through 5.6.4 allows remote attackers to cause a denial
    of service or possibly have unspecified other impact via unknown
    vectors.

- Vulnerability: CVE-2013-1862

  - CVSS Score: 5.1
  - Description: mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server
    2.2.x before 2.2.25 writes data to a log file without sanitizing
    non-printable characters, which might allow remote attackers to
    execute arbitrary commands via an HTTP request containing an escape
    sequence for a terminal emulator.

- Vulnerability: CVE-2014-9426

  - CVSS Score: 7.5
  - Description: The apprentice_load function in libmagic/apprentice.c in the Fileinfo
    component in PHP through 5.6.4 attempts to perform a free operation
    on a stack-based character array, which allows remote attackers to
    cause a denial of service (memory corruption or application crash)
    or possibly have unspecified other impact via unknown vectors. NOTE:
    this is disputed by the vendor because the standard erealloc behavior
    makes the free operation unreachable

- Vulnerability: CVE-2013-4113

  - CVSS Score: 6.8
  - Description: ext/xml/xml.c in PHP before 5.3.27 does not properly consider parsing
    depth, which allows remote attackers to cause a denial of service
    (heap memory corruption) or possibly have unspecified other impact
    via a crafted document that is processed by the xml_parse_into_struct
    function.

- Vulnerability: CVE-2014-0098

  – CVSS Score: 5
  – Description: The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.

- Vulnerability: CVE-2024-40898

  – CVSS Score: N/A
  – Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2018-15132

  – CVSS Score: 5
  – Description: An issue was discovered in ext/standard/link_win32.c in PHP before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8. The linkinfo function on Windows doesn't implement the open_basedir check. This could be abused to find files on paths outside of the allowed directories.

- Vulnerability: CVE-2016-7124

  – CVSS Score: 7.5
  – Description: ext/standard/var_unserializer.c in PHP before 5.6.25 and 7.x before 7.0.10 mishandles certain invalid objects, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data that leads to a (1) __destruct call or (2) magic method call.

- Vulnerability: CVE-2016-7125

  – CVSS Score: 5
  – Description: ext/session/session.c in PHP before 5.6.25 and 7.x before 7.0.10 skips invalid session names in a way that triggers incorrect parsing, which allows remote attackers to inject arbitrary-type session data by leveraging control of a session name, as demonstrated by object injection.

- Vulnerability: CVE-2016-7126

  – CVSS Score: 7.5
  – Description: The imagetruecolortopalette function in ext/gd/gd.c in PHP before 5.6.25 and 7.x before 7.0.10 does not properly validate the number of colors, which allows remote attackers to cause a denial of service (select_colors allocation error and out-of-bounds write) or possibly have unspecified other impact via a large value in the third argument.

- Vulnerability: CVE-2016-7127

  – CVSS Score: 7.5
  – Description: The imagegammacorrect function in ext/gd/gd.c in PHP before 5.6.25 and 7.x before 7.0.10 does not properly validate gamma values, which allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact by providing different signs for the second and third arguments.

- Vulnerability: CVE-2016-7128

- CVSS Score: 5
- Description: The exif_process_IFD_in_TIFF function in ext/exif/exif.c in PHP before 5.6.25 and 7.x before 7.0.10 mishandles the case of a thumbnail offset that exceeds the file size, which allows remote attackers to obtain sensitive information from process memory via a crafted TIFF image.

- Vulnerability: CVE-2016-7129

  - CVSS Score: 7.5
  - Description: The php_wddx_process_data function in ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via an invalid ISO 8601 time value, as demonstrated by a wddx_deserialize call that mishandles a dateTime element in a wddxPacket XML document.

- Vulnerability: CVE-2011-3267

  - CVSS Score: 5
  - Description: PHP before 5.3.7 does not properly implement the error_log function, which allows context-dependent attackers to cause a denial of service (application crash) via unspecified vectors.

- Vulnerability: CVE-2017-11628

  - CVSS Score: 6.8
  - Description: In PHP before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7, a stack-based buffer overflow in the zend_ini_do_op() function in Zend/zend_ini_parser.c could cause a denial of service or potentially allow executing code. NOTE: this is only relevant for PHP applications that accept untrusted input (instead of the system's php.ini file) for the parse_ini_string or parse_ini_file function, e.g., a web application for syntax validation of php.ini directives.

- Vulnerability: CVE-2017-12933

  - CVSS Score: 7.5
  - Description: The finish_nested_data function in ext/standard/var_unserializer.re in PHP before 5.6.31, 7.0.x before 7.0.21, and 7.1.x before 7.1.7 is prone to a buffer over-read while unserializing untrusted data. Exploitation of this issue can have an unspecified impact on the integrity of PHP.

- Vulnerability: CVE-2011-3268

  - CVSS Score: 10
  - Description: Buffer overflow in the crypt function in PHP before 5.3.7 allows context-dependent attackers to have an unspecified impact via a long salt argument, a different vulnerability than CVE-2011-2483.

- Vulnerability: CVE-2014-9767

  - CVSS Score: 4.3
  - Description: Directory traversal vulnerability in the ZipArchive::extractTo function in ext/zip/php_zip.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 and ext/zip/ext_zip.cpp in HHVM before 3.12.1 allows remote attackers to create arbitrary empty directories via a crafted ZIP archive.

- Vulnerability: CVE-2015-2331

  - CVSS Score: 7.5

- Description: Integer overflow in the _zip_cdir_new function in zip_dirent.c in libzip 0.11.2 and earlier, as used in the ZIP extension in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 and other products, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a ZIP archive that contains many entries, leading to a heap-based buffer overflow.

- Vulnerability: CVE-2012-2336

  - CVSS Score: 5
  - Description: sapi/cgi/cgi_main.c in PHP before 5.3.13 and 5.4.x before 5.4.3, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to cause a denial of service (resource consumption) by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'T' case. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1823.

- Vulnerability: CVE-2012-4001

  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2016-5114

  - CVSS Score: 6.4
  - Description: sapi/fpm/fpm/fpm_log.c in PHP before 5.5.31, 5.6.x before 5.6.17, and 7.x before 7.0.2 misinterprets the semantics of the snprintf return value, which allows attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read and buffer overflow) via a long string, as demonstrated by a long URI in a configuration with custom REQUEST_URI logging.

- Vulnerability: CVE-2016-4343

  - CVSS Score: 6.8
  - Description: The phar_make_dirstream function in ext/phar/dirstream.c in PHP before 5.6.18 and 7.x before 7.0.3 mishandles zero-size ./.@LongLink files, which allows remote attackers to cause a denial of service (uninitialized pointer dereference) or possibly have unspecified other impact via a crafted TAR archive.

- Vulnerability: CVE-2016-4342

  - CVSS Score: 8.3
  - Description: ext/phar/phar_object.c in PHP before 5.5.32, 5.6.x before 5.6.18, and 7.x before 7.0.3 mishandles zero-length uncompressed data, which allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via a crafted (1) TAR, (2) ZIP, or (3) PHAR archive.

- Vulnerability: CVE-2015-0228

  - CVSS Score: 5
  - Description: The lua_websocket_read function in lua_request.c in the mod_lua module in the Apache HTTP Server through 2.4.12 allows remote attackers to cause a denial of service (child-process crash) by sending a crafted WebSocket Ping frame after a Lua script has called the wsupgrade function.

- Vulnerability: CVE-2015-3330
  - CVSS Score: 6.8
  - Description: The php_handler function in sapi/apache2handler/sapi_apache2.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8, when the Apache HTTP Server 2.4.x is used, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via pipelined HTTP requests that result in a "deconfigured interpreter."

- Vulnerability: CVE-2010-2068
  - CVSS Score: 5
  - Description: mod_proxy_http.c in mod_proxy_http in the Apache HTTP Server 2.2.9 through 2.2.15, 2.3.4-alpha, and 2.3.5-alpha on Windows, NetWare, and OS/2, in certain configurations involving proxy worker pools, does not properly detect timeouts, which allows remote attackers to obtain a potentially sensitive response intended for a different client in opportunistic circumstances via a normal HTTP request.

- Vulnerability: CVE-2016-3142
  - CVSS Score: 6.4
  - Description: The phar_parse_zipfile function in zip.c in the PHAR extension in PHP before 5.5.33 and 5.6.x before 5.6.19 allows remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read and application crash) by placing a PK\{}x05\{}x06 signature at an invalid location.

- Vulnerability: CVE-2016-3141
  - CVSS Score: 7.5
  - Description: Use-after-free vulnerability in wddx.c in the WDDX extension in PHP before 5.5.33 and 5.6.x before 5.6.19 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact by triggering a wddx_deserialize call on XML data containing a crafted var element.

- Vulnerability: CVE-2017-9798
  - CVSS Score: 5
  - Description: Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.

- Vulnerability: CVE-2013-4365
  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2013-4248
  - CVSS Score: 4.3

- Description: The openssl_x509_parse function in openssl.c in the OpenSSL module in PHP before 5.4.18 and 5.5.x before 5.5.2 does not properly handle a '\{}0' character in a domain name in the Subject Alternative Name field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- **Vulnerability:** CVE-2021-32791

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

- **Vulnerability:** CVE-2021-32792

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.

- **Vulnerability:** CVE-2023-31122

  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- **Vulnerability:** CVE-2009-0796

  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- **Vulnerability:** CVE-2011-1468

  - CVSS Score: 4.3
  - Description: Multiple memory leaks in the OpenSSL extension in PHP before 5.3.6 might allow remote attackers to cause a denial of service (memory consumption) via (1) plaintext data to the openssl_encrypt function or (2) ciphertext data to the openssl_decrypt function.

- **Vulnerability:** CVE-2011-1469

  - CVSS Score: 4.3
  - Description: Unspecified vulnerability in the Streams component in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) by accessing an ftp:// URL during use of an HTTP proxy with the FTP wrapper.

- **Vulnerability:** CVE-2011-1466

  - CVSS Score: 5

– Description: Integer overflow in the SdnToJulian function in the Calendar extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via a large integer in the first argument to the cal_from_jd function.

- Vulnerability: CVE-2011-1467

    – CVSS Score: 5
    – Description: Unspecified vulnerability in the NumberFormatter::setSymbol (aka numfmt_set_symbol) function in the Intl extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via an invalid argument, a related issue to CVE-2010-4409.

- Vulnerability: CVE-2011-1464

    – CVSS Score: 4.3
    – Description: Buffer overflow in the strval function in PHP before 5.3.6, when the precision configuration option has a large value, might allow context-dependent attackers to cause a denial of service (application crash) via a small numerical value in the argument.

- Vulnerability: CVE-2015-4148

    – CVSS Score: 5
    – Description: The do_soap_call function in ext/soap/soap.c in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 does not verify that the uri property is a string, which allows remote attackers to obtain sensitive information by providing crafted serialized data with an int data type, related to a "type confusion" issue.

- Vulnerability: CVE-2015-8935

    – CVSS Score: 4.3
    – Description: The sapi_header_op function in main/SAPI.c in PHP before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6 supports deprecated line folding without considering browser compatibility, which allows remote attackers to conduct cross-site scripting (XSS) attacks against Internet Explorer by leveraging (1) %0A%20 or (2) %0D%0A%20 mishandling in the header function.

- Vulnerability: CVE-2015-4147

    – CVSS Score: 7.5
    – Description: The SoapClient::__call method in ext/soap/soap.c in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 does not verify that __default_headers is an array, which allows remote attackers to execute arbitrary code by providing crafted serialized data with an unexpected data type, related to a "type confusion" issue.

- Vulnerability: CVE-2012-0057

    – CVSS Score: 6.4
    – Description: PHP before 5.3.9 has improper libxslt security settings, which allows remote attackers to create arbitrary files via a crafted XSLT stylesheet that uses the libxslt output extension.

- Vulnerability: CVE-2017-3167

    – CVSS Score: 7.5
    – Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.

- Vulnerability: CVE-2012-0053
  - CVSS Score: 4.3
  - Description: protocol.c in the Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header information during construction of Bad Request (aka 400) error documents, which allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a (1) long or (2) malformed header in conjunction with crafted web script.
- Vulnerability: CVE-2012-0883
  - CVSS Score: 6.9
  - Description: envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the LD_LIBRARY_PATH, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of apachectl.
- Vulnerability: CVE-2017-3169
  - CVSS Score: 7.5
  - Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.
- Vulnerability: CVE-2021-44790
  - CVSS Score: 7.5
  - Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.
- Vulnerability: CVE-2018-14851
  - CVSS Score: 4.3
  - Description: exif_process_IFD_in_MAKERNOTE in ext/exif/exif.c in PHP before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted JPEG file.
- Vulnerability: CVE-2011-3639
  - CVSS Score: 4.3
  - Description: The mod_proxy module in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x before 2.2.18, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers by using the HTTP/0.9 protocol with a malformed URI containing an initial @ (at sign) character. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-3368.
- Vulnerability: CVE-2013-6501
  - CVSS Score: 4.6
  - Description: The default soap.wsdl_cache_dir setting in (1) php.ini-production and (2) php.ini-development in PHP through 5.6.7 specifies the /tmp directory, which makes it easier for local users to conduct WSDL injection attacks by creating a file under /tmp with a predictable filename that is used by the get_sdl function in ext/soap/php_sdl.c.
- Vulnerability: CVE-2013-1643

- CVSS Score: 5
- Description: The SOAP parser in PHP before 5.3.23 and 5.4.x before 5.4.13 allows remote attackers to read arbitrary files via a SOAP WSDL file containing an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue in the soap_xmlParseFile and soap_xmlParseMemory functions. NOTE: this vulnerability exists because of an incorrect fix for CVE-2013-1824.

- Vulnerability: CVE-2021-34798

  - CVSS Score: 5
  - Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2014-3668

  - CVSS Score: 5
  - Description: Buffer overflow in the date_from_ISO8601 function in the mkgmtime implementation in libxmlrpc/xmlrpc.c in the XMLRPC extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) via (1) a crafted first argument to the xmlrpc_set_type function or (2) a crafted argument to the xmlrpc_decode function, related to an out-of-bounds read operation.

- Vulnerability: CVE-2011-4885

  - CVSS Score: 5
  - Description: PHP before 5.3.9 computes hash values for form parameters without restricting the ability to trigger hash collisions predictably, which allows remote attackers to cause a denial of service (CPU consumption) by sending many crafted parameters.

- Vulnerability: CVE-2018-19396

  - CVSS Score: 5
  - Description: ext/standard/var_unserializer.c in PHP 5.x through 7.1.24 allows attackers to cause a denial of service (application crash) via an unserialize call for the com, dotnet, or variant class.

- Vulnerability: CVE-2018-19395

  - CVSS Score: 5
  - Description: ext/standard/var.c in PHP 5.x through 7.1.24 on Windows allows attackers to cause a denial of service (NULL pointer dereference and application crash) because com and com_safearray_proxy return NULL in com_properties_get in ext/com_dotnet/com_handlers.c, as demonstrated by a serialize call on COM("WScript.Shell").

- Vulnerability: CVE-2013-3735

  - CVSS Score: 5
  - Description: The Zend Engine in PHP before 5.4.16 RC1, and 5.5.0 before RC2, does not properly determine whether a parser error occurred, which allows context-dependent attackers to cause a denial of service (memory consumption and application crash) via a crafted function definition, as demonstrated by an attack within a shared web-hosting environment. NOTE: the vendor's http://php.net/security-note.php page says "for critical security situations you should be using OS-level security by running multiple web servers each as their own user id.

- Vulnerability: CVE-2012-2376

- CVSS Score: 10
- Description: Buffer overflow in the com_print_typeinfo function in PHP 5.4.3 and earlier on Windows allows remote attackers to execute arbitrary code via crafted arguments that trigger incorrect handling of COM object VARIANT types, as exploited in the wild in May 2012.

• Vulnerability: CVE-2010-3870

- CVSS Score: 6.8
- Description: The utf8_decode function in PHP before 5.3.4 does not properly handle non-shortest form UTF-8 encoding and ill-formed subsequences in UTF-8 data, which makes it easier for remote attackers to bypass cross-site scripting (XSS) and SQL injection protection mechanisms via a crafted string.

• Vulnerability: CVE-2012-0831

- CVSS Score: 6.8
- Description: PHP before 5.3.10 does not properly perform a temporary change to the magic_quotes_gpc directive during the importing of environment variables, which makes it easier for remote attackers to conduct SQL injection attacks via a crafted request, related to main/php_variables.c, sapi/cgi/cgi_main.c, and sapi/fpm/fpm/fpm_main.c.

• Vulnerability: CVE-2010-4409

- CVSS Score: 5
- Description: Integer overflow in the NumberFormatter::getSymbol (aka numfmt_get_symbol) function in PHP 5.3.3 and earlier allows context-dependent attackers to cause a denial of service (application crash) via an invalid argument.

• Vulnerability: CVE-2022-31813

- CVSS Score: 7.5
- Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

• Vulnerability: CVE-2014-3597

- CVSS Score: 6.8
- Description: Multiple buffer overflows in the php_parserr function in ext/standard/dns.c in PHP before 5.4.32 and 5.5.x before 5.5.16 allow remote DNS servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted DNS record, related to the dns_get_record function and the dn_expand function. NOTE: this issue exists because of an incomplete fix for CVE-2014-4049.

• Vulnerability: CVE-2012-3450

- CVSS Score: 2.6
- Description: pdo_sql_parser.re in the PDO extension in PHP before 5.3.14 and 5.4.x before 5.4.4 does not properly determine the end of the query string during parsing of prepared statements, which allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted parameter value.

• Vulnerability: CVE-2014-9652

- CVSS Score: 5

- Description: The mconvert function in softmagic.c in file before 5.21, as used in the Fileinfo component in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5, does not properly handle a certain string-length field during a copy of a truncated version of a Pascal string, which might allow remote attackers to cause a denial of service (out-of-bounds memory access and application crash) via a crafted file.

- Vulnerability: CVE-2014-9653

  - CVSS Score: 7.5
  - Description: readelf.c in file before 5.22, as used in the Fileinfo component in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5, does not consider that pread calls sometimes read only a subset of the available data, which allows remote attackers to cause a denial of service (uninitialized memory access) or possibly have unspecified other impact via a crafted ELF file.

- Vulnerability: CVE-2019-9023

  - CVSS Score: 7.5
  - Description: An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A number of heap-based buffer over-read instances are present in mbstring regular expression functions when supplied with invalid multibyte data. These occur in ext/mbstring/oniguruma/regcomp.c, ext/mbstring/oniguruma/regexec.c, ext/mbstring/oniguruma/regparse.c, ext/mbstring/oniguruma/enc/unicode.c, and ext/mbstring/oniguruma/src/utf32_be when a multibyte regular expression pattern contains invalid multibyte sequences.

- Vulnerability: CVE-2019-9020

  - CVSS Score: 7.5
  - Description: An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. Invalid input to the function xmlrpc_decode() can lead to an invalid memory access (heap out of bounds read or read after free). This is related to xml_elem_parse_buf in ext/xmlrpc/libxmlrpc/xml_element.c.

- Vulnerability: CVE-2019-9021

  - CVSS Score: 7.5
  - Description: An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A heap-based buffer over-read in PHAR reading functions in the PHAR extension may allow an attacker to read allocated or unallocated memory past the actual data when trying to parse the file name, a different vulnerability than CVE-2018-20783. This is related to phar_detect_phar_fname_ext in ext/phar/phar.c.

- Vulnerability: CVE-2019-9024

  - CVSS Score: 5
  - Description: An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. xmlrpc_decode() can allow a hostile XMLRPC server to cause PHP to read memory outside of allocated areas in base64_decode_xmlrpc in ext/xmlrpc/libxmlrpc/base64.c.

- Vulnerability: CVE-2016-6291

  - CVSS Score: 7.5

– Description: The exif_process_IFD_in_MAKERNOTE function in ext/exif/exif.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (out-of-bounds array access and memory corruption), obtain sensitive information from process memory, or possibly have unspecified other impact via a crafted JPEG image.

- Vulnerability: CVE-2016-6290

  – CVSS Score: 7.5

  – Description: ext/session/session.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 does not properly maintain a certain hash data structure, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via vectors related to session deserialization.

- Vulnerability: CVE-2016-6292

  – CVSS Score: 4.3

  – Description: The exif_process_user_comment function in ext/exif/exif.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted JPEG image.

- Vulnerability: CVE-2016-6295

  – CVSS Score: 7.5

  – Description: ext/snmp/snmp.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to cause a denial of service (use-after-free and application crash) or possibly have unspecified other impact via crafted serialized data, a related issue to CVE-2016-5773.

- Vulnerability: CVE-2016-6294

  – CVSS Score: 7.5

  – Description: The locale_accept_from_http function in ext/intl/locale/locale_methods.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 does not properly restrict calls to the ICU uloc_acceptLanguageFromHTTP function, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a call with a long argument.

- Vulnerability: CVE-2016-6297

  – CVSS Score: 6.8

  – Description: Integer overflow in the php_stream_zip_opener function in ext/zip/zip_stream.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a crafted zip:// URL.

- Vulnerability: CVE-2016-6296

  – CVSS Score: 7.5

  – Description: Integer signedness error in the simplestring_addn function in simplestring.c in xmlrpc-epi through 0.54.2, as used in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9, allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a long first argument to the PHP xmlrpc_encode_request function.

- Vulnerability: CVE-2022-22720

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2015-0273

  - CVSS Score: 7.5
  - Description: Multiple use-after-free vulnerabilities in ext/date/php_date.c in PHP before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6 allow remote attackers to execute arbitrary code via crafted serialized input containing a (1) R or (2) r type specifier in (a) DateTimeZone data handled by the php_date_timezone_initialize_from_hash function or (b) DateTime data handled by the php_date_initialize_from_hash function.

- Vulnerability: CVE-2016-9138

  - CVSS Score: 7.5
  - Description: PHP through 5.6.27 and 7.x through 7.0.12 mishandles property modification during __wakeup processing, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data, as demonstrated by Exception::__toString with DateInterval::__wakeup.

- Vulnerability: CVE-2016-10397

  - CVSS Score: 5
  - Description: In PHP before 5.6.28 and 7.x before 7.0.13, incorrect handling of various URI components in the URL parser could be used by attackers to bypass hostname-specific URL checks, as demonstrated by evil.example.com:80#@good.example.com/ and evil.example.com:80?@good.example.com/ inputs to the parse_url function (implemented in the php_url_parse_ex function in ext/standard/url.c).

- Vulnerability: CVE-2014-3669

  - CVSS Score: 7.5
  - Description: Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.

- Vulnerability: CVE-2011-1092

  - CVSS Score: 7.5
  - Description: Integer overflow in ext/shmop/shmop.c in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (crash) and possibly read sensitive memory via a large third argument to the shmop_read function.

- Vulnerability: CVE-2015-3307

  - CVSS Score: 7.5
  - Description: The phar_parse_metadata function in ext/phar/phar.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service (heap metadata corruption) or possibly have unspecified other impact via a crafted tar archive.

- Vulnerability: CVE-2012-4388

  - CVSS Score: 4.3
  - Description: The sapi_header_op function in main/SAPI.c in PHP 5.4.0RC2 through 5.4.0 does not properly determine a pointer during checks for %0D sequences (aka carriage return characters), which allows remote attackers to bypass an HTTP response-splitting protection mechanism via a crafted URL, related to improper interaction between the PHP header function and certain browsers, as demonstrated by Internet Explorer and Google Chrome. NOTE: this vulnerability exists because of an incorrect fix for CVE-2011-1398.

- Vulnerability: CVE-2021-40438

  - CVSS Score: 6.8
  - Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2010-4699

  - CVSS Score: 5
  - Description: The iconv_mime_decode_headers function in the Iconv extension in PHP before 5.3.4 does not properly handle encodings that are unrecognized by the iconv and mbstring (aka Multibyte String) implementations, which allows remote attackers to trigger an incomplete output array, and possibly bypass spam detection or have unspecified other impact, via a crafted Subject header in an e-mail message, as demonstrated by the ks_c_5601-1987 character set.

- Vulnerability: CVE-2016-9935

  - CVSS Score: 7.5
  - Description: The php_wddx_push_element function in ext/wddx/wddx.c in PHP before 5.6.29 and 7.x before 7.0.14 allows remote attackers to cause a denial of service (out-of-bounds read and memory corruption) or possibly have unspecified other impact via an empty boolean element in a wddxPacket XML document.

- Vulnerability: CVE-2010-2950

  - CVSS Score: 6.8
  - Description: Format string vulnerability in stream.c in the phar extension in PHP 5.3.x through 5.3.3 allows context-dependent attackers to obtain sensitive information (memory contents) and possibly execute arbitrary code via a crafted phar:// URI that is not properly handled by the phar_stream_flush function, leading to errors in the php_stream_wrapper_log_error function. NOTE: this vulnerability exists because of an incomplete fix for CVE-2010-2094.

- Vulnerability: CVE-2015-3183

  - CVSS Score: 5

152

– Description: The chunked transfer coding implementation in the Apache HTTP
Server before 2.4.14 does not properly parse chunk headers,
which allows remote attackers to conduct HTTP request smuggling
attacks via a crafted request, related to mishandling of large
chunk-size values and invalid chunk-extension characters in
modules/http/http_filters.c.

- Vulnerability: CVE-2011-0753

  – CVSS Score: 4.3

  – Description: Race condition in the PCNTL extension in PHP before 5.3.4, when a
  user-defined signal handler exists, might allow context-dependent
  attackers to cause a denial of service (memory corruption) via a
  large number of concurrent signals.

- Vulnerability: CVE-2011-0755

  – CVSS Score: 5

  – Description: Integer overflow in the mt_rand function in PHP before 5.3.4 might
  make it easier for context-dependent attackers to predict the return
  values by leveraging a script's use of a large max parameter, as
  demonstrated by a value that exceeds mt_getrandmax.

- Vulnerability: CVE-2011-0754

  – CVSS Score: 4.4

  – Description: The SplFileInfo::getType function in the Standard PHP Library (SPL)
  extension in PHP before 5.3.4 on Windows does not properly detect
  symbolic links, which might make it easier for local users to conduct
  symlink attacks by leveraging cross-platform differences in the stat
  structure, related to lack of a FILE_ATTRIBUTE_REPARSE_POINT check.

- Vulnerability: CVE-2016-5094

  – CVSS Score: 7.5

  – Description: Integer overflow in the php_html_entities function in
  ext/standard/html.c in PHP before 5.5.36 and 5.6.x before 5.6.22
  allows remote attackers to cause a denial of service or possibly have
  unspecified other impact by triggering a large output string from the
  htmlspecialchars function.

- Vulnerability: CVE-2016-2554

  – CVSS Score: 10

  – Description: Stack-based buffer overflow in ext/phar/tar.c in PHP before 5.5.32,
  5.6.x before 5.6.18, and 7.x before 7.0.3 allows remote attackers
  to cause a denial of service (application crash) or possibly have
  unspecified other impact via a crafted TAR archive.

- Vulnerability: CVE-2013-1896

  – CVSS Score: 4.3

  – Description: mod_dav.c in the Apache HTTP Server before 2.2.25 does not properly
  determine whether DAV is enabled for a URI, which allows remote
  attackers to cause a denial of service (segmentation fault) via a
  MERGE request in which the URI is configured for handling by the
  mod_dav_svn module, but a certain href attribute in XML data refers to
  a non-DAV URI.

- Vulnerability: CVE-2016-8612

  – CVSS Score: 3.3

– Description: Apache HTTP Server mod_cluster before version httpd 2.4.23 is
                vulnerable to an Improper Input Validation in the protocol parsing
                logic in the load balancer resulting in a Segmentation Fault in the
                serving httpd process.

- Vulnerability: CVE-2022-37436

  – CVSS Score: N/A
  – Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause
                  the response headers to be truncated early, resulting in some headers
                  being incorporated into the response body. If the later headers have
                  any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2017-16642

  – CVSS Score: 5
  – Description: In PHP before 5.6.32, 7.x before 7.0.25, and 7.1.x before 7.1.11, an
                  error in the date extension's timelib_meridian handling of 'front
                  of' and 'back of' directives could be used by attackers able to
                  supply date strings to leak information from the interpreter,
                  related to ext/date/lib/parse_date.c out-of-bounds reads affecting
                  the php_parse_date function. NOTE: this is a different issue than
                  CVE-2017-11145.

- Vulnerability: CVE-2012-3499

  – CVSS Score: 4.3
  – Description: Multiple cross-site scripting (XSS) vulnerabilities in the Apache
                  HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow
                  remote attackers to inject arbitrary web script or HTML via vectors
                  involving hostnames and URIs in the (1) mod_imagemap, (2) mod_info,
                  (3) mod_ldap, (4) mod_proxy_ftp, and (5) mod_status modules.

- Vulnerability: CVE-2010-4657

  – CVSS Score: 5
  – Description: PHP5 before 5.4.4 allows passing invalid utf-8 strings via the
                  xmlTextWriterWriteAttribute, which are then misparsed by libxml2.
                  This results in memory leak into the resulting output.

- Vulnerability: CVE-2010-4156

  – CVSS Score: 5
  – Description: The mb_strcut function in Libmbfl 1.1.0, as used in PHP 5.3.x through
                  5.3.3, allows context-dependent attackers to obtain potentially
                  sensitive information via a large value of the third parameter (aka
                  the length parameter).

- Vulnerability: CVE-2008-0455

  – CVSS Score: 4.3
  – Description: Cross-site scripting (XSS) vulnerability in the mod_negotiation
                  module in the Apache HTTP Server 2.2.6 and earlier in the 2.2.x
                  series, 2.0.61 and earlier in the 2.0.x series, and 1.3.39 and
                  earlier in the 1.3.x series allows remote authenticated users to
                  inject arbitrary web script or HTML by uploading a file with a
                  name containing XSS sequences and a file extension, which leads to
                  injection within a (1) "406 Not Acceptable" or (2) "300 Multiple
                  Choices" HTTP response when the extension is omitted in a request for
                  the file.

- Vulnerability: CVE-2010-4150

- CVSS Score: 5
- Description: Double free vulnerability in the imap_do_open function in the IMAP extension (ext/imap/php_imap.c) in PHP 5.2 before 5.2.15 and 5.3 before 5.3.4 allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors.

- Vulnerability: CVE-2011-4566

  - CVSS Score: 6.4
  - Description: Integer overflow in the exif_process_IFD_TAG function in exif.c in the exif extension in PHP 5.4.0beta2 on 32-bit platforms allows remote attackers to read the contents of arbitrary memory locations or cause a denial of service via a crafted offset_val value in an EXIF header in a JPEG file, a different vulnerability than CVE-2011-0708.

- Vulnerability: CVE-2015-7803

  - CVSS Score: 6.8
  - Description: The phar_get_entry_data function in ext/phar/util.c in PHP before 5.5.30 and 5.6.x before 5.6.14 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a .phar file with a crafted TAR archive entry in which the Link indicator references a file that does not exist.

- Vulnerability: CVE-2015-7804

  - CVSS Score: 6.8
  - Description: Off-by-one error in the phar_parse_zipfile function in ext/phar/zip.c in PHP before 5.5.30 and 5.6.x before 5.6.14 allows remote attackers to cause a denial of service (uninitialized pointer dereference and application crash) by including the / filename in a .zip PHAR archive.

- Vulnerability: CVE-2014-3479

  - CVSS Score: 4.3
  - Description: The cdf_check_stream_offset function in cdf.c in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, relies on incorrect sector-size data, which allows remote attackers to cause a denial of service (application crash) via a crafted stream offset in a CDF file.

- Vulnerability: CVE-2012-0789

  - CVSS Score: 5
  - Description: Memory leak in the timezone functionality in PHP before 5.3.9 allows remote attackers to cause a denial of service (memory consumption) by triggering many strtotime function calls, which are not properly handled by the php_date_parse_tzfile cache.

- Vulnerability: CVE-2012-0788

  - CVSS Score: 5
  - Description: The PDORow implementation in PHP before 5.3.9 does not properly interact with the session feature, which allows remote attackers to cause a denial of service (application crash) via a crafted application that uses a PDO driver for a fetch and then calls the session_start function, as demonstrated by a crash of the Apache HTTP Server.

11.2 IP Address: 159.149.53.16

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 5

- High Vulnerabilities: 31

- Medium Vulnerabilities: 231

- Low Vulnerabilities: 21

- Total Vulnerabilities: 288

Services Running on IP Address

- Service: Apache httpd

  - Port: 80
  - Version: 2.4.6
  - Location: /

- Service: Apache httpd

  - Port: 443
  - Version: 2.4.6
  - Location: /

- Service: N/A

  - Port: 6443
  - Version: N/A
  - Location: /

Vulnerabilities Found

- Vulnerability: CVE-2014-0117

  - CVSS Score: 4.3
  - Description: The mod_proxy module in the Apache HTTP Server 2.4.x before 2.4.10, when a reverse proxy is enabled, allows remote attackers to cause a denial of service (child-process crash) via a crafted HTTP Connection header.

- Vulnerability: CVE-2017-7679

  - CVSS Score: 7.5
  - Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

- Vulnerability: CVE-2017-9798

  - CVSS Score: 5
  - Description: Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.

- Vulnerability: CVE-2015-3185
    - CVSS Score: 4.3
    - Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

- Vulnerability: CVE-2015-3184
    - CVSS Score: 5
    - Description: mod_authz_svn in Apache Subversion 1.7.x before 1.7.21 and 1.8.x before 1.8.14, when using Apache httpd 2.4.x, does not properly restrict anonymous access, which allows remote anonymous users to read hidden files via the path name.

- Vulnerability: CVE-2015-3183
    - CVSS Score: 5
    - Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

- Vulnerability: CVE-2013-4365
    - CVSS Score: 7.5
    - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2018-5407
    - CVSS Score: 1.9
    - Description: Simultaneous Multi-threading (SMT) in processors can enable local users to exploit software vulnerable to timing attacks via a side-channel timing attack on 'port contention'.

- Vulnerability: CVE-2022-28330
    - CVSS Score: 5
    - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2021-32791
    - CVSS Score: 4.3
    - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2021-32792

  – CVSS Score: 4.3

  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.

- Vulnerability: CVE-2024-38476

  – CVSS Score: N/A

  – Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-38477

  – CVSS Score: N/A

  – Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2023-31122

  – CVSS Score: N/A

  – Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2009-0796

  – CVSS Score: 2.6

  – Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2022-2068

  – CVSS Score: 10

  – Description: In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze).

- Vulnerability: CVE-2014-0118

  – CVSS Score: 4.3

- Description: The deflate_in_filter function in mod_deflate.c in the mod_deflate module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.

- Vulnerability: CVE-2013-6438

  - CVSS Score: 5
  - Description: The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.

- Vulnerability: CVE-2020-1927

  - CVSS Score: 5.8
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.

- Vulnerability: CVE-2023-0286

  - CVSS Score: N/A
  - Description: There is a type confusion vulnerability relating to X.400 address processinginside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING butthe public structure definition for GENERAL_NAME incorrectly specified the typeof the x400Address field as ASN1_TYPE. This field is subsequently interpreted bythe OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than anASN1_STRING.When CRL checking is enabled (i.e. the application sets theX509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to passarbitrary pointers to a memcmp call, enabling them to read memory contents orenact a denial of service. In most cases, the attack requires the attacker toprovide both the certificate chain and CRL, neither of which need to have avalid signature. If the attacker only controls one of these inputs, the otherinput must already contain an X.400 address as a CRL distribution point, whichis uncommon. As such, this vulnerability is most likely to only affectapplications which have implemented their own functionality for retrieving CRLsover a network.

- Vulnerability: CVE-2023-3817

  - CVSS Score: N/A

– Description: Issue summary: Checking excessively long DH keys or parameters may
                  be very slow.Impact summary: Applications that use the functions
                  DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH
                  key or DH parameters may experience longdelays. Where the key or
                  parameters that are being checked have been obtainedfrom an untrusted
                  source this may lead to a Denial of Service.The function DH_check()
                  performs various checks on DH parameters. After fixingCVE-2023-3446
                  it was discovered that a large q parameter value can also triggeran
                  overly long computation during some of these checks. A correct q
                  value,if present, cannot be larger than the modulus p parameter, thus
                  it isunnecessary to perform these checks if q is larger than p.An
                  application that calls DH_check() and supplies a key or parameters
                  obtainedfrom an untrusted source could be vulnerable to a Denial of
                  Service attack.The function DH_check() is itself called by a number
                  of other OpenSSL functions.An application calling any of those other
                  functions may similarly be affected.The other functions affected
                  by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable
                  are the OpenSSL dhparam and pkeyparam command line applicationswhen
                  using the "-check" option.The OpenSSL SSL/TLS implementation is not
                  affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not
                  affected by this issue.

- Vulnerability: CVE-2017-3167

  – CVSS Score: 7.5

  – Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use
                  of the ap_get_basic_auth_pw() by third-party modules outside of the
                  authentication phase may lead to authentication requirements being
                  bypassed.

- Vulnerability: CVE-2021-32786

  – CVSS Score: 5.8

  – Description: mod_auth_openidc is an authentication/authorization module for the
                  Apache 2.x HTTP server that functions as an OpenID Connect Relying
                  Party, authenticating users against an OpenID Connect Provider. In
                  versions prior to 2.4.9, 'oidc_validate_redirect_url()' does not parse
                  URLs the same way as most browsers do. As a result, this function
                  can be bypassed and leads to an Open Redirect vulnerability in the
                  logout functionality. This bug has been fixed in version 2.4.9
                  by replacing any backslash of the URL to redirect with slashes
                  to address a particular breaking change between the different
                  specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this
                  vulnerability can be mitigated by configuring 'mod_auth_openidc' to
                  only allow redirection whose destination matches a given regular
                  expression.

- Vulnerability: CVE-2021-32785

  – CVSS Score: 4.3

- Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache (`OIDCCacheEncrypt off`, `OIDCSessionType server-cache`, `OIDCCacheType redis`), `mod_auth_openidc` wrongly performed argument interpolation before passing Redis requests to `hiredis`, which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the `hiredis` API. As a workaround, this vulnerability can be mitigated by setting `OIDCCacheEncrypt` to `on`, as cache keys are cryptographically hashed before use when this option is enabled.

- Vulnerability: CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2021-44790

  - CVSS Score: 7.5
  - Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

- Vulnerability: CVE-2016-4975

  - CVSS Score: 4.3
  - Description: Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).

- Vulnerability: CVE-2020-13938

  - CVSS Score: 2.1
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

- Vulnerability: CVE-2023-2650

  - CVSS Score: N/A

- Description: Issue summary: Processing some specially crafted ASN.1 object identifiers ordata containing them may be very slow.Impact summary: Applications that use OBJ_obj2txt() directly, or use any ofthe OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no messagesize limit may experience notable to very long delays when processing thosemessages, which may lead to a Denial of Service.An OBJECT IDENTIFIER is composed of a series of numbers – sub-identifiers –most of which have no size limit. OBJ_obj2txt() may be used to translatean ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSLtype ASN1_OBJECT) to its canonical numeric text form, which are thesub-identifiers of the OBJECT IDENTIFIER in decimal form, separated byperiods.When one of the sub-identifiers in the OBJECT IDENTIFIER is very large(these are sizes that are seen as absurdly large, taking up tens or hundredsof KiBs), the translation to a decimal number in text may take a very longtime. The time complexity is $O(n^2)$ with 'n' being the size of thesub-identifiers in bytes (*).With OpenSSL 3.0, support to fetch cryptographic algorithms using names /identifiers in string form was introduced. This includes using OBJECTIDENTIFIERs in canonical numeric text form as identifiers for fetchingalgorithms.Such OBJECT IDENTIFIERs may be received through the ASN.1 structureAlgorithmIdentifier, which is commonly used in multiple protocols to specifywhat cryptographic algorithm should be used to sign or verify, encrypt ordecrypt, or digest passed data.Applications that call OBJ_obj2txt() directly with untrusted data areaffected, with any version of OpenSSL. If the use is for the mere purposeof display, the severity is considered low.In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME,CMS, CMP/CRMF or TS. It also impacts anything that processes X.509certificates, including simple things like verifying its signature.The impact on TLS is relatively low, because all versions of OpenSSL have a100KiB limit on the peer's certificate chain. Additionally, this onlyimpacts clients, or servers that have explicitly enabled clientauthentication.In OpenSSL 1.1.1 and 1.0.2, this only affects displaying diverse objects,such as X.509 certificates. This is assumed to not happen in such a waythat it would cause a Denial of Service, so these versions are considerednot affected by this issue in such a way that it would be cause for concern,and the severity is therefore considered low.

- Vulnerability: CVE-2023-0215

  - CVSS Score: N/A

- Description: The public API function BIO_new_NDEF is a helper function used for streamingASN.1 data via a BIO. It is primarily used internally to OpenSSL to support theSMIME, CMS and PKCS7 streaming capabilities, but may also be called directly byend user applications.The function receives a BIO from the caller, prepends a new BIO_f_asn1 filterBIO onto the front of it to form a BIO chain, and then returns the new head ofthe BIO chain to the caller. Under certain conditions, for example if a CMSrecipient public key is invalid, the new filter BIO is freed and the functionreturns a NULL result indicating a failure. However, in this case, the BIO chainis not properly cleaned up and the BIO passed by the caller still retainsinternal pointers to the previously freed filter BIO. If the caller then goes onto call BIO_pop() on the BIO then a use-after-free will occur. This will mostlikely result in a crash.This scenario occurs directly in the internal function B64_write_ASN1() whichmay cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() onthe BIO. This internal function is in turn called by the public API functionsPEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream,SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7.Other public API functions that may be impacted by this includei2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream andi2d_PKCS7_bio_stream.The OpenSSL cms and smime command line applications are similarly affected.

- Vulnerability: CVE-2020-35452

  - CVSS Score: 6.8
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

- Vulnerability: CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2020-1934

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

- Vulnerability: CVE-2022-36760

  - CVSS Score: N/A
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-4304

  - CVSS Score: N/A

– Description: A timing based side channel exists in the OpenSSL RSA Decryption implementationwhich could be sufficient to recover a plaintext across a network in aBleichenbacher style attack. To achieve a successful decryption an attackerwould have to be able to send a very large number of trial messages fordecryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5,RSA-OEAP and RSASVE.For example, in a TLS connection, RSA is commonly used by a client to send anencrypted pre-master secret to the server. An attacker that had observed agenuine connection between a client and a server could use this flaw to sendtrial messages to the server and record the time taken to process them. After asufficiently large number of messages the attacker could recover the pre-mastersecret used for the original connection and thus be able to decrypt theapplication data sent over that connection.

• Vulnerability: CVE-2019-1563

– CVSS Score: 4.3

– Description: In situations where an attacker receives automated notification of the success or failure of a decryption attempt an attacker, after sending a very large number of messages to be decrypted, can recover a CMS/PKCS7 transported encryption key or decrypt any RSA encrypted message that was encrypted with the public RSA key, using a Bleichenbacher padding oracle attack. Applications are not affected if they use a certificate together with the private RSA key to the CMS_decrypt or PKCS7_decrypt functions to select the correct recipient info to decrypt. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).

• Vulnerability: CVE-2014-3523

– CVSS Score: 5

– Description: Memory leak in the winnt_accept function in server/mpm/winnt/child.c in the WinNT MPM in the Apache HTTP Server 2.4.x before 2.4.10 on Windows, when the default AcceptFilter is enabled, allows remote attackers to cause a denial of service (memory consumption) via crafted requests.

• Vulnerability: CVE-2013-5704

– CVSS Score: 5

– Description: The mod_headers module in the Apache HTTP Server 2.2.22 allows remote attackers to bypass "RequestHeader unset" directives by placing a header in the trailer portion of data sent with chunked transfer coding. NOTE: the vendor states "this is not a security issue in httpd as such."

• Vulnerability: CVE-2019-17567

– CVSS Score: 5

– Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

• Vulnerability: CVE-2022-31813

– CVSS Score: 7.5

- Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-*
  headers to the origin server based on client side Connection
  header hop-by-hop mechanism. This may be used to bypass IP based
  authentication on the origin server/application.

- Vulnerability: CVE-2012-4360

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module
    0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote
    attackers to inject arbitrary web script or HTML via unspecified
    vectors.

- Vulnerability: CVE-2014-0231

  - CVSS Score: 5
  - Description: The mod_cgid module in the Apache HTTP Server before 2.4.10 does not
    have a timeout mechanism, which allows remote attackers to cause a
    denial of service (process hang) via a request to a CGI script that
    does not read from its stdin file descriptor.

- Vulnerability: CVE-2021-26690

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted
    Cookie header handled by mod_session can cause a NULL pointer
    dereference and crash, leading to a possible Denial Of Service

- Vulnerability: CVE-2021-26691

  - CVSS Score: 7.5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted
    SessionHeader sent by an origin server could cause a heap overflow

- Vulnerability: CVE-2019-0220

  - CVSS Score: 5
  - Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38.
    When the path component of a request URL contains multiple
    consecutive slashes ('/'), directives such as LocationMatch and
    RewriteRule must account for duplicates in regular expressions while
    other aspects of the servers processing will implicitly collapse
    them.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to
    applications calling r:wsread() that point past the end of the
    storage allocated for the buffer.

- Vulnerability: CVE-2021-39275

  - CVSS Score: 7.5
  - Description: ap_escape_quotes() may write beyond the end of a buffer when given
    malicious input. No included modules pass untrusted data to these
    functions, but third-party / external modules may. This issue
    affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2014-3581

  - CVSS Score: 5

- Description: The cache_merge_headers_out function in modules/cache/cache_util.c
  in the mod_cache module in the Apache HTTP Server before 2.4.11
  allows remote attackers to cause a denial of service (NULL pointer
  dereference and application crash) via an empty HTTP Content-Type
  header.

- Vulnerability: CVE-2016-0736

  – CVSS Score: 5
  – Description: In Apache HTTP Server versions 2.4.0 to 2.4.23, mod_session_crypto was
    encrypting its data/cookie using the configured ciphers with possibly
    either CBC or ECB modes of operation (AES256-CBC by default), hence
    no selectable or builtin authenticated encryption. This made it
    vulnerable to padding oracle attacks, particularly with CBC.

- Vulnerability: CVE-2022-29404

  – CVSS Score: 5
  – Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a
    lua script that calls r:parsebody(0) may cause a denial of service
    due to no default limit on possible input size.

- Vulnerability: CVE-2018-1312

  – CVSS Score: 6.8
  – Description: In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest
    authentication challenge, the nonce sent to prevent reply attacks
    was not correctly generated using a pseudo-random seed. In a cluster
    of servers using a common Digest authentication configuration, HTTP
    requests could be replayed across servers by an attacker without
    detection.

- Vulnerability: CVE-2006-20001

  – CVSS Score: N/A
  – Description: A carefully crafted If: request header can cause a memory read, or
    write of a single zero byte, in a pool (heap) memory location beyond
    the header value sent. This could cause the process to crash.This
    issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2017-15710

  – CVSS Score: 5
  – Description: In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to
    2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig,
    uses the Accept-Language header value to lookup the right charset
    encoding when verifying the user's credentials. If the header value
    is not present in the charset conversion table, a fallback mechanism
    is used to truncate it to a two characters value to allow a quick
    retry (for example, 'en-US' is truncated to 'en'). A header value of
    less than two characters forces an out of bound write of one NUL byte
    to a memory location that is not part of the string. In the worst
    case, quite unlikely, the process would crash which could be used as
    a Denial of Service attack. In the more likely case, this memory is
    already reserved for future use and the issue has no effect at all.

- Vulnerability: CVE-2014-0226

  – CVSS Score: 6.8

- Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

- Vulnerability: CVE-2024-0727
  - CVSS Score: N/A
  - Description: Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSLto crash leading to a potential Denial of Service attackImpact summary: Applications loading files in the PKCS12 format from untrustedsources might terminate abruptly.A file in PKCS12 format can contain certificates and keys and may come from anuntrusted source. The PKCS12 specification allows certain fields to be NULL, butOpenSSL does not correctly check for this case. This can lead to a NULL pointerdereference that results in OpenSSL crashing. If an application processes PKCS12files from an untrusted source using the OpenSSL APIs then that application willbe vulnerable to this issue.OpenSSL APIs that are vulnerable to this are: PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a similar issue in SMIME_write_PKCS7(). However since thisfunction is related to writing data we do not consider it security significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.

- Vulnerability: CVE-2009-3766
  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when OpenSSL is used, does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

- Vulnerability: CVE-2009-3767
  - CVSS Score: 4.3
  - Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other versions, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2009-3765
  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2022-22721
  - CVSS Score: 5.8

- Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2022-22720

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2019-10092

  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

- Vulnerability: CVE-2021-3712

  - CVSS Score: 5.8
  - Description: ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own "d2i" functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the "data" and "length" fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the "data" field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). It can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y).

- Vulnerability: CVE-2023-0464

– CVSS Score: N/A

– Description: A security vulnerability has been identified in all supported versionsof OpenSSL related to the verification of X.509 certificate chainsthat include policy constraints. Attackers may be able to exploit thisvulnerability by creating a malicious certificate chain that triggersexponential use of computational resources, leading to a denial-of-service(DoS) attack on affected systems.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.

- **Vulnerability: CVE-2023-0465**

  – CVSS Score: N/A

  – Description: Applications that use a non-default option when verifying certificates may bevulnerable to an attack from a malicious CA to circumvent certain checks.Invalid certificate policies in leaf certificates are silently ignored byOpenSSL and other certificate policy checks are skipped for that certificate.A malicious CA could use this to deliberately assert invalid certificate policiesin order to circumvent policy checking on the certificate altogether.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.

- **Vulnerability: CVE-2023-0466**

  – CVSS Score: N/A

  – Description: The function X509_VERIFY_PARAM_add0_policy() is documented toimplicitly enable the certificate policy check when doing certificateverification. However the implementation of the function does notenable the check which allows certificates with invalid or incorrectpolicies to pass the certificate verification.As suddenly enabling the policy check could break existing deployments it wasdecided to keep the existing behavior of the X509_VERIFY_PARAM_add0_policy()function.Instead the applications that require OpenSSL to perform certificatepolicy check need to use X509_VERIFY_PARAM_set1_policies() or explicitlyenable the policy check by calling X509_VERIFY_PARAM_set_flags() withthe X509_V_FLAG_POLICY_CHECK flag argument.Certificate policy checks are disabled by default in OpenSSL and are notcommonly used by applications.

- **Vulnerability: CVE-2019-10098**

  – CVSS Score: 5.8

  – Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.

- **Vulnerability: CVE-2015-0228**

  – CVSS Score: 5

  – Description: The lua_websocket_read function in lua_request.c in the mod_lua module in the Apache HTTP Server through 2.4.12 allows remote attackers to cause a denial of service (child-process crash) by sending a crafted WebSocket Ping frame after a Lua script has called the wsupgrade function.

- **Vulnerability: CVE-2016-5387**

– CVSS Score: 6.8

– Description: The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18
                 and therefore does not protect applications from the presence of
                 untrusted client data in the HTTP_PROXY environment variable, which
                 might allow remote attackers to redirect an application's outbound
                 HTTP traffic to an arbitrary proxy server via a crafted Proxy header
                 in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states
                 "This mitigation has been assigned the identifier CVE-2016-5387"; in
                 other words, this is not a CVE ID for a vulnerability.

• Vulnerability: CVE-2017-15715

  – CVSS Score: 6.8

  – Description: In Apache httpd 2.4.0 to 2.4.29, the expression specified in
                   <FilesMatch> could match '$' to a newline character in a malicious
                   filename, rather than matching only the end of the filename. This
                   could be exploited in environments where uploads of some files are
                   are externally blocked, but only by matching the trailing portion of
                   the filename.

• Vulnerability: CVE-2021-40438

  – CVSS Score: 6.8

  – Description: A crafted request uri-path can cause mod_proxy to forward the request
                   to an origin server choosen by the remote user. This issue affects
                   Apache HTTP Server 2.4.48 and earlier.

• Vulnerability: CVE-2011-1176

  – CVSS Score: 4.3

  – Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk
                   Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP
                   Server does not properly handle certain configuration sections that
                   specify NiceValue but not AssignUserID, which might allow remote
                   attackers to gain privileges by leveraging the root uid and root gid
                   of an mpm-itk process.

• Vulnerability: CVE-2022-23943

  – CVSS Score: 7.5

  – Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server
                   allows an attacker to overwrite heap memory with possibly attacker
                   provided data. This issue affects Apache HTTP Server 2.4 version
                   2.4.52 and prior versions.

• Vulnerability: CVE-2018-17199

  – CVSS Score: 5

  – Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session
                   checks the session expiry time before decoding the session. This
                   causes session expiry time to be ignored for mod_session_cookie
                   sessions since the expiry time is loaded when the session is decoded.

• Vulnerability: CVE-2021-23841

  – CVSS Score: 4.3

- Description: The OpenSSL public API function X509_issuer_and_serial_hash() attempts
  to create a unique hash value based on the issuer and serial number
  data contained within an X509 certificate. However it fails to
  correctly handle any errors that may occur while parsing the
  issuer field (which might occur if the issuer field is maliciously
  constructed). This may subsequently result in a NULL pointer deref
  and a crash leading to a potential denial of service attack. The
  function X509_issuer_and_serial_hash() is never directly called by
  OpenSSL itself so applications are only vulnerable if they use this
  function directly and they use it on certificates that may have been
  obtained from untrusted sources. OpenSSL versions 1.1.1i and below
  are affected by this issue. Users of these versions should upgrade
  to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected
  by this issue. However OpenSSL 1.0.2 is out of support and no longer
  receiving public updates. Premium support customers of OpenSSL 1.0.2
  should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j.
  Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL
  1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2018-1301

  - CVSS Score: 4.3
  - Description: A specially crafted request could have crashed the Apache HTTP Server
    prior to version 2.4.30, due to an out of bound access after a size
    limit is reached by reading the HTTP header. This vulnerability
    is considered very hard if not impossible to trigger in non-debug
    mode (both log and build level), so it is classified as low risk for
    common server usage.

- Vulnerability: CVE-2018-1302

  - CVSS Score: 4.3
  - Description: When an HTTP/2 stream was destroyed after being handled, the Apache
    HTTP Server prior to version 2.4.30 could have written a NULL pointer
    potentially to an already freed memory. The memory pools maintained
    by the server make this vulnerability hard to trigger in usual
    configurations, the reporter and the team could not reproduce it
    outside debug builds, so it is classified as low risk.

- Vulnerability: CVE-2018-1303

  - CVSS Score: 5
  - Description: A specially crafted HTTP request header could have crashed the Apache
    HTTP Server prior to version 2.4.30 due to an out of bound read while
    preparing data to be cached in shared memory. It could be used as
    a Denial of Service attack against users of mod_cache_socache. The
    vulnerability is considered as low risk since mod_cache_socache is not
    widely used, mod_cache_disk is not concerned by this vulnerability.

- Vulnerability: CVE-2021-34798

  - CVSS Score: 5
  - Description: Malformed requests may cause the server to dereference a NULL
    pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2023-25690

  - CVSS Score: N/A

- Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2020-11985

  - CVSS Score: 4.3
  - Description: IP address spoofing when proxying using mod_remoteip and mod_rewrite For configurations using proxying with mod_remoteip and certain mod_rewrite rules, an attacker could spoof their IP address for logging and PHP scripts. Note this issue was fixed in Apache HTTP Server 2.4.24 but was retrospectively allocated a low severity CVE in 2020.

- Vulnerability: CVE-2021-4160

  - CVSS Score: 4.3
  - Description: There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that is available to premium support customers only. It will be made available in 1.0.2zc when it is released. The issue only affects OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0). Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL 1.0.2zc-dev (Affected 1.0.2-1.0.2zb).

- Vulnerability: CVE-2013-4352

  - CVSS Score: 4.3
  - Description: The cache_invalidate function in modules/cache/cache_storage.c in the mod_cache module in the Apache HTTP Server 2.4.6, when a caching forward proxy is enabled, allows remote HTTP servers to cause a denial of service (NULL pointer dereference and daemon crash) via vectors that trigger a missing hostname value.

- Vulnerability: CVE-2022-26377

  - CVSS Score: 5

- Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2014-0098

  - CVSS Score: 5
  - Description: The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.

- Vulnerability: CVE-2016-8743

  - CVSS Score: 5
  - Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

- Vulnerability: CVE-2024-40898

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2024-38474

  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2022-0778

  - CVSS Score: 5

- Description: The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - TLS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

- Vulnerability: CVE-2020-1971

  - CVSS Score: 4.3

- Description: The X.509 GeneralName type is a generic type for representing
  different types of names. One of those name types is known as
  EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which
  compares different instances of a GENERAL_NAME to see if they
  are equal or not. This function behaves incorrectly when both
  GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference
  and a crash may occur leading to a possible denial of service
  attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two
  purposes: 1) Comparing CRL distribution point names between an
  available CRL and a CRL distribution point embedded in an X509
  certificate 2) When verifying that a timestamp response token signer
  matches the timestamp authority name (exposed via the API functions
  TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can
  control both items being compared then that attacker could trigger
  a crash. For example if the attacker can trick a client or server
  into checking a malicious certificate against a malicious CRL then
  this may occur. Note that some applications automatically download
  CRLs based on a URL embedded in a certificate. This checking happens
  prior to the signatures on the certificate and CRL being verified.
  OpenSSL's s_server, s_client and verify tools have support for the
  "-crl_download" option which implements automatic CRL downloading and
  this attack has been demonstrated to work against those tools. Note
  that an unrelated bug means that affected versions of OpenSSL cannot
  parse or construct correct encodings of EDIPARTYNAME. However it is
  possible to construct a malformed EDIPARTYNAME that OpenSSL's parser
  will accept and hence trigger this attack. All OpenSSL 1.1.1 and
  1.0.2 versions are affected by this issue. Other OpenSSL releases
  are out of support and have not been checked. Fixed in OpenSSL
  1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected
  1.0.2-1.0.2w).

- Vulnerability: CVE-2009-1390

  - CVSS Score: 6.8
  - Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2)
    GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS
    certificate in the chain is accepted instead of verifying the entire
    chain, which allows remote attackers to spoof trusted servers via a
    man-in-the-middle attack.

- Vulnerability: CVE-2012-3526

  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the
    Apache HTTP Server allows remote attackers to cause a denial of
    service (server or application crash) via multiple X-Forwarded-For
    headers in a request.

- Vulnerability: CVE-2023-5678

  - CVSS Score: N/A

- Description: Issue summary: Generating excessively long X9.42 DH keys or checkingexcessively long X9.42 DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_generate_key() togenerate an X9.42 DH key may experience long delays. Likewise, applicationsthat use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check()to check an X9.42 DH key or X9.42 DH parameters may experience long delays.Where the key or parameters that are being checked have been obtained froman untrusted source this may lead to a Denial of Service.While DH_check() performs all the necessary checks (as of CVE-2023-3817),DH_check_pub_key() doesn't make any of these checks, and is thereforevulnerable for excessively large P and Q parameters.Likewise, while DH_generate_key() performs a check for an excessively largeP, it doesn't check for an excessively large Q.An application that calls DH_generate_key() or DH_check_pub_key() andsupplies a key or parameters obtained from an untrusted source could bevulnerable to a Denial of Service attack.DH_generate_key() and DH_check_pub_key() are also called by a number ofother OpenSSL functions. An application calling any of those otherfunctions may similarly be affected. The other functions affected by thisare DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate().Also vulnerable are the OpenSSL pkey command line application when using the"-pubcheck" option, as well as the OpenSSL genpkey command line application.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2017-3736

  - CVSS Score: 4

  - Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

- Vulnerability: CVE-2017-3737

  - CVSS Score: 4.3

– Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

- Vulnerability: CVE-2019-1547

  – CVSS Score: 1.9

  – Description: Normally in OpenSSL EC groups always have a co-factor present and this is used in side channel resistant code paths. However, in some cases, it is possible to construct a group using explicit parameters (instead of using a named curve). In those cases it is possible that such a group does not have the cofactor present. This can occur even where all the parameters match a known named curve. If such a curve is used then OpenSSL falls back to non-side channel resistant code paths which may result in full key recovery during an ECDSA signature operation. In order to be vulnerable an attacker would have to have the ability to time the creation of a large number of signatures where explicit parameters with no co-factor present are in use by an application using libcrypto. For the avoidance of doubt libssl is not vulnerable because explicit parameters are never used. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).

- Vulnerability: CVE-2017-3735

  – CVSS Score: 5

  – Description: While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL before 1.0.2m and 1.1.0g.

- Vulnerability: CVE-2009-2299

  – CVSS Score: 5

  – Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2022-1292

  – CVSS Score: 10

– Description: The c_rehash script does not properly sanitise shell metacharacters
   to prevent command injection. This script is distributed by
   some operating systems in a manner where it is automatically
   executed. On such operating systems, an attacker could execute
   arbitrary commands with the privileges of the script. Use of the
   c_rehash script is considered obsolete and should be replaced by the
   OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected
   3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n).
   Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).

- Vulnerability: CVE-2017-3738

  – CVSS Score: 4.3
  – Description: There is an overflow bug in the AVX2 Montgomery multiplication
     procedure used in exponentiation with 1024-bit moduli. No EC
     algorithms are affected. Analysis suggests that attacks against
     RSA and DSA as a result of this defect would be very difficult to
     perform and are not believed likely. Attacks against DH1024 are
     considered just feasible, because most of the work necessary to
     deduce information about a private key may be performed offline. The
     amount of resources required for such an attack would be significant.
     However, for an attack on TLS to be meaningful, the server would have
     to share the DH1024 private key among multiple clients, which is no
     longer an option since CVE-2016-0701. This only affects processors
     that support the AVX2 but not ADX extensions like Intel Haswell
     (4th generation). Note: The impact from this issue is similar to
     CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version
     1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n.
     Due to the low severity of this issue we are not issuing a new
     release of OpenSSL 1.1.0 at this time. The fix will be included in
     OpenSSL 1.1.0h when it becomes available. The fix is also available
     in commit e502cc86d in the OpenSSL git repository.

- Vulnerability: CVE-2012-4001

  – CVSS Score: 5
  – Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server
     does not properly verify its host name, which allows remote attackers
     to trigger HTTP requests to arbitrary hosts via unspecified vectors,
     as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2022-37436

  – CVSS Score: N/A
  – Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause
     the response headers to be truncated early, resulting in some headers
     being incorporated into the response body. If the later headers have
     any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2021-23840

  – CVSS Score: 5

- Description: Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissable length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2018-0737

  - CVSS Score: 4.3
  - Description: The OpenSSL RSA Key generation algorithm has been shown to be vulnerable to a cache timing side channel attack. An attacker with sufficient access to mount cache timing attacks during the RSA key generation process could recover the private key. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2b-1.0.2o).

- Vulnerability: CVE-2018-0734

  - CVSS Score: 4.3
  - Description: The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.1a (Affected 1.1.1). Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.0.2q (Affected 1.0.2-1.0.2p).

- Vulnerability: CVE-2018-0732

  - CVSS Score: 5
  - Description: During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime value to the client. This will cause the client to spend an unreasonably long period of time generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2-1.0.2o).

- Vulnerability: CVE-2017-9788

  - CVSS Score: 6.4
  - Description: In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.

- Vulnerability: CVE-2018-0739

  - CVSS Score: 4.3

- Description: Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o (Affected 1.0.2b-1.0.2n).

- Vulnerability: CVE-2014-8109

  - CVSS Score: 4.3
  - Description: mod_lua.c in the mod_lua module in the Apache HTTP Server 2.3.x and 2.4.x through 2.4.10 does not support an httpd configuration in which the same Lua authorization provider is used with different arguments within different contexts, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives, as demonstrated by a configuration that specifies authorization for one group to access a certain directory, and authorization for a second group to access a second directory.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2016-2161

  - CVSS Score: 5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.23, malicious input to mod_auth_digest can cause the server to crash, and each instance continues to crash even for subsequently valid requests.

- Vulnerability: CVE-2016-8612

  - CVSS Score: 3.3
  - Description: Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.

- Vulnerability: CVE-2019-1552

  - CVSS Score: 1.9

– Description: OpenSSL has internal defaults for a directory tree where it
can find a configuration file as well as certificates used for
verification in TLS. This directory is most commonly referred to
as OPENSSLDIR, and is configurable with the --prefix / --openssldir
configuration options. For OpenSSL versions 1.1.0 and 1.1.1, the
mingw configuration targets assume that resulting programs and
libraries are installed in a Unix-like environment and the default
prefix for program installation as well as for OPENSSLDIR should be
'/usr/local'. However, mingw programs are Windows programs, and as
such, find themselves looking at sub-directories of 'C:/usr/local',
which may be world writable, which enables untrusted users to modify
OpenSSL's default configuration, insert CA certificates, modify (or
even replace) existing engine modules, etc. For OpenSSL 1.0.2,
'/usr/local/ssl' is used as default for OPENSSLDIR on all Unix and
Windows targets, including Visual C builds. However, some build
instructions for the diverse Windows targets on 1.0.2 encourage
you to specify your own --prefix. OpenSSL versions 1.1.1, 1.1.0
and 1.0.2 are affected by this issue. Due to the limited scope
of affected deployments this has been assessed as low severity and
therefore we are not creating new releases at this time. Fixed
in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL
1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected
1.0.2-1.0.2s).

- Vulnerability: CVE-2013-0941

  – CVSS Score: 2.1

  – Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5
  for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM
  Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows
  use an improper encryption algorithm and a weak key for maintaining
  the stored data of the node secret for the SecurID Authentication
  API, which allows local users to obtain sensitive information via
  cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  – CVSS Score: 4.3

  – Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication
  Agent 7.1 before 7.1.1 for Web for Internet Information Services,
  and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to
  inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2019-1551

  – CVSS Score: 5

  – Description: There is an overflow bug in the x64_64 Montgomery squaring procedure
  used in exponentiation with 512-bit moduli. No EC algorithms are
  affected. Analysis suggests that attacks against 2-prime RSA1024,
  3-prime RSA1536, and DSA1024 as a result of this defect would be
  very difficult to perform and are not believed likely. Attacks
  against DH512 are considered just feasible. However, for an attack
  the target would have to re-use the DH512 private key, which is not
  recommended anyway. Also applications directly using the low level
  API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME. Fixed
  in OpenSSL 1.1.1e (Affected 1.1.1-1.1.1d). Fixed in OpenSSL 1.0.2u
  (Affected 1.0.2-1.0.2t).

- Vulnerability: CVE-2019-1559

  – CVSS Score: 4.3

- Description: If an application encounters a fatal protocol error and then calls
  SSL_shutdown() twice (once to send a close_notify, and once to
  receive one) then OpenSSL can respond differently to the calling
  application if a 0 byte record is received with invalid padding
  compared to if a 0 byte record is received with an invalid MAC. If
  the application then behaves differently based on that in a way that
  is detectable to the remote peer, then this amounts to a padding
  oracle that could be used to decrypt data. In order for this to be
  exploitable "non-stitched" ciphersuites must be in use. Stitched
  ciphersuites are optimised implementations of certain commonly
  used ciphersuites. Also the application must call SSL_shutdown()
  twice even if a protocol error has occurred (applications should
  not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected
  1.0.2-1.0.2q).

- Vulnerability: CVE-2023-45802

  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a
    time window were the request's memory resources were not reclaimed
    immediately. Instead, de-allocation was deferred to connection
    close. A client could send new requests and resets, keeping the
    connection busy and open and causing the memory footprint to keep
    on growing. On connection close, all resources were reclaimed, but
    the process might run out of memory before that.This was found by
    the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset
    Exploit) with their own test client. During "normal" HTTP/2 use, the
    probability to hit this bug is very low. The kept memory would not
    become noticeable before the connection closes or times out.Users are
    recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2018-1283

  - CVSS Score: 3.5
  - Description: In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to
    forward its session data to CGI applications (SessionEnv on, not
    the default), a remote user may influence their content by using a
    "Session" header. This comes from the "HTTP_SESSION" variable name
    used by mod_session to forward its data to CGIs, since the prefix
    "HTTP_" is also used by the Apache HTTP Server to pass HTTP header
    fields, per CGI specifications.

- Vulnerability: CVE-2020-1968

  - CVSS Score: 4.3
  - Description: The Raccoon attack exploits a flaw in the TLS specification which
    can lead to an attacker being able to compute the pre-master
    secret in connections which have used a Diffie-Hellman (DH) based
    ciphersuite. In such a case this would result in the attacker being
    able to eavesdrop on all encrypted communications sent over that TLS
    connection. The attack can only be exploited if an implementation
    re-uses a DH secret across multiple TLS connections. Note that this
    issue only impacts DH ciphersuites and not ECDH ciphersuites. This
    issue affects OpenSSL 1.0.2 which is out of support and no longer
    receiving public updates. OpenSSL 1.1.1 is not vulnerable to this
    issue. Fixed in OpenSSL 1.0.2w (Affected 1.0.2-1.0.2v).

- Vulnerability: CVE-2019-0217

  - CVSS Score: 6

- Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.

- Vulnerability: CVE-2022-28615

  - CVSS Score: 6.4
  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer.   While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- Vulnerability: CVE-2022-28614

  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function.   Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

- Vulnerability: CVE-2014-0117

  - CVSS Score: 4.3
  - Description: The mod_proxy module in the Apache HTTP Server 2.4.x before 2.4.10, when a reverse proxy is enabled, allows remote attackers to cause a denial of service (child-process crash) via a crafted HTTP Connection header.

- Vulnerability: CVE-2017-7679

  - CVSS Score: 7.5
  - Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

- Vulnerability: CVE-2017-9798

  - CVSS Score: 5
  - Description: Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27.   The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data.   This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration.   Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.

- Vulnerability: CVE-2015-3185

  - CVSS Score: 4.3
  - Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

- Vulnerability: CVE-2015-3184

  - CVSS Score: 5
  - Description: mod_authz_svn in Apache Subversion 1.7.x before 1.7.21 and 1.8.x
    before 1.8.14, when using Apache httpd 2.4.x, does not properly
    restrict anonymous access, which allows remote anonymous users to
    read hidden files via the path name.

- Vulnerability: CVE-2015-3183

  - CVSS Score: 5
  - Description: The chunked transfer coding implementation in the Apache HTTP
    Server before 2.4.14 does not properly parse chunk headers,
    which allows remote attackers to conduct HTTP request smuggling
    attacks via a crafted request, related to mishandling of large
    chunk-size values and invalid chunk-extension characters in
    modules/http/http_filters.c.

- Vulnerability: CVE-2013-4365

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function
    in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache
    HTTP Server allows remote attackers to have an unspecified impact via
    unknown vectors.

- Vulnerability: CVE-2018-5407

  - CVSS Score: 1.9
  - Description: Simultaneous Multi-threading (SMT) in processors can enable local
    users to exploit software vulnerable to timing attacks via a
    side-channel timing attack on 'port contention'.

- Vulnerability: CVE-2022-28330

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond
    bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2021-32791

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the
    Apache 2.x HTTP server that functions as an OpenID Connect Relying
    Party, authenticating users against an OpenID Connect Provider.
    In mod_auth_openidc before version 2.4.9, the AES GCM encryption in
    mod_auth_openidc uses a static IV and AAD. It is important to fix
    because this creates a static nonce and since aes-gcm is a stream
    cipher, this can lead to known cryptographic issues, since the same
    key is being reused. From 2.4.9 onwards this has been patched to use
    dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2021-32792

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the
    Apache 2.x HTTP server that functions as an OpenID Connect Relying
    Party, authenticating users against an OpenID Connect Provider. In
    mod_auth_openidc before version 2.4.9, there is an XSS vulnerability
    in when using 'OIDCPreservePost On'.

- Vulnerability: CVE-2024-38476

- CVSS Score: N/A
- Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- **Vulnerability: CVE-2024-38477**

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- **Vulnerability: CVE-2023-31122**

  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- **Vulnerability: CVE-2009-0796**

  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- **Vulnerability: CVE-2022-2068**

  - CVSS Score: 10
  - Description: In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze).

- **Vulnerability: CVE-2014-0118**

  - CVSS Score: 4.3
  - Description: The deflate_in_filter function in mod_deflate.c in the mod_deflate module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.

- **Vulnerability: CVE-2013-6438**

  - CVSS Score: 5

– Description: The dav_xml_get_cdata function in main/util.c in the mod_dav module
in the Apache HTTP Server before 2.4.8 does not properly remove
whitespace characters from CDATA sections, which allows remote
attackers to cause a denial of service (daemon crash) via a crafted
DAV WRITE request.

- Vulnerability: CVE-2020-1927

  – CVSS Score: 5.8
  – Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with
mod_rewrite that were intended to be self-referential might be fooled
by encoded newlines and redirect instead to an an unexpected URL
within the request URL.

- Vulnerability: CVE-2023-0286

  – CVSS Score: N/A
  – Description: There is a type confusion vulnerability relating to X.400 address
processinginside an X.509 GeneralName. X.400 addresses were
parsed as an ASN1_STRING butthe public structure definition for
GENERAL_NAME incorrectly specified the typeof the x400Address
field as ASN1_TYPE. This field is subsequently interpreted bythe
OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than
anASN1_STRING.When CRL checking is enabled (i.e. the application
sets theX509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an
attacker to passarbitrary pointers to a memcmp call, enabling them to
read memory contents orenact a denial of service. In most cases,
the attack requires the attacker toprovide both the certificate
chain and CRL, neither of which need to have avalid signature. If
the attacker only controls one of these inputs, the otherinput
must already contain an X.400 address as a CRL distribution point,
whichis uncommon. As such, this vulnerability is most likely to only
affectapplications which have implemented their own functionality for
retrieving CRLsover a network.

- Vulnerability: CVE-2023-3817

  – CVSS Score: N/A
  – Description: Issue summary: Checking excessively long DH keys or parameters may
be very slow.Impact summary: Applications that use the functions
DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH
key or DH parameters may experience longdelays. Where the key or
parameters that are being checked have been obtainedfrom an untrusted
source this may lead to a Denial of Service.The function DH_check()
performs various checks on DH parameters. After fixingCVE-2023-3446
it was discovered that a large q parameter value can also triggeran
overly long computation during some of these checks. A correct q
value,if present, cannot be larger than the modulus p parameter, thus
it isunnecessary to perform these checks if q is larger than p.An
application that calls DH_check() and supplies a key or parameters
obtainedfrom an untrusted source could be vulnerable to a Denial of
Service attack.The function DH_check() is itself called by a number
of other OpenSSL functions.An application calling any of those other
functions may similarly be affected.The other functions affected
by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable
are the OpenSSL dhparam and pkeyparam command line applicationswhen
using the "-check" option.The OpenSSL SSL/TLS implementation is not
affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not
affected by this issue.

- Vulnerability: CVE-2017-3167

– CVSS Score: 7.5

– Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.

- Vulnerability: CVE-2021-32786

  – CVSS Score: 5.8

  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, 'oidc_validate_redirect_url()' does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring 'mod_auth_openidc' to only allow redirection whose destination matches a given regular expression.

- Vulnerability: CVE-2021-32785

  – CVSS Score: 4.3

  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache ('OIDCCacheEncrypt off', 'OIDCSessionType server-cache', 'OIDCCacheType redis'), 'mod_auth_openidc' wrongly performed argument interpolation before passing Redis requests to 'hiredis', which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the 'hiredis' API. As a workaround, this vulnerability can be mitigated by setting 'OIDCCacheEncrypt' to 'on', as cache keys are cryptographically hashed before use when this option is enabled.

- Vulnerability: CVE-2007-4723

  – CVSS Score: 7.5

  – Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2021-44790

  – CVSS Score: 7.5

  – Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

- Vulnerability: CVE-2016-4975

  - CVSS Score: 4.3
  - Description: Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).

- Vulnerability: CVE-2020-13938

  - CVSS Score: 2.1
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

- Vulnerability: CVE-2023-2650

  - CVSS Score: N/A
  - Description: Issue summary: Processing some specially crafted ASN.1 object identifiers ordata containing them may be very slow.Impact summary: Applications that use OBJ_obj2txt() directly, or use any ofthe OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no messagesize limit may experience notable to very long delays when processing thosemessages, which may lead to a Denial of Service.An OBJECT IDENTIFIER is composed of a series of numbers - sub-identifiers -most of which have no size limit. OBJ_obj2txt() may be used to translatean ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSLtype ASN1_OBJECT) to its canonical numeric text form, which are thesub-identifiers of the OBJECT IDENTIFIER in decimal form, separated byperiods.When one of the sub-identifiers in the OBJECT IDENTIFIER is very large(these are sizes that are seen as absurdly large, taking up tens or hundredsof KiBs), the translation to a decimal number in text may take a very longtime. The time complexity is $O(n^2)$ with 'n' being the size of thesub-identifiers in bytes (*).With OpenSSL 3.0, support to fetch cryptographic algorithms using names /identifiers in string form was introduced. This includes using OBJECTIDENTIFIERs in canonical numeric text form as identifiers for fetchingalgorithms.Such OBJECT IDENTIFIERs may be received through the ASN.1 structureAlgorithmIdentifier, which is commonly used in multiple protocols to specifywhat cryptographic algorithm should be used to sign or verify, encrypt ordecrypt, or digest passed data.Applications that call OBJ_obj2txt() directly with untrusted data areaffected, with any version of OpenSSL. If the use is for the mere purposeof display, the severity is considered low.In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME,CMS, CMP/CRMF or TS. It also impacts anything that processes X.509certificates, including simple things like verifying its signature.The impact on TLS is relatively low, because all versions of OpenSSL have a100KiB limit on the peer's certificate chain. Additionally, this onlyimpacts clients, or servers that have explicitly enabled clientauthentication.In OpenSSL 1.1.1 and 1.0.2, this only affects displaying diverse objects,such as X.509 certificates. This is assumed to not happen in such a waythat it would cause a Denial of Service, so these versions are considerednot affected by this issue in such a way that it would be cause for concern,and the severity is therefore considered low.

- Vulnerability: CVE-2023-0215

  - CVSS Score: N/A

- Description: The public API function BIO_new_NDEF is a helper function used for streamingASN.1 data via a BIO. It is primarily used internally to OpenSSL to support theSMIME, CMS and PKCS7 streaming capabilities, but may also be called directly byend user applications.The function receives a BIO from the caller, prepends a new BIO_f_asn1 filterBIO onto the front of it to form a BIO chain, and then returns the new head ofthe BIO chain to the caller. Under certain conditions, for example if a CMSrecipient public key is invalid, the new filter BIO is freed and the functionreturns a NULL result indicating a failure. However, in this case, the BIO chainis not properly cleaned up and the BIO passed by the caller still retainsinternal pointers to the previously freed filter BIO. If the caller then goes onto call BIO_pop() on the BIO then a use-after-free will occur. This will mostlikely result in a crash.This scenario occurs directly in the internal function B64_write_ASN1() whichmay cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() onthe BIO. This internal function is in turn called by the public API functionsPEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream,SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7.Other public API functions that may be impacted by this includei2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream andi2d_PKCS7_bio_stream.The OpenSSL cms and smime command line applications are similarly affected.

- Vulnerability: CVE-2020-35452

  - CVSS Score: 6.8
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

- Vulnerability: CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2020-1934

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

- Vulnerability: CVE-2022-36760

  - CVSS Score: N/A
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-4304

  - CVSS Score: N/A

- Description: A timing based side channel exists in the OpenSSL RSA Decryption implementationwhich could be sufficient to recover a plaintext across a network in aBleichenbacher style attack. To achieve a successful decryption an attackerwould have to be able to send a very large number of trial messages fordecryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5,RSA-OEAP and RSASVE.For example, in a TLS connection, RSA is commonly used by a client to send anencrypted pre-master secret to the server. An attacker that had observed agenuine connection between a client and a server could use this flaw to sendtrial messages to the server and record the time taken to process them. After asufficiently large number of messages the attacker could recover the pre-mastersecret used for the original connection and thus be able to decrypt theapplication data sent over that connection.

- Vulnerability: CVE-2019-1563

  - CVSS Score: 4.3
  - Description: In situations where an attacker receives automated notification of the success or failure of a decryption attempt an attacker, after sending a very large number of messages to be decrypted, can recover a CMS/PKCS7 transported encryption key or decrypt any RSA encrypted message that was encrypted with the public RSA key, using a Bleichenbacher padding oracle attack. Applications are not affected if they use a certificate together with the private RSA key to the CMS_decrypt or PKCS7_decrypt functions to select the correct recipient info to decrypt. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).

- Vulnerability: CVE-2014-3523

  - CVSS Score: 5
  - Description: Memory leak in the winnt_accept function in server/mpm/winnt/child.c in the WinNT MPM in the Apache HTTP Server 2.4.x before 2.4.10 on Windows, when the default AcceptFilter is enabled, allows remote attackers to cause a denial of service (memory consumption) via crafted requests.

- Vulnerability: CVE-2013-5704

  - CVSS Score: 5
  - Description: The mod_headers module in the Apache HTTP Server 2.2.22 allows remote attackers to bypass "RequestHeader unset" directives by placing a header in the trailer portion of data sent with chunked transfer coding. NOTE: the vendor states "this is not a security issue in httpd as such."

- Vulnerability: CVE-2019-17567

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

- Vulnerability: CVE-2022-31813

  - CVSS Score: 7.5

- Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

- Vulnerability: CVE-2012-4360

  – CVSS Score: 4.3
  – Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2014-0231

  – CVSS Score: 5
  – Description: The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.

- Vulnerability: CVE-2021-26690

  – CVSS Score: 5
  – Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service

- Vulnerability: CVE-2021-26691

  – CVSS Score: 7.5
  – Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow

- Vulnerability: CVE-2019-0220

  – CVSS Score: 5
  – Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.

- Vulnerability: CVE-2022-30556

  – CVSS Score: 5
  – Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- Vulnerability: CVE-2021-39275

  – CVSS Score: 7.5
  – Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2014-3581

  – CVSS Score: 5

- Description: The cache_merge_headers_out function in modules/cache/cache_util.c
  in the mod_cache module in the Apache HTTP Server before 2.4.11
  allows remote attackers to cause a denial of service (NULL pointer
  dereference and application crash) via an empty HTTP Content-Type
  header.

- **Vulnerability: CVE-2016-0736**

  - CVSS Score: 5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.23, mod_session_crypto was
    encrypting its data/cookie using the configured ciphers with possibly
    either CBC or ECB modes of operation (AES256-CBC by default), hence
    no selectable or builtin authenticated encryption. This made it
    vulnerable to padding oracle attacks, particularly with CBC.

- **Vulnerability: CVE-2022-29404**

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a
    lua script that calls r:parsebody(0) may cause a denial of service
    due to no default limit on possible input size.

- **Vulnerability: CVE-2018-1312**

  - CVSS Score: 6.8
  - Description: In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest
    authentication challenge, the nonce sent to prevent reply attacks
    was not correctly generated using a pseudo-random seed. In a cluster
    of servers using a common Digest authentication configuration, HTTP
    requests could be replayed across servers by an attacker without
    detection.

- **Vulnerability: CVE-2006-20001**

  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or
    write of a single zero byte, in a pool (heap) memory location beyond
    the header value sent. This could cause the process to crash.This
    issue affects Apache HTTP Server 2.4.54 and earlier.

- **Vulnerability: CVE-2017-15710**

  - CVSS Score: 5
  - Description: In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to
    2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig,
    uses the Accept-Language header value to lookup the right charset
    encoding when verifying the user's credentials. If the header value
    is not present in the charset conversion table, a fallback mechanism
    is used to truncate it to a two characters value to allow a quick
    retry (for example, 'en-US' is truncated to 'en'). A header value of
    less than two characters forces an out of bound write of one NUL byte
    to a memory location that is not part of the string. In the worst
    case, quite unlikely, the process would crash which could be used as
    a Denial of Service attack. In the more likely case, this memory is
    already reserved for future use and the issue has no effect at all.

- **Vulnerability: CVE-2014-0226**

  - CVSS Score: 6.8

- Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

- **Vulnerability:** CVE-2024-0727

  - CVSS Score: N/A

  - Description: Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSLto crash leading to a potential Denial of Service attackImpact summary: Applications loading files in the PKCS12 format from untrustedsources might terminate abruptly.A file in PKCS12 format can contain certificates and keys and may come from anuntrusted source. The PKCS12 specification allows certain fields to be NULL, butOpenSSL does not correctly check for this case. This can lead to a NULL pointerdereference that results in OpenSSL crashing. If an application processes PKCS12files from an untrusted source using the OpenSSL APIs then that application willbe vulnerable to this issue.OpenSSL APIs that are vulnerable to this are: PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a similar issue in SMIME_write_PKCS7(). However since thisfunction is related to writing data we do not consider it security significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.

- **Vulnerability:** CVE-2009-3766

  - CVSS Score: 6.8

  - Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when OpenSSL is used, does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

- **Vulnerability:** CVE-2009-3767

  - CVSS Score: 4.3

  - Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other versions, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- **Vulnerability:** CVE-2009-3765

  - CVSS Score: 6.8

  - Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- **Vulnerability:** CVE-2022-22721

  - CVSS Score: 5.8

- Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- **Vulnerability:** CVE-2022-22720

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- **Vulnerability:** CVE-2019-10092

  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

- **Vulnerability:** CVE-2021-3712

  - CVSS Score: 5.8
  - Description: ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own "d2i" functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the "data" and "length" fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the "data" field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). It can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y).

- **Vulnerability:** CVE-2023-0464

- CVSS Score: N/A
- Description: A security vulnerability has been identified in all supported versionsof OpenSSL related to the verification of X.509 certificate chainsthat include policy constraints. Attackers may be able to exploit thisvulnerability by creating a malicious certificate chain that triggersexponential use of computational resources, leading to a denial-of-service(DoS) attack on affected systems.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0465

  - CVSS Score: N/A
  - Description: Applications that use a non-default option when verifying certificates may bevulnerable to an attack from a malicious CA to circumvent certain checks.Invalid certificate policies in leaf certificates are silently ignored byOpenSSL and other certificate policy checks are skipped for that certificate.A malicious CA could use this to deliberately assert invalid certificate policiesin order to circumvent policy checking on the certificate altogether.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0466

  - CVSS Score: N/A
  - Description: The function X509_VERIFY_PARAM_add0_policy() is documented toimplicitly enable the certificate policy check when doing certificateverification. However the implementation of the function does notenable the check which allows certificates with invalid or incorrectpolicies to pass the certificate verification.As suddenly enabling the policy check could break existing deployments it wasdecided to keep the existing behavior of the X509_VERIFY_PARAM_add0_policy()function.Instead the applications that require OpenSSL to perform certificatepolicy check need to use X509_VERIFY_PARAM_set1_policies() or explicitlyenable the policy check by calling X509_VERIFY_PARAM_set_flags() withthe X509_V_FLAG_POLICY_CHECK flag argument.Certificate policy checks are disabled by default in OpenSSL and are notcommonly used by applications.

- Vulnerability: CVE-2019-10098

  - CVSS Score: 5.8
  - Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.

- Vulnerability: CVE-2015-0228

  - CVSS Score: 5
  - Description: The lua_websocket_read function in lua_request.c in the mod_lua module in the Apache HTTP Server through 2.4.12 allows remote attackers to cause a denial of service (child-process crash) by sending a crafted WebSocket Ping frame after a Lua script has called the wsupgrade function.

- Vulnerability: CVE-2016-5387

- CVSS Score: 6.8
- Description: The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.

- Vulnerability: CVE-2017-15715

  - CVSS Score: 6.8
  - Description: In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.

- Vulnerability: CVE-2021-40438

  - CVSS Score: 6.8
  - Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2022-23943

  - CVSS Score: 7.5
  - Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

- Vulnerability: CVE-2018-17199

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

- Vulnerability: CVE-2021-23841

  - CVSS Score: 4.3

- Description: The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack. The function X509_issuer_and_serial_hash() is never directly called by OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on certificates that may have been obtained from untrusted sources. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2018-1301

  - CVSS Score: 4.3
  - Description: A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.

- Vulnerability: CVE-2018-1302

  - CVSS Score: 4.3
  - Description: When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.

- Vulnerability: CVE-2018-1303

  - CVSS Score: 5
  - Description: A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache. The vulnerability is considered as low risk since mod_cache_socache is not widely used, mod_cache_disk is not concerned by this vulnerability.

- Vulnerability: CVE-2021-34798

  - CVSS Score: 5
  - Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2023-25690

  - CVSS Score: N/A

- Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2020-11985

  - CVSS Score: 4.3
  - Description: IP address spoofing when proxying using mod_remoteip and mod_rewrite For configurations using proxying with mod_remoteip and certain mod_rewrite rules, an attacker could spoof their IP address for logging and PHP scripts. Note this issue was fixed in Apache HTTP Server 2.4.24 but was retrospectively allocated a low severity CVE in 2020.

- Vulnerability: CVE-2021-4160

  - CVSS Score: 4.3
  - Description: There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that is available to premium support customers only. It will be made available in 1.0.2zc when it is released. The issue only affects OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0). Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL 1.0.2zc-dev (Affected 1.0.2-1.0.2zb).

- Vulnerability: CVE-2013-4352

  - CVSS Score: 4.3
  - Description: The cache_invalidate function in modules/cache/cache_storage.c in the mod_cache module in the Apache HTTP Server 2.4.6, when a caching forward proxy is enabled, allows remote HTTP servers to cause a denial of service (NULL pointer dereference and daemon crash) via vectors that trigger a missing hostname value.

- Vulnerability: CVE-2022-26377

  - CVSS Score: 5

– Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

• Vulnerability: CVE-2014-0098

– CVSS Score: 5

– Description: The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.

• Vulnerability: CVE-2016-8743

– CVSS Score: 5

– Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

• Vulnerability: CVE-2024-40898

– CVSS Score: N/A

– Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

• Vulnerability: CVE-2024-38474

– CVSS Score: N/A

– Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

• Vulnerability: CVE-2022-0778

– CVSS Score: 5

– Description: The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - TLS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

• Vulnerability: CVE-2020-1971

  – CVSS Score: 4.3

- Description: The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s_server, s_client and verify tools have support for the "-crl_download" option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue. Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w).

- Vulnerability: CVE-2009-1390

  - CVSS Score: 6.8
  - Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2) GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS certificate in the chain is accepted instead of verifying the entire chain, which allows remote attackers to spoof trusted servers via a man-in-the-middle attack.

- Vulnerability: CVE-2012-3526

  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2023-5678

  - CVSS Score: N/A

- Description: Issue summary: Generating excessively long X9.42 DH keys or checkingexcessively long X9.42 DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_generate_key() togenerate an X9.42 DH key may experience long delays. Likewise, applicationsthat use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check()to check an X9.42 DH key or X9.42 DH parameters may experience long delays.Where the key or parameters that are being checked have been obtained froman untrusted source this may lead to a Denial of Service.While DH_check() performs all the necessary checks (as of CVE-2023-3817),DH_check_pub_key() doesn't make any of these checks, and is thereforevulnerable for excessively large P and Q parameters.Likewise, while DH_generate_key() performs a check for an excessively largeP, it doesn't check for an excessively large Q.An application that calls DH_generate_key() or DH_check_pub_key() andsupplies a key or parameters obtained from an untrusted source could bevulnerable to a Denial of Service attack.DH_generate_key() and DH_check_pub_key() are also called by a number ofother OpenSSL functions. An application calling any of those otherfunctions may similarly be affected. The other functions affected by thisare DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate().Also vulnerable are the OpenSSL pkey command line application when using the"-pubcheck" option, as well as the OpenSSL genpkey command line application.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2017-3736
  - CVSS Score: 4
  - Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

- Vulnerability: CVE-2017-3737
  - CVSS Score: 4.3

– Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error
state" mechanism. The intent was that if a fatal error occurred
during a handshake then OpenSSL would move into the error state and
would immediately fail if you attempted to continue the handshake.
This works as designed for the explicit handshake functions
(SSL_do_handshake(), SSL_accept() and SSL_connect()), however due
to a bug it does not work correctly if SSL_read() or SSL_write()
is called directly. In that scenario, if the handshake fails then
a fatal error will be returned in the initial function call. If
SSL_read()/SSL_write() is subsequently called by the application
for the same SSL object then it will succeed and the data is passed
without being decrypted/encrypted directly from the SSL/TLS record
layer. In order to exploit this issue an application bug would have
to be present that resulted in a call to SSL_read()/SSL_write() being
issued after having already received a fatal error. OpenSSL version
1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0
is not affected.

• Vulnerability: CVE-2019-1547

– CVSS Score: 1.9

– Description: Normally in OpenSSL EC groups always have a co-factor present and
this is used in side channel resistant code paths. However, in some
cases, it is possible to construct a group using explicit parameters
(instead of using a named curve). In those cases it is possible
that such a group does not have the cofactor present. This can occur
even where all the parameters match a known named curve. If such a
curve is used then OpenSSL falls back to non-side channel resistant
code paths which may result in full key recovery during an ECDSA
signature operation. In order to be vulnerable an attacker would
have to have the ability to time the creation of a large number of
signatures where explicit parameters with no co-factor present are
in use by an application using libcrypto. For the avoidance of doubt
libssl is not vulnerable because explicit parameters are never used.
Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL
1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected
1.0.2-1.0.2s).

• Vulnerability: CVE-2017-3735

– CVSS Score: 5

– Description: While parsing an IPAddressFamily extension in an X.509 certificate,
it is possible to do a one-byte overread. This would result in an
incorrect text display of the certificate. This bug has been present
since 2006 and is present in all versions of OpenSSL before 1.0.2m
and 1.1.0g.

• Vulnerability: CVE-2009-2299

– CVSS Score: 5

– Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module
before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before
3.1.1-11637, a module for the Apache HTTP Server, allows remote
attackers to cause a denial of service (memory consumption) via an
HTTP request with a large Content-Length value but no POST data.

• Vulnerability: CVE-2022-1292

– CVSS Score: 10

- Description: The c_rehash script does not properly sanitise shell metacharacters
  to prevent command injection. This script is distributed by
  some operating systems in a manner where it is automatically
  executed. On such operating systems, an attacker could execute
  arbitrary commands with the privileges of the script. Use of the
  c_rehash script is considered obsolete and should be replaced by the
  OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected
  3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n).
  Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).

- Vulnerability: CVE-2017-3738

  - CVSS Score: 4.3
  - Description: There is an overflow bug in the AVX2 Montgomery multiplication
    procedure used in exponentiation with 1024-bit moduli. No EC
    algorithms are affected. Analysis suggests that attacks against
    RSA and DSA as a result of this defect would be very difficult to
    perform and are not believed likely. Attacks against DH1024 are
    considered just feasible, because most of the work necessary to
    deduce information about a private key may be performed offline. The
    amount of resources required for such an attack would be significant.
    However, for an attack on TLS to be meaningful, the server would have
    to share the DH1024 private key among multiple clients, which is no
    longer an option since CVE-2016-0701. This only affects processors
    that support the AVX2 but not ADX extensions like Intel Haswell
    (4th generation). Note: The impact from this issue is similar to
    CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version
    1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n.
    Due to the low severity of this issue we are not issuing a new
    release of OpenSSL 1.1.0 at this time. The fix will be included in
    OpenSSL 1.1.0h when it becomes available. The fix is also available
    in commit e502cc86d in the OpenSSL git repository.

- Vulnerability: CVE-2012-4001

  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server
    does not properly verify its host name, which allows remote attackers
    to trigger HTTP requests to arbitrary hosts via unspecified vectors,
    as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2022-37436

  - CVSS Score: N/A
  - Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause
    the response headers to be truncated early, resulting in some headers
    being incorporated into the response body. If the later headers have
    any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2021-23840

  - CVSS Score: 5

- Description: Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissable length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2018-0737

  - CVSS Score: 4.3
  - Description: The OpenSSL RSA Key generation algorithm has been shown to be vulnerable to a cache timing side channel attack. An attacker with sufficient access to mount cache timing attacks during the RSA key generation process could recover the private key. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2b-1.0.2o).

- Vulnerability: CVE-2018-0734

  - CVSS Score: 4.3
  - Description: The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.1a (Affected 1.1.1). Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.0.2q (Affected 1.0.2-1.0.2p).

- Vulnerability: CVE-2018-0732

  - CVSS Score: 5
  - Description: During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime value to the client. This will cause the client to spend an unreasonably long period of time generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2-1.0.2o).

- Vulnerability: CVE-2017-9788

  - CVSS Score: 6.4
  - Description: In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.

- Vulnerability: CVE-2018-0739

  - CVSS Score: 4.3

- Description: Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o (Affected 1.0.2b-1.0.2n).

- Vulnerability: CVE-2014-8109

  - CVSS Score: 4.3
  - Description: mod_lua.c in the mod_lua module in the Apache HTTP Server 2.3.x and 2.4.x through 2.4.10 does not support an httpd configuration in which the same Lua authorization provider is used with different arguments within different contexts, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives, as demonstrated by a configuration that specifies authorization for one group to access a certain directory, and authorization for a second group to access a second directory.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2016-2161

  - CVSS Score: 5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.23, malicious input to mod_auth_digest can cause the server to crash, and each instance continues to crash even for subsequently valid requests.

- Vulnerability: CVE-2016-8612

  - CVSS Score: 3.3
  - Description: Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.

- Vulnerability: CVE-2019-1552

  - CVSS Score: 1.9

- Description: OpenSSL has internal defaults for a directory tree where it
  can find a configuration file as well as certificates used for
  verification in TLS. This directory is most commonly referred to
  as OPENSSLDIR, and is configurable with the --prefix / --openssldir
  configuration options. For OpenSSL versions 1.1.0 and 1.1.1, the
  mingw configuration targets assume that resulting programs and
  libraries are installed in a Unix-like environment and the default
  prefix for program installation as well as for OPENSSLDIR should be
  '/usr/local'. However, mingw programs are Windows programs, and as
  such, find themselves looking at sub-directories of 'C:/usr/local',
  which may be world writable, which enables untrusted users to modify
  OpenSSL's default configuration, insert CA certificates, modify (or
  even replace) existing engine modules, etc. For OpenSSL 1.0.2,
  '/usr/local/ssl' is used as default for OPENSSLDIR on all Unix and
  Windows targets, including Visual C builds. However, some build
  instructions for the diverse Windows targets on 1.0.2 encourage
  you to specify your own --prefix. OpenSSL versions 1.1.1, 1.1.0
  and 1.0.2 are affected by this issue. Due to the limited scope
  of affected deployments this has been assessed as low severity and
  therefore we are not creating new releases at this time. Fixed
  in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL
  1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected
  1.0.2-1.0.2s).

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5
    for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM
    Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows
    use an improper encryption algorithm and a weak key for maintaining
    the stored data of the node secret for the SecurID Authentication
    API, which allows local users to obtain sensitive information via
    cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication
    Agent 7.1 before 7.1.1 for Web for Internet Information Services,
    and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to
    inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2019-1551

  - CVSS Score: 5
  - Description: There is an overflow bug in the x64_64 Montgomery squaring procedure
    used in exponentiation with 512-bit moduli. No EC algorithms are
    affected. Analysis suggests that attacks against 2-prime RSA1024,
    3-prime RSA1536, and DSA1024 as a result of this defect would be
    very difficult to perform and are not believed likely. Attacks
    against DH512 are considered just feasible. However, for an attack
    the target would have to re-use the DH512 private key, which is not
    recommended anyway. Also applications directly using the low level
    API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME. Fixed
    in OpenSSL 1.1.1e (Affected 1.1.1-1.1.1d). Fixed in OpenSSL 1.0.2u
    (Affected 1.0.2-1.0.2t).

- Vulnerability: CVE-2019-1559

  - CVSS Score: 4.3

- Description: If an application encounters a fatal protocol error and then calls
  SSL_shutdown() twice (once to send a close_notify, and once to
  receive one) then OpenSSL can respond differently to the calling
  application if a 0 byte record is received with invalid padding
  compared to if a 0 byte record is received with an invalid MAC. If
  the application then behaves differently based on that in a way that
  is detectable to the remote peer, then this amounts to a padding
  oracle that could be used to decrypt data. In order for this to be
  exploitable "non-stitched" ciphersuites must be in use. Stitched
  ciphersuites are optimised implementations of certain commonly
  used ciphersuites. Also the application must call SSL_shutdown()
  twice even if a protocol error has occurred (applications should
  not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected
  1.0.2-1.0.2q).

- Vulnerability: CVE-2023-45802

  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a
    time window were the request's memory resources were not reclaimed
    immediately. Instead, de-allocation was deferred to connection
    close. A client could send new requests and resets, keeping the
    connection busy and open and causing the memory footprint to keep
    on growing. On connection close, all resources were reclaimed, but
    the process might run out of memory before that.This was found by
    the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset
    Exploit) with their own test client. During "normal" HTTP/2 use, the
    probability to hit this bug is very low. The kept memory would not
    become noticeable before the connection closes or times out.Users are
    recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2018-1283

  - CVSS Score: 3.5
  - Description: In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to
    forward its session data to CGI applications (SessionEnv on, not
    the default), a remote user may influence their content by using a
    "Session" header. This comes from the "HTTP_SESSION" variable name
    used by mod_session to forward its data to CGIs, since the prefix
    "HTTP_" is also used by the Apache HTTP Server to pass HTTP header
    fields, per CGI specifications.

- Vulnerability: CVE-2020-1968

  - CVSS Score: 4.3
  - Description: The Raccoon attack exploits a flaw in the TLS specification which
    can lead to an attacker being able to compute the pre-master
    secret in connections which have used a Diffie-Hellman (DH) based
    ciphersuite. In such a case this would result in the attacker being
    able to eavesdrop on all encrypted communications sent over that TLS
    connection. The attack can only be exploited if an implementation
    re-uses a DH secret across multiple TLS connections. Note that this
    issue only impacts DH ciphersuites and not ECDH ciphersuites. This
    issue affects OpenSSL 1.0.2 which is out of support and no longer
    receiving public updates. OpenSSL 1.1.1 is not vulnerable to this
    issue. Fixed in OpenSSL 1.0.2w (Affected 1.0.2-1.0.2v).

- Vulnerability: CVE-2019-0217

  - CVSS Score: 6

– Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition
            in mod_auth_digest when running in a threaded server could allow a
            user with valid credentials to authenticate using another username,
            bypassing configured access control restrictions.

- Vulnerability: CVE-2022-28615

  – CVSS Score: 6.4
  – Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose
            information due to a read beyond bounds in ap_strcmp_match() when
            provided with an extremely large input buffer. While no code
            distributed with the server can be coerced into such a call,
            third-party modules or lua scripts that use ap_strcmp_match() may
            hypothetically be affected.

- Vulnerability: CVE-2022-28614

  – CVSS Score: 5
  – Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier
            may read unintended memory if an attacker can cause the server to
            reflect very large input using ap_rwrite() or ap_rputs(), such as
            with mod_luas r:puts() function. Modules compiled and distributed
            separately from Apache HTTP Server that use the 'ap_rputs' function
            and may pass it a very large (INT_MAX or larger) string must be
            compiled against current headers to resolve the issue.

- Vulnerability: CVE-2020-7041

  – CVSS Score: 5
  – Description: An issue was discovered in openfortivpn 1.11.0 when used with OpenSSL
            1.0.2 or later. tunnel.c mishandles certificate validation because
            an X509_check_host negative error code is interpreted as a successful
            return value.

- Vulnerability: CVE-2015-3196

  – CVSS Score: 4.3
  – Description: ssl/s3_clnt.c in OpenSSL 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1p,
            and 1.0.2 before 1.0.2d, when used for a multi-threaded client,
            writes the PSK identity hint to an incorrect data structure, which
            allows remote servers to cause a denial of service (race condition
            and double free) via a crafted ServerKeyExchange message.

- Vulnerability: CVE-2009-3765

  – CVSS Score: 6.8
  – Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does
            not properly handle a '\{}0' character in a domain name in the
            subject's Common Name (CN) field of an X.509 certificate, which
            allows man-in-the-middle attackers to spoof arbitrary SSL servers via
            a crafted certificate issued by a legitimate Certification Authority,
            a related issue to CVE-2009-2408.

- Vulnerability: CVE-2012-0027

  – CVSS Score: 5
  – Description: The GOST ENGINE in OpenSSL before 1.0.0f does not properly handle
            invalid parameters for the GOST block cipher, which allows remote
            attackers to cause a denial of service (daemon crash) via crafted
            data from a TLS client.

- Vulnerability: CVE-2011-4577

  – CVSS Score: 4.3

- Description: OpenSSL before 0.9.8s and 1.x before 1.0.0f, when RFC 3779
  support is enabled, allows remote attackers to cause a denial of
  service (assertion failure) via an X.509 certificate containing
  certificate-extension data associated with (1) IP address blocks
  or (2) Autonomous System (AS) identifiers.

- Vulnerability: CVE-2011-4576

  - CVSS Score: 5
  - Description: The SSL 3.0 implementation in OpenSSL before 0.9.8s and 1.x before
    1.0.0f does not properly initialize data structures for block cipher
    padding, which might allow remote attackers to obtain sensitive
    information by decrypting the padding data sent by an SSL peer.

- Vulnerability: CVE-2014-0076

  - CVSS Score: 1.9
  - Description: The Montgomery ladder implementation in OpenSSL through 1.0.0l
    does not ensure that certain swap operations have a constant-time
    behavior, which makes it easier for local users to obtain ECDSA
    nonces via a FLUSH+RELOAD cache side-channel attack.

- Vulnerability: CVE-2009-4355

  - CVSS Score: 5
  - Description: Memory leak in the zlib_stateful_finish function in
    crypto/comp/c_zlib.c in OpenSSL 0.9.8l and earlier and 1.0.0 Beta
    through Beta 4 allows remote attackers to cause a denial of service
    (memory consumption) via vectors that trigger incorrect calls to
    the CRYPTO_cleanup_all_ex_data function, as demonstrated by use
    of SSLv3 and PHP with the Apache HTTP Server, a related issue to
    CVE-2008-1678.

- Vulnerability: CVE-2012-2333

  - CVSS Score: 6.8
  - Description: Integer underflow in OpenSSL before 0.9.8x, 1.0.0 before 1.0.0j,
    and 1.0.1 before 1.0.1c, when TLS 1.1, TLS 1.2, or DTLS is used with
    CBC encryption, allows remote attackers to cause a denial of service
    (buffer over-read) or possibly have unspecified other impact via a
    crafted TLS packet that is not properly handled during a certain
    explicit IV calculation.

- Vulnerability: CVE-2011-1945

  - CVSS Score: 2.6
  - Description: The elliptic curve cryptography (ECC) subsystem in OpenSSL 1.0.0d
    and earlier, when the Elliptic Curve Digital Signature Algorithm
    (ECDSA) is used for the ECDHE_ECDSA cipher suite, does not properly
    implement curves over binary fields, which makes it easier for
    context-dependent attackers to determine private keys via a timing
    attack and a lattice calculation.

- Vulnerability: CVE-2014-3470

  - CVSS Score: 4.3
  - Description: The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL
    before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h, when an
    anonymous ECDH cipher suite is used, allows remote attackers to cause
    a denial of service (NULL pointer dereference and client crash) by
    triggering a NULL certificate value.

- Vulnerability: CVE-2015-1789

- CVSS Score: 4.3
- Description: The X509_cmp_time function in crypto/x509/x509_vfy.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted length field in ASN1_TIME data, as demonstrated by an attack against a server that supports client authentication with a custom verification callback.

- Vulnerability: CVE-2015-1788

  - CVSS Score: 4.3
  - Description: The BN_GF2m_mod_inv function in crypto/bn/bn_gf2m.c in OpenSSL before 0.9.8s, 1.0.0 before 1.0.0e, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b does not properly handle ECParameters structures in which the curve is over a malformed binary polynomial field, which allows remote attackers to cause a denial of service (infinite loop) via a session that uses an Elliptic Curve algorithm, as demonstrated by an attack against a server that supports client authentication.

- Vulnerability: CVE-2009-1390

  - CVSS Score: 6.8
  - Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2) GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS certificate in the chain is accepted instead of verifying the entire chain, which allows remote attackers to spoof trusted servers via a man-in-the-middle attack.

- Vulnerability: CVE-2010-4252

  - CVSS Score: 7.5
  - Description: OpenSSL before 1.0.0c, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol.

- Vulnerability: CVE-2014-8176

  - CVSS Score: 7.5
  - Description: The dtls1_clear_queues function in ssl/d1_lib.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h frees data structures without considering that application data can arrive between a ChangeCipherSpec message and a Finished message, which allows remote DTLS peers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unexpected application data.

- Vulnerability: CVE-2010-4180

  - CVSS Score: 4.3
  - Description: OpenSSL before 0.9.8q, and 1.0.x before 1.0.0c, when SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG is enabled, does not properly prevent modification of the ciphersuite in the session cache, which allows remote attackers to force the downgrade to an unintended cipher via vectors involving sniffing network traffic to discover a session identifier.

- Vulnerability: CVE-2011-4969

  - CVSS Score: 4.3

- Description: Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

- Vulnerability: CVE-2016-2176

  - CVSS Score: 6.4
  - Description: The X509_NAME_oneline function in crypto/x509/x509_obj.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to obtain sensitive information from process stack memory or cause a denial of service (buffer over-read) via crafted EBCDIC ASN.1 data.

- Vulnerability: CVE-2014-3505

  - CVSS Score: 5
  - Description: Double free vulnerability in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (application crash) via crafted DTLS packets that trigger an error condition.

- Vulnerability: CVE-2014-3506

  - CVSS Score: 5
  - Description: d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via crafted DTLS handshake messages that trigger memory allocations corresponding to large length values.

- Vulnerability: CVE-2014-3507

  - CVSS Score: 5
  - Description: Memory leak in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via zero-length DTLS fragments that trigger improper handling of the return value of a certain insert function.

- Vulnerability: CVE-2014-3566

  - CVSS Score: 4.3
  - Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

- Vulnerability: CVE-2014-3567

  - CVSS Score: 7.1
  - Description: Memory leak in the tls_decrypt_ticket function in t1_lib.c in OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted session ticket that triggers an integrity-check failure.

- Vulnerability: CVE-2017-3735

  - CVSS Score: 5
  - Description: While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL before 1.0.2m and 1.1.0g.

- Vulnerability: CVE-2013-6450

  - CVSS Score: 5.8
  - Description: The DTLS retransmission implementation in OpenSSL 1.0.0 before 1.0.0l and 1.0.1 before 1.0.1f does not properly maintain data structures for digest and encryption contexts, which might allow man-in-the-middle attackers to trigger the use of a different context and cause a denial of service (application crash) by interfering with packet delivery, related to ssl/d1_both.c and ssl/t1_enc.c.

- Vulnerability: CVE-2010-3864

  - CVSS Score: 7.6
  - Description: Multiple race conditions in ssl/t1_lib.c in OpenSSL 0.9.8f through 0.9.8o, 1.0.0, and 1.0.0a, when multi-threading and internal caching are enabled on a TLS server, might allow remote attackers to execute arbitrary code via client data that triggers a heap-based buffer overflow, related to (1) the TLS server name extension and (2) elliptic curve cryptography.

- Vulnerability: CVE-2014-3568

  - CVSS Score: 4.3
  - Description: OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j does not properly enforce the no-ssl3 build option, which allows remote attackers to bypass intended access restrictions via an SSL 3.0 handshake, related to s23_clnt.c and s23_srvr.c.

- Vulnerability: CVE-2011-3207

  - CVSS Score: 5
  - Description: crypto/x509/x509_vfy.c in OpenSSL 1.0.x before 1.0.0e does not initialize certain structure members, which makes it easier for remote attackers to bypass CRL validation by using a nextUpdate value corresponding to a time in the past.

- Vulnerability: CVE-2014-3508

  - CVSS Score: 4.3
  - Description: The OBJ_obj2txt function in crypto/objects/obj_dat.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i, when pretty printing is used, does not ensure the presence of '\{}0' characters, which allows context-dependent attackers to obtain sensitive information from process stack memory by reading output from X509_name_oneline, X509_name_print_ex, and unspecified other functions.

- Vulnerability: CVE-2014-3509

  - CVSS Score: 6.8
  - Description: Race condition in the ssl_parse_serverhello_tlsext function in t1_lib.c in OpenSSL 1.0.0 before 1.0.0n and 1.0.1 before 1.0.1i, when multithreading and session resumption are used, allows remote SSL servers to cause a denial of service (memory overwrite and client application crash) or possibly have unspecified other impact by sending Elliptic Curve (EC) Supported Point Formats Extension data.

- Vulnerability: CVE-2015-3195

  - CVSS Score: 5

- Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.

- Vulnerability: CVE-2015-0292

  - CVSS Score: 7.5
  - Description: Integer underflow in the EVP_DecodeUpdate function in crypto/evp/encode.c in the base64-decoding implementation in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted base64 data that triggers a buffer overflow.

- Vulnerability: CVE-2015-0293

  - CVSS Score: 5
  - Description: The SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a allows remote attackers to cause a denial of service (s2_lib.c assertion failure and daemon exit) via a crafted CLIENT-MASTER-KEY message.

- Vulnerability: CVE-2011-4108

  - CVSS Score: 4.3
  - Description: The DTLS implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f performs a MAC check only if certain padding is valid, which makes it easier for remote attackers to recover plaintext via a padding oracle attack.

- Vulnerability: CVE-2012-1165

  - CVSS Score: 5
  - Description: The mime_param_cmp function in crypto/asn1/asn_mime.c in OpenSSL before 0.9.8u and 1.x before 1.0.0h allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted S/MIME message, a different vulnerability than CVE-2006-7250.

- Vulnerability: CVE-2011-0014

  - CVSS Score: 5
  - Description: ssl/t1_lib.c in OpenSSL 0.9.8h through 0.9.8q and 1.0.0 through 1.0.0c allows remote attackers to cause a denial of service (crash), and possibly obtain sensitive information in applications that use OpenSSL, via a malformed ClientHello handshake message that triggers an out-of-bounds memory access, aka "OCSP stapling vulnerability."

- Vulnerability: CVE-2020-7656

  - CVSS Score: 4.3
  - Description: jquery prior to 1.9.0 allows Cross-site Scripting attacks via the load method. The load method fails to recognize and remove "<script>" HTML tags that contain a whitespace character, i.e: "</script >", which results in the enclosed script logic to be executed.

- Vulnerability: CVE-2014-3510

  - CVSS Score: 4.3

- Description: The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote DTLS servers to cause a denial of service (NULL pointer dereference and client application crash) via a crafted handshake message in conjunction with a (1) anonymous DH or (2) anonymous ECDH ciphersuite.

- Vulnerability: CVE-2015-9251

  - CVSS Score: 4.3
  - Description: jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.

- Vulnerability: CVE-2011-4619

  - CVSS Score: 5
  - Description: The Server Gated Cryptography (SGC) implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly handle handshake restarts, which allows remote attackers to cause a denial of service (CPU consumption) via unspecified vectors.

- Vulnerability: CVE-2020-11022

  - CVSS Score: 4.3
  - Description: In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

- Vulnerability: CVE-2020-11023

  - CVSS Score: 4.3
  - Description: In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

- Vulnerability: CVE-2010-5298

  - CVSS Score: 4
  - Description: Race condition in the ssl3_read_bytes function in s3_pkt.c in OpenSSL through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, allows remote attackers to inject data across sessions or cause a denial of service (use-after-free and parsing error) via an SSL connection in a multithreaded environment.

- Vulnerability: CVE-2014-0221

  - CVSS Score: 4.3
  - Description: The dtls1_get_message_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (recursion and client crash) via a DTLS hello message in an invalid DTLS handshake.

- Vulnerability: CVE-2011-3210

  - CVSS Score: 5

- Description: The ephemeral ECDH ciphersuite functionality in OpenSSL 0.9.8 through 0.9.8r and 1.0.x before 1.0.0e does not ensure thread safety during processing of handshake messages from clients, which allows remote attackers to cause a denial of service (daemon crash) via out-of-order messages that violate the TLS protocol.

- **Vulnerability:** CVE-2012-6708

  - CVSS Score: 4.3
  - Description: jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

- **Vulnerability:** CVE-2010-0742

  - CVSS Score: 7.5
  - Description: The Cryptographic Message Syntax (CMS) implementation in crypto/cms/cms_asn1.c in OpenSSL before 0.9.8o and 1.x before 1.0.0a does not properly handle structures that contain OriginatorInfo, which allows context-dependent attackers to modify invalid memory locations or conduct double-free attacks, and possibly execute arbitrary code, via unspecified vectors.

- **Vulnerability:** CVE-2010-1633

  - CVSS Score: 6.4
  - Description: RSA verification recovery in the EVP_PKEY_verify_recover function in OpenSSL 1.x before 1.0.0a, as used by pkeyutl and possibly other applications, returns uninitialized memory upon failure, which might allow context-dependent attackers to bypass intended key requirements or obtain sensitive information via unspecified vectors. NOTE: some of these details are obtained from third party information.

- **Vulnerability:** CVE-2015-0209

  - CVSS Score: 6.8
  - Description: Use-after-free vulnerability in the d2i_ECPrivateKey function in crypto/ec/ec_asn1.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via a malformed Elliptic Curve (EC) private-key file that is improperly handled during import.

- **Vulnerability:** CVE-2013-0166

  - CVSS Score: 5
  - Description: OpenSSL before 0.9.8y, 1.0.0 before 1.0.0k, and 1.0.1 before 1.0.1d does not properly perform signature verification for OCSP responses, which allows remote OCSP servers to cause a denial of service (NULL pointer dereference and application crash) via an invalid key.

- **Vulnerability:** CVE-2016-0703

  - CVSS Score: 4.3

- Description: The get_client_master_key function in s2_srvr.c in the SSLv2
  implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r,
  1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero
  CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher,
  which allows man-in-the-middle attackers to determine the MASTER-KEY
  value and decrypt TLS ciphertext data by leveraging a Bleichenbacher
  RSA padding oracle, a related issue to CVE-2016-0800.

- Vulnerability: CVE-2015-1790

  - CVSS Score: 5
  - Description: The PKCS7_dataDecodefunction in crypto/pkcs7/pk7_doit.c in OpenSSL
    before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2
    before 1.0.2b allows remote attackers to cause a denial of service
    (NULL pointer dereference and application crash) via a PKCS#7 blob
    that uses ASN.1 encoding and lacks inner EncryptedContent data.

- Vulnerability: CVE-2016-0704

  - CVSS Score: 4.3
  - Description: An oracle protection mechanism in the get_client_master_key function
    in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf,
    1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a
    overwrites incorrect MASTER-KEY bytes during use of export cipher
    suites, which makes it easier for remote attackers to decrypt TLS
    ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a
    related issue to CVE-2016-0800.

- Vulnerability: CVE-2015-1792

  - CVSS Score: 5
  - Description: The do_free_upto function in crypto/cms/cms_smime.c in OpenSSL before
    0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before
    1.0.2b allows remote attackers to cause a denial of service (infinite
    loop) via vectors that trigger a NULL value of a BIO data structure,
    as demonstrated by an unrecognized X.660 OID for a hash function.

- Vulnerability: CVE-2021-4044

  - CVSS Score: 5
  - Description: Internally libssl in OpenSSL calls X509_verify_cert() on the client
    side to verify a certificate supplied by a server. That function
    may return a negative return value to indicate an internal error (for
    example out of memory). Such a negative return value is mishandled
    by OpenSSL and will cause an IO function (such as SSL_connect() or
    SSL_do_handshake()) to not indicate success and a subsequent call
    to SSL_get_error() to return the value SSL_ERROR_WANT_RETRY_VERIFY.
    This return value is only supposed to be returned by OpenSSL if the
    application has previously called SSL_CTX_set_cert_verify_callback().
    Since most applications do not do this the SSL_ERROR_WANT_RETRY_VERIFY
    return value from SSL_get_error() will be totally unexpected and
    applications may not behave correctly as a result. The exact
    behaviour will depend on the application but it could result in
    crashes, infinite loops or other similar incorrect responses. This
    issue is made more serious in combination with a separate bug in
    OpenSSL 3.0 that will cause X509_verify_cert() to indicate an internal
    error when processing a certificate chain. This will occur where a
    certificate does not include the Subject Alternative Name extension
    but where a Certificate Authority has enforced name constraints.
    This issue can occur even with valid chains. By combining the two
    issues an attacker could induce incorrect, application dependent
    behaviour. Fixed in OpenSSL 3.0.1 (Affected 3.0.0).

- Vulnerability: CVE-2014-0224

  - CVSS Score: 5.8
  - Description: OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability.

- Vulnerability: CVE-2012-2110

  - CVSS Score: 7.5
  - Description: The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in OpenSSL before 0.9.8v, 1.0.0 before 1.0.0i, and 1.0.1 before 1.0.1a does not properly interpret integer data, which allows remote attackers to conduct buffer overflow attacks, and cause a denial of service (memory corruption) or possibly have unspecified other impact, via crafted DER data, as demonstrated by an X.509 certificate or an RSA public key.

- Vulnerability: CVE-2013-0169

  - CVSS Score: 2.6
  - Description: The TLS protocol 1.1 and 1.2 and the DTLS protocol 1.0 and 1.2, as used in OpenSSL, OpenJDK, PolarSSL, and other products, do not properly consider timing side-channel attacks on a MAC check requirement during the processing of malformed CBC padding, which allows remote attackers to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, aka the "Lucky Thirteen" issue.

- Vulnerability: CVE-2009-3767

  - CVSS Score: 4.3
  - Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other versions, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2012-0884

  - CVSS Score: 5
  - Description: The implementation of Cryptographic Message Syntax (CMS) and PKCS #7 in OpenSSL before 0.9.8u and 1.x before 1.0.0h does not properly restrict certain oracle behavior, which makes it easier for context-dependent attackers to decrypt data via a Million Message Attack (MMA) adaptive chosen ciphertext attack.

- Vulnerability: CVE-2015-4000

  - CVSS Score: 4.3
  - Description: The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the "Logjam" issue.

- Vulnerability: CVE-2014-0198

- CVSS Score: 4.3
- Description: The do_ssl3_write function in s3_pkt.c in OpenSSL 1.x through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, does not properly manage a buffer pointer during certain recursive calls, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via vectors that trigger an alert condition.

- Vulnerability: CVE-2016-2109

  - CVSS Score: 7.8
  - Description: The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in the ASN.1 BIO implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (memory consumption) via a short invalid encoding.

- Vulnerability: CVE-2016-2108

  - CVSS Score: 10
  - Description: The ASN.1 implementation in OpenSSL before 1.0.1o and 1.0.2 before 1.0.2c allows remote attackers to execute arbitrary code or cause a denial of service (buffer underflow and memory corruption) via an ANY field in crafted serialized data, aka the "negative zero" issue.

- Vulnerability: CVE-2013-6449

  - CVSS Score: 4.3
  - Description: The ssl_get_algorithm2 function in ssl/s3_lib.c in OpenSSL before 1.0.2 obtains a certain version number from an incorrect data structure, which allows remote attackers to cause a denial of service (daemon crash) via crafted traffic from a TLS 1.2 client.

- Vulnerability: CVE-2020-7042

  - CVSS Score: 5
  - Description: An issue was discovered in openfortivpn 1.11.0 when used with OpenSSL 1.0.2 or later. tunnel.c mishandles certificate validation because the hostname check operates on uninitialized memory. The outcome is that a valid certificate is never accepted (only a malformed certificate may be accepted).

- Vulnerability: CVE-2020-7043

  - CVSS Score: 6.4
  - Description: An issue was discovered in openfortivpn 1.11.0 when used with OpenSSL before 1.0.2. tunnel.c mishandles certificate validation because hostname comparisons do not consider '\{}0' characters, as demonstrated by a good.example.com\{}x00evil.example.com attack.

- Vulnerability: CVE-2016-2107

  - CVSS Score: 2.6
  - Description: The AES-NI implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h does not consider memory allocation during a certain padding check, which allows remote attackers to obtain sensitive cleartext information via a padding-oracle attack against an AES CBC session. NOTE: this vulnerability exists because of an incorrect fix for CVE-2013-0169.

- Vulnerability: CVE-2016-2106

  - CVSS Score: 5

- Description: Integer overflow in the EVP_EncryptUpdate function in crypto/evp/evp_enc.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of data.

- Vulnerability: CVE-2019-11358

  - CVSS Score: 4.3
  - Description: jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.

- Vulnerability: CVE-2014-0195

  - CVSS Score: 6.8
  - Description: The dtls1_reassemble_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly validate fragment lengths in DTLS ClientHello messages, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a long non-initial fragment.

- Vulnerability: CVE-2009-3766

  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when OpenSSL is used, does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

- Vulnerability: CVE-2009-1379

  - CVSS Score: 5
  - Description: Use-after-free vulnerability in the dtls1_retrieve_buffered_fragment function in ssl/d1_both.c in OpenSSL 1.0.0 Beta 2 allows remote attackers to cause a denial of service (openssl s_client crash) and possibly have unspecified other impact via a DTLS packet, as demonstrated by a packet from a server that uses a crafted server certificate.

- Vulnerability: CVE-2015-0287

  - CVSS Score: 5
  - Description: The ASN1_item_ex_d2i function in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not reinitialize CHOICE and ADB data structures, which might allow attackers to cause a denial of service (invalid write operation and memory corruption) by leveraging an application that relies on ASN.1 structure reuse.

- Vulnerability: CVE-2015-0286

  - CVSS Score: 5
  - Description: The ASN1_TYPE_cmp function in crypto/asn1/a_type.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not properly perform boolean-type comparisons, which allows remote attackers to cause a denial of service (invalid read operation and application crash) via a crafted X.509 certificate to an endpoint that uses the certificate-verification feature.

- Vulnerability: CVE-2015-0289

  - CVSS Score: 5
  - Description: The PKCS#7 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not properly handle a lack of outer ContentInfo, which allows attackers to cause a denial of service (NULL pointer dereference and application crash) by leveraging an application that processes arbitrary PKCS#7 data and providing malformed data with ASN.1 encoding, related to crypto/pkcs7/pk7_doit.c and crypto/pkcs7/pk7_lib.c.

- Vulnerability: CVE-2015-0288

  - CVSS Score: 5
  - Description: The X509_to_X509_REQ function in crypto/x509/x509_req.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow attackers to cause a denial of service (NULL pointer dereference and application crash) via an invalid certificate key.

- Vulnerability: CVE-2016-7056

  - CVSS Score: 2.1
  - Description: A timing attack flaw was found in OpenSSL 1.0.1u and before that could allow a malicious user with local access to recover ECDSA P-256 private keys.

- Vulnerability: CVE-2014-3512

  - CVSS Score: 7.5
  - Description: Multiple buffer overflows in crypto/srp/srp_lib.c in the SRP implementation in OpenSSL 1.0.1 before 1.0.1i allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via an invalid SRP (1) g, (2) A, or (3) B parameter.

- Vulnerability: CVE-2014-3511

  - CVSS Score: 4.3
  - Description: The ssl23_get_client_hello function in s23_srvr.c in OpenSSL 1.0.1 before 1.0.1i allows man-in-the-middle attackers to force the use of TLS 1.0 by triggering ClientHello message fragmentation in communication between a client and server that both support later TLS versions, related to a "protocol downgrade" issue.

- Vulnerability: CVE-2015-1791

  - CVSS Score: 6.8
  - Description: Race condition in the ssl3_get_new_session_ticket function in ssl/s3_clnt.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b, when used for a multi-threaded client, allows remote attackers to cause a denial of service (double free and application crash) or possibly have unspecified other impact by providing a NewSessionTicket during an attempt to reuse a ticket that had been obtained earlier.

11.3 IP Address: 159.149.130.110

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 5

- High Vulnerabilities: 30

- Medium Vulnerabilities: 144

- Low Vulnerabilities: 9

- Total Vulnerabilities: 188

Services Running on IP Address

- Service: OpenSSH

  – Port: 22
  – Version: 8.0
  – Location:

- Service: Apache httpd

  – Port: 80
  – Version: 2.4.37
  – Location: /

- Service: Apache httpd

  – Port: 443
  – Version: 2.4.37
  – Location: /

- Service: N/A

  – Port: 9418
  – Version: N/A
  – Location:

Vulnerabilities Found

- Vulnerability: CVE-2019-16905

  – CVSS Score: 4.4
  – Description: OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.

- Vulnerability: CVE-2016-20012

  – CVSS Score: 4.3
  – Description: OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product

- Vulnerability: CVE-2021-36368

  - CVSS Score: 2.6
  - Description: An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is "this is not an authentication bypass, since nothing is being bypassed.

- Vulnerability: CVE-2020-14145

  - CVSS Score: 4.3
  - Description: The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.

- Vulnerability: CVE-2023-51767

  - CVSS Score: N/A
  - Description: OpenSSH through 9.6, when common types of DRAM are used, might allow row hammer attacks (for authentication bypass) because the integer value of authenticated in mm_answer_authpassword does not resist flips of a single bit. NOTE: this is applicable to a certain threat model of attacker-victim co-location in which the attacker has user privileges.

- Vulnerability: CVE-2020-15778

  - CVSS Score: 6.8
  - Description: scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."

- Vulnerability: CVE-2023-48795

  - CVSS Score: N/A

- Description: The SSH transport protocol with certain OpenSSH extensions,
found in OpenSSH before 9.6 and other products, allows remote
attackers to bypass integrity checks such that some packets are
omitted (from the extension negotiation message), and a client and
server may consequently end up with a connection for which some
security features have been downgraded or disabled, aka a Terrapin
attack. This occurs because the SSH Binary Packet Protocol (BPP),
implemented by these extensions, mishandles the handshake phase
and mishandles use of sequence numbers. For example, there is an
effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with
Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com
and (if CBC is used) the -etm@openssh.com MAC algorithms. This also
affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear
through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80,
AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh
before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway
before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch
before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through
23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0,
ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before
2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0,
ConnectBot SSH library before 2.2.22, Apache MINA sshd through
2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2
6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before
11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before
5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2,
Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY
through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2
module before 1.15.0 for Node.js, the thrussh library before 0.35.1
for Rust, and the Russh crate before 0.40.2 for Rust.

- **Vulnerability:** CVE-2023-38408

  - CVSS Score: N/A
  - Description: The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an
insufficiently trustworthy search path, leading to remote code
execution if an agent is forwarded to an attacker-controlled
system. (Code in /usr/lib is not necessarily safe for loading into
ssh-agent.) NOTE: this issue exists because of an incomplete fix for
CVE-2016-10009.

- **Vulnerability:** CVE-2007-2768

  - CVSS Score: 4.3
  - Description: OpenSSH, when using OPIE (One-Time Passwords in Everything) for PAM,
allows remote attackers to determine the existence of certain user
accounts, which displays a different response if the user account
exists and is configured to use one-time passwords (OTP), a similar
issue to CVE-2007-2243.

- **Vulnerability:** CVE-2021-41617

  - CVSS Score: 4.4
  - Description: sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default
configurations are used, allows privilege escalation because
supplemental groups are not initialized as expected. Helper programs
for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run
with privileges associated with group memberships of the sshd
process, if the configuration specifies running the command as a
different user.

- **Vulnerability:** CVE-2023-51385

- CVSS Score: N/A
- Description: In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.

- Vulnerability: CVE-2008-3844

  - CVSS Score: 9.3
  - Description: Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, as signed in August 2008 using a legitimate Red Hat GPG key, contain an externally introduced modification (Trojan Horse) that allows the package authors to have an unknown impact. NOTE: since the malicious packages were not distributed from any official Red Hat sources, the scope of this issue is restricted to users who may have obtained these packages through unofficial distribution points. As of 20080827, no unofficial distributions of this software are known.

- Vulnerability: CVE-2019-0215

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in mod_ssl when using per-location client certificate verification with TLSv1.3 allowed a client to bypass configured access control restrictions.

- Vulnerability: CVE-2024-4577

  - CVSS Score: N/A
  - Description: In PHP versions8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in command line given toWin32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc.

- Vulnerability: CVE-2013-4365

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2022-28330

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2021-32791

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2021-32792

  – CVSS Score: 4.3
  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using `OIDCPreservePost On`.

- Vulnerability: CVE-2020-7070

  – CVSS Score: 5
  – Description: In PHP versions 7.2.x below 7.2.34, 7.3.x below 7.3.23 and 7.4.x below 7.4.11, when PHP is processing incoming HTTP cookie values, the cookie names are url-decoded. This may lead to cookies with prefixes like __Host confused with cookies that decode to such prefix, thus leading to an attacker being able to forge cookie which is supposed to be secure. See also CVE-2020-8184 for more information.

- Vulnerability: CVE-2024-38476

  – CVSS Score: N/A
  – Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-27316

  – CVSS Score: N/A
  – Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

- Vulnerability: CVE-2023-31122

  – CVSS Score: N/A
  – Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2009-0796

  – CVSS Score: 2.6
  – Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2024-0727

  – CVSS Score: N/A

– Description: Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSLto crash leading to a potential Denial of Service attackImpact summary: Applications loading files in the PKCS12 format from untrustedsources might terminate abruptly.A file in PKCS12 format can contain certificates and keys and may come from anuntrusted source. The PKCS12 specification allows certain fields to be NULL, butOpenSSL does not correctly check for this case. This can lead to a NULL pointerdereference that results in OpenSSL crashing. If an application processes PKCS12files from an untrusted source using the OpenSSL APIs then that application willbe vulnerable to this issue.OpenSSL APIs that are vulnerable to this are: PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a similar issue in SMIME_write_PKCS7(). However since thisfunction is related to writing data we do not consider it security significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.

- Vulnerability: CVE-2021-36160

    – CVSS Score: 5
    – Description: A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS). This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48 (inclusive).

- Vulnerability: CVE-2020-7061

    – CVSS Score: 6.4
    – Description: In PHP versions 7.3.x below 7.3.15 and 7.4.x below 7.4.3, while extracting PHAR files on Windows using phar extension, certain content inside PHAR file could lead to one-byte read past the allocated buffer. This could potentially lead to information disclosure or crash.

- Vulnerability: CVE-2020-1927

    – CVSS Score: 5.8
    – Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.

- Vulnerability: CVE-2023-0286

    – CVSS Score: N/A
    – Description: There is a type confusion vulnerability relating to X.400 address processinginside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING butthe public structure definition for GENERAL_NAME incorrectly specified the typeof the x400Address field as ASN1_TYPE. This field is subsequently interpreted bythe OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than anASN1_STRING.When CRL checking is enabled (i.e. the application sets theX509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to passarbitrary pointers to a memcmp call, enabling them to read memory contents orenact a denial of service. In most cases, the attack requires the attacker toprovide both the certificate chain and CRL, neither of which need to have avalid signature. If the attacker only controls one of these inputs, the otherinput must already contain an X.400 address as a CRL distribution point, whichis uncommon. As such, this vulnerability is most likely to only affectapplications which have implemented their own functionality for retrieving CRLsover a network.

- Vulnerability: CVE-2023-3817

  – CVSS Score: N/A

  – Description: Issue summary: Checking excessively long DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH key or DH parameters may experience longdelays. Where the key or parameters that are being checked have been obtainedfrom an untrusted source this may lead to a Denial of Service.The function DH_check() performs various checks on DH parameters. After fixingCVE-2023-3446 it was discovered that a large q parameter value can also triggeran overly long computation during some of these checks. A correct q value,if present, cannot be larger than the modulus p parameter, thus it isunnecessary to perform these checks if q is larger than p.An application that calls DH_check() and supplies a key or parameters obtainedfrom an untrusted source could be vulnerable to a Denial of Service attack.The function DH_check() is itself called by a number of other OpenSSL functions.An application calling any of those other functions may similarly be affected.The other functions affected by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable are the OpenSSL dhparam and pkeyparam command line applicationswhen using the "-check" option.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2021-32786

  – CVSS Score: 5.8

  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, 'oidc_validate_redirect_url()' does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring 'mod_auth_openidc' to only allow redirection whose destination matches a given regular expression.

- Vulnerability: CVE-2021-32785

  – CVSS Score: 4.3

  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache ('OIDCCacheEncrypt off', 'OIDCSessionType server-cache', 'OIDCCacheType redis'), 'mod_auth_openidc' wrongly performed argument interpolation before passing Redis requests to 'hiredis', which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the 'hiredis' API. As a workaround, this vulnerability can be mitigated by setting 'OIDCCacheEncrypt' to 'on', as cache keys are cryptographically hashed before use when this option is enabled.

- Vulnerability: CVE-2020-9490

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2020-7060

  - CVSS Score: 6.4
  - Description: When using certain mbstring functions to convert multibyte encodings, in PHP versions 7.2.x below 7.2.27, 7.3.x below 7.3.14 and 7.4.x below 7.4.2 it is possible to supply data that will cause function mbfl_filt_conv_big5_wchar to read past the allocated buffer. This may lead to information disclosure or crash.

- Vulnerability: CVE-2021-44790

  - CVSS Score: 7.5
  - Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

- Vulnerability: CVE-2020-7062

  - CVSS Score: 4.3
  - Description: In PHP versions 7.2.x below 7.2.28, 7.3.x below 7.3.15 and 7.4.x below 7.4.3, when using file upload functionality, if upload progress tracking is enabled, but session.upload_progress.cleanup is set to 0 (disabled), and the file upload fails, the upload procedure would try to clean up data that does not exist and encounter null pointer dereference, which would likely lead to a crash.

- Vulnerability: CVE-2020-7063

  - CVSS Score: 5
  - Description: In PHP versions 7.2.x below 7.2.28, 7.3.x below 7.3.15 and 7.4.x below 7.4.3, when creating PHAR archive using PharData::buildFromIterator() function, the files are added with default permissions (0666, or all access) even if the original files on the filesystem were with more restrictive permissions. This may result in files having more lax permissions than intended when such archive is extracted.

- Vulnerability: CVE-2020-7064

  - CVSS Score: 5.8

229

- Description: In PHP versions 7.2.x below 7.2.9, 7.3.x below 7.3.16 and 7.4.x below 7.4.4, while parsing EXIF data with exif_read_data() function, it is possible for malicious data to cause PHP to read one byte of uninitialized memory. This could potentially lead to information disclosure or crash.

- Vulnerability: CVE-2020-7066

  - CVSS Score: 4.3
  - Description: In PHP versions 7.2.x below 7.2.29, 7.3.x below 7.3.16 and 7.4.x below 7.4.4, while using get_headers() with user-supplied URL, if the URL contains zero (\{}0) character, the URL will be silently truncated at it. This may cause some software to make incorrect assumptions about the target of the get_headers() and possibly send some information to a wrong server.

- Vulnerability: CVE-2020-7067

  - CVSS Score: 5
  - Description: In PHP versions 7.2.x below 7.2.30, 7.3.x below 7.3.17 and 7.4.x below 7.4.5, if PHP is compiled with EBCDIC support (uncommon), urldecode() function can be made to access locations past the allocated memory, due to erroneously using signed numbers as array indexes.

- Vulnerability: CVE-2020-7068

  - CVSS Score: 3.3
  - Description: In PHP versions 7.2.x below 7.2.33, 7.3.x below 7.3.21 and 7.4.x below 7.4.9, while processing PHAR files using phar extension, phar_parse_zipfile could be tricked into accessing freed memory, which could lead to a crash or information disclosure.

- Vulnerability: CVE-2020-7069

  - CVSS Score: 6.4
  - Description: In PHP versions 7.2.x below 7.2.34, 7.3.x below 7.3.23 and 7.4.x below 7.4.11, when AES-CCM mode is used with openssl_encrypt() function with 12 bytes IV, only first 7 bytes of the IV is actually used. This can lead to both decreased security and incorrect encryption data.

- Vulnerability: CVE-2022-37436

  - CVSS Score: N/A
  - Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2020-13938

  - CVSS Score: 2.1
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

- Vulnerability: CVE-2023-2650

  - CVSS Score: N/A

- Description: Issue summary: Processing some specially crafted ASN.1 object
                identifiers ordata containing them may be very slow.Impact summary:
                Applications that use OBJ_obj2txt() directly, or use any ofthe
                OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with
                no messagesize limit may experience notable to very long delays
                when processing thosemessages, which may lead to a Denial of
                Service.An OBJECT IDENTIFIER is composed of a series of numbers –
                sub-identifiers -most of which have no size limit. OBJ_obj2txt() may
                be used to translatean ASN.1 OBJECT IDENTIFIER given in DER encoding
                form (using the OpenSSLtype ASN1_OBJECT) to its canonical numeric
                text form, which are thesub-identifiers of the OBJECT IDENTIFIER in
                decimal form, separated byperiods.When one of the sub-identifiers in
                the OBJECT IDENTIFIER is very large(these are sizes that are seen as
                absurdly large, taking up tens or hundredsof KiBs), the translation
                to a decimal number in text may take a very longtime. The time
                complexity is $O(n^2)$ with 'n' being the size of thesub-identifiers
                in bytes (*).With OpenSSL 3.0, support to fetch cryptographic
                algorithms using names /identifiers in string form was introduced.
                This includes using OBJECTIDENTIFIERs in canonical numeric text form
                as identifiers for fetchingalgorithms.Such OBJECT IDENTIFIERs may
                be received through the ASN.1 structureAlgorithmIdentifier, which
                is commonly used in multiple protocols to specifywhat cryptographic
                algorithm should be used to sign or verify, encrypt ordecrypt, or
                digest passed data.Applications that call OBJ_obj2txt() directly
                with untrusted data areaffected, with any version of OpenSSL. If the
                use is for the mere purposeof display, the severity is considered
                low.In OpenSSL 3.0 and newer, this affects the subsystems OCSP,
                PKCS7/SMIME,CMS, CMP/CRMF or TS. It also impacts anything that
                processes X.509certificates, including simple things like verifying
                its signature.The impact on TLS is relatively low, because all
                versions of OpenSSL have a100KiB limit on the peer's certificate
                chain. Additionally, this onlyimpacts clients, or servers that
                have explicitly enabled clientauthentication.In OpenSSL 1.1.1 and
                1.0.2, this only affects displaying diverse objects,such as X.509
                certificates. This is assumed to not happen in such a waythat it
                would cause a Denial of Service, so these versions are considerednot
                affected by this issue in such a way that it would be cause for
                concern,and the severity is therefore considered low.

- Vulnerability: CVE-2023-0215

  - CVSS Score: N/A

- Description: The public API function BIO_new_NDEF is a helper function used for streamingASN.1 data via a BIO. It is primarily used internally to OpenSSL to support theSMIME, CMS and PKCS7 streaming capabilities, but may also be called directly byend user applications.The function receives a BIO from the caller, prepends a new BIO_f_asn1 filterBIO onto the front of it to form a BIO chain, and then returns the new head ofthe BIO chain to the caller. Under certain conditions, for example if a CMSrecipient public key is invalid, the new filter BIO is freed and the functionreturns a NULL result indicating a failure. However, in this case, the BIO chainis not properly cleaned up and the BIO passed by the caller still retainsinternal pointers to the previously freed filter BIO. If the caller then goes onto call BIO_pop() on the BIO then a use-after-free will occur. This will mostlikely result in a crash.This scenario occurs directly in the internal function B64_write_ASN1() whichmay cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() onthe BIO. This internal function is in turn called by the public API functionsPEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream,SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7.Other public API functions that may be impacted by this includei2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream andi2d_PKCS7_bio_stream.The OpenSSL cms and smime command line applications are similarly affected.

- **Vulnerability: CVE-2019-9517**

  - CVSS Score: 7.8
  - Description: Some HTTP/2 implementations are vulnerable to unconstrained interal data buffering, potentially leading to a denial of service. The attacker opens the HTTP/2 window so the peer can send without constraint; however, they leave the TCP window closed so the peer cannot actually write (many of) the bytes on the wire. The attacker then sends a stream of requests for a large response object. Depending on how the servers queue the responses, this can consume excess memory, CPU, or both.

- **Vulnerability: CVE-2020-35452**

  - CVSS Score: 6.8
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

- **Vulnerability: CVE-2022-22719**

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- **Vulnerability: CVE-2022-31628**

  - CVSS Score: N/A
  - Description: In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the phar uncompressor code would recursively uncompress "quines" gzip files, resulting in an infinite loop.

- **Vulnerability: CVE-2022-31629**

- CVSS Score: N/A
- Description: In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the vulnerability enables network and same-site attackers to set a standard insecure cookie in the victim's browser which is treated as a '__Host-' or '__Secure-' cookie by PHP applications.

- **Vulnerability: CVE-2020-1934**

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

- **Vulnerability: CVE-2022-36760**

  - CVSS Score: N/A
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- **Vulnerability: CVE-2022-4304**

  - CVSS Score: N/A
  - Description: A timing based side channel exists in the OpenSSL RSA Decryption implementationwhich could be sufficient to recover a plaintext across a network in aBleichenbacher style attack. To achieve a successful decryption an attackerwould have to be able to send a very large number of trial messages fordecryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5,RSA-OEAP and RSASVE.For example, in a TLS connection, RSA is commonly used by a client to send anencrypted pre-master secret to the server. An attacker that had observed agenuine connection between a client and a server could use this flaw to sendtrial messages to the server and record the time taken to process them. After asufficiently large number of messages the attacker could recover the pre-mastersecret used for the original connection and thus be able to decrypt theapplication data sent over that connection.

- **Vulnerability: CVE-2017-8923**

  - CVSS Score: 7.5
  - Description: The zend_string_extend function in Zend/zend_string.h in PHP through 7.1.5 does not prevent changes to string objects that result in a negative length, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact by leveraging a script's use of .= with a long string.

- **Vulnerability: CVE-2019-0217**

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.

- **Vulnerability: CVE-2019-0197**

  - CVSS Score: 4.9

- Description: A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38.
  When HTTP/2 was enabled for a http: host or H2Upgrade was enabled
  for h2 on a https: host, an Upgrade request from http/1.1 to
  http/2 that was not the first request on a connection could lead
  to a misconfiguration and crash. Server that never enabled the
  h2 protocol or that only enabled it for https: and did not set
  "H2Upgrade on" are unaffected by this issue.

- Vulnerability: CVE-2019-0196

  – CVSS Score: 5
  – Description: A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38.
    Using fuzzed network input, the http/2 request handling could be
    made to access freed memory in string comparison when determining the
    method of a request and thus process the request incorrectly.

- Vulnerability: CVE-2019-0190

  – CVSS Score: 5
  – Description: A bug exists in the way mod_ssl handled client renegotiations. A
    remote attacker could send a carefully crafted request that would
    cause mod_ssl to enter a loop leading to a denial of service. This
    bug can be only triggered with Apache HTTP Server version 2.4.37
    when using OpenSSL version 1.1.1 or later, due to an interaction in
    changes to handling of renegotiation attempts.

- Vulnerability: CVE-2021-33193

  – CVSS Score: 5
  – Description: A crafted method sent through HTTP/2 will bypass validation and be
    forwarded by mod_proxy, which can lead to request splitting or cache
    poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.

- Vulnerability: CVE-2019-0211

  – CVSS Score: 7.2
  – Description: In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event,
    worker or prefork, code executing in less-privileged child processes
    or threads (including scripts executed by an in-process scripting
    interpreter) could execute arbitrary code with the privileges of
    the parent process (usually root) by manipulating the scoreboard.
    Non-Unix systems are not affected.

- Vulnerability: CVE-2019-17567

  – CVSS Score: 5
  – Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel
    configured on an URL that is not necessarily Upgraded by the origin
    server was tunneling the whole connection regardless, thus allowing
    for subsequent requests on the same connection to pass through
    with no HTTP validation, authentication or authorization possibly
    configured.

- Vulnerability: CVE-2022-31813

  – CVSS Score: 7.5
  – Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-*
    headers to the origin server based on client side Connection
    header hop-by-hop mechanism. This may be used to bypass IP based
    authentication on the origin server/application.

- Vulnerability: CVE-2013-2220

- CVSS Score: 7.5
- Description: Buffer overflow in the radius_get_vendor_attr function in the Radius extension before 1.2.7 for PHP allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a large Vendor Specific Attributes (VSA) length value.

- Vulnerability: CVE-2012-4360

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2023-4807

  - CVSS Score: N/A
  - Description: Issue summary: The POLY1305 MAC (message authentication code) implementationcontains a bug that might corrupt the internal state of applications on theWindows 64 platform when running on newer X86_64 processors supporting theAVX512-IFMA instructions.Impact summary: If in an application that uses the OpenSSL library an attackercan influence whether the POLY1305 MAC algorithm is used, the applicationstate might be corrupted with various application dependent consequences.The POLY1305 MAC (message authentication code) implementation in OpenSSL doesnot save the contents of non-volatile XMM registers on Windows 64 platformwhen calculating the MAC of data larger than 64 bytes. Before returning tothe caller all the XMM registers are set to zero rather than restoring theirprevious content. The vulnerable code is used only on newer x86_64 processorssupporting the AVX512-IFMA instructions.The consequences of this kind of internal application state corruption canbe various - from no consequences, if the calling application does notdepend on the contents of non-volatile XMM registers at all, to the worstconsequences, where the attacker could get complete control of the applicationprocess. However given the contents of the registers are just zeroized sothe attacker cannot put arbitrary values inside, the most likely consequence,if any, would be an incorrect result of some application dependentcalculations or a crash leading to a denial of service.The POLY1305 MAC algorithm is most frequently used as part of theCHACHA20-POLY1305 AEAD (authenticated encryption with associated data)algorithm. The most common usage of this AEAD cipher is with TLS protocolversions 1.2 and 1.3 and a malicious client can influence whether this AEADcipher is used by the server. This implies that server applications usingOpenSSL can be potentially impacted. However we are currently not aware ofany concrete application that would be affected by this issue therefore weconsider this a Low severity security issue.As a workaround the AVX512-IFMA instructions support can be disabled atruntime by setting the environment variable OPENSSL_ia32cap: OPENSSL_ia32cap=:~0x200000The FIPS provider is not affected by this issue.

- Vulnerability: CVE-2009-3767

  - CVSS Score: 4.3
  - Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other versions, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2021-26690

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service

- Vulnerability: CVE-2021-26691

  - CVSS Score: 7.5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow

- Vulnerability: CVE-2019-0220

  - CVSS Score: 5
  - Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.

- Vulnerability: CVE-2024-38477

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-38474

  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2021-39275

  - CVSS Score: 7.5
  - Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2018-17189

  - CVSS Score: 5
  - Description: In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 (mod_http2) connections.

- Vulnerability: CVE-2022-29404

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2022-37454

  - CVSS Score: N/A
  - Description: The Keccak XKCP SHA-3 reference implementation before fdc6fef has an
                   integer overflow and resultant buffer overflow that allows attackers
                   to execute arbitrary code or eliminate expected cryptographic
                   properties. This occurs in the sponge function interface.

- Vulnerability: CVE-2007-3205

  - CVSS Score: 5
  - Description: The parse_str function in (1) PHP, (2) Hardened-PHP, and (3) Suhosin,
                   when called without a second parameter, might allow remote attackers
                   to overwrite arbitrary variables by specifying variable names and
                   values in the string to be parsed. NOTE: it is not clear whether
                   this is a design limitation of the function or a bug in PHP, although
                   it is likely to be regarded as a bug in Hardened-PHP and Suhosin.

- Vulnerability: CVE-2020-11993

  - CVSS Score: 4.3
  - Description: Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug
                   was enabled for the HTTP/2 module and on certain traffic edge
                   patterns, logging statements were made on the wrong connection,
                   causing concurrent use of memory pools. Configuring the LogLevel of
                   mod_http2 above "info" will mitigate this vulnerability for unpatched
                   servers.

- Vulnerability: CVE-2019-10092

  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting
                   issue was reported affecting the mod_proxy error page. An attacker
                   could cause the link on the error page to be malformed and instead
                   point to a page of their choice. This would only be exploitable
                   where a server was set up with proxying enabled but was misconfigured
                   in such a way that the Proxy Error page was displayed.

- Vulnerability: CVE-2022-2068

  - CVSS Score: 10
  - Description: In addition to the c_rehash shell command injection identified in
                   CVE-2022-1292, further circumstances where the c_rehash script
                   does not properly sanitise shell metacharacters to prevent command
                   injection were found by code review. When the CVE-2022-1292 was
                   fixed it was not discovered that there are other places in the
                   script where the file names of certificates being hashed were
                   possibly passed to a command executed through the shell. This
                   script is distributed by some operating systems in a manner where
                   it is automatically executed. On such operating systems, an
                   attacker could execute arbitrary commands with the privileges of
                   the script. Use of the c_rehash script is considered obsolete and
                   should be replaced by the OpenSSL rehash command line tool. Fixed in
                   OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL
                   1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected
                   1.0.2-1.0.2ze).

- Vulnerability: CVE-2009-3766

  - CVSS Score: 6.8

– Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when
                OpenSSL is used, does not verify the domain name in the subject's
                Common Name (CN) field of an X.509 certificate, which allows
                man-in-the-middle attackers to spoof SSL servers via an arbitrary
                valid certificate.

- Vulnerability: CVE-2021-44224

  – CVSS Score: 6.4
  – Description: A crafted URI sent to httpd configured as a forward proxy
                  (ProxyRequests on) can cause a crash (NULL pointer dereference) or,
                  for configurations mixing forward and reverse proxy declarations, can
                  allow for requests to be directed to a declared Unix Domain Socket
                  endpoint (Server Side Request Forgery). This issue affects Apache
                  HTTP Server 2.4.7 up to 2.4.51 (included).

- Vulnerability: CVE-2009-3765

  – CVSS Score: 6.8
  – Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does
                  not properly handle a '\{}0' character in a domain name in the
                  subject's Common Name (CN) field of an X.509 certificate, which
                  allows man-in-the-middle attackers to spoof arbitrary SSL servers via
                  a crafted certificate issued by a legitimate Certification Authority,
                  a related issue to CVE-2009-2408.

- Vulnerability: CVE-2022-22721

  – CVSS Score: 5.8
  – Description: If LimitXMLRequestBody is set to allow request bodies larger than
                  350MB (defaults to 1M) on 32 bit systems an integer overflow happens
                  which later causes out of bounds writes. This issue affects Apache
                  HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2006-20001

  – CVSS Score: N/A
  – Description: A carefully crafted If: request header can cause a memory read, or
                  write of a single zero byte, in a pool (heap) memory location beyond
                  the header value sent. This could cause the process to crash.This
                  issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2021-3711

  – CVSS Score: 7.5

– Description: In order to decrypt SM2 encrypted data an application is expected to call the API function EVP_PKEY_decrypt(). Typically an application will call this function twice. The first time, on entry, the "out" parameter can be NULL and, on exit, the "outlen" parameter is populated with the buffer size required to hold the decrypted plaintext. The application can then allocate a sufficiently sized buffer and call EVP_PKEY_decrypt() again, but this time passing a non-NULL value for the "out" parameter. A bug in the implementation of the SM2 decryption code means that the calculation of the buffer size required to hold the plaintext returned by the first call to EVP_PKEY_decrypt() can be smaller than the actual size required by the second call. This can lead to a buffer overflow when EVP_PKEY_decrypt() is called by the application a second time with a buffer that is too small. A malicious attacker who is able present SM2 content for decryption to an application could cause attacker chosen data to overflow the buffer by up to a maximum of 62 bytes altering the contents of other data held after the buffer, possibly changing application behaviour or causing the application to crash. The location of the buffer is application dependent but is typically heap allocated. Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k).

- Vulnerability: CVE-2021-3712

  – CVSS Score: 5.8
  – Description: ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own "d2i" functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the "data" and "length" fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the "data" field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). It can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y).

- Vulnerability: CVE-2023-0464

- CVSS Score: N/A
- Description: A security vulnerability has been identified in all supported versionsof OpenSSL related to the verification of X.509 certificate chainsthat include policy constraints. Attackers may be able to exploit thisvulnerability by creating a malicious certificate chain that triggersexponential use of computational resources, leading to a denial-of-service(DoS) attack on affected systems.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0465

  - CVSS Score: N/A
  - Description: Applications that use a non-default option when verifying certificates may bevulnerable to an attack from a malicious CA to circumvent certain checks.Invalid certificate policies in leaf certificates are silently ignored byOpenSSL and other certificate policy checks are skipped for that certificate.A malicious CA could use this to deliberately assert invalid certificate policiesin order to circumvent policy checking on the certificate altogether.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0466

  - CVSS Score: N/A
  - Description: The function X509_VERIFY_PARAM_add0_policy() is documented toimplicitly enable the certificate policy check when doing certificateverification. However the implementation of the function does notenable the check which allows certificates with invalid or incorrectpolicies to pass the certificate verification.As suddenly enabling the policy check could break existing deployments it wasdecided to keep the existing behavior of the X509_VERIFY_PARAM_add0_policy()function.Instead the applications that require OpenSSL to perform certificatepolicy check need to use X509_VERIFY_PARAM_set1_policies() or explicitlyenable the policy check by calling X509_VERIFY_PARAM_set_flags() withthe X509_V_FLAG_POLICY_CHECK flag argument.Certificate policy checks are disabled by default in OpenSSL and are notcommonly used by applications.

- Vulnerability: CVE-2019-10098

  - CVSS Score: 5.8
  - Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.

- Vulnerability: CVE-2019-10097

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4.32-2.4.39, when mod_remoteip was configured to use a trusted intermediary proxy server using the "PROXY" protocol, a specially crafted PROXY header could trigger a stack buffer overflow or NULL pointer deference. This vulnerability could only be triggered by a trusted proxy and not by untrusted HTTP clients.

- Vulnerability: CVE-2021-40438
  - CVSS Score: 6.8
  - Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2011-1176
  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2022-23943
  - CVSS Score: 7.5
  - Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

- Vulnerability: CVE-2018-17199
  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

- Vulnerability: CVE-2022-22720
  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2021-34798
  - CVSS Score: 5
  - Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2023-25690
  - CVSS Score: N/A
  - Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2020-11984

  - CVSS Score: 7.5
  - Description: Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE

- Vulnerability: CVE-2021-4160

  - CVSS Score: 4.3
  - Description: There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that is available to premium support customers only. It will be made available in 1.0.2zc when it is released. The issue only affects OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0). Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL 1.0.2zc-dev (Affected 1.0.2-1.0.2zb).

- Vulnerability: CVE-2022-26377

  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2019-10081

  - CVSS Score: 5
  - Description: HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example configured with "H2PushResource", could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client.

- Vulnerability: CVE-2019-10082

  - CVSS Score: 6.4
  - Description: In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.

- Vulnerability: CVE-2024-40898

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2022-0778

  – CVSS Score: 5

  – Description: The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - TLS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

- Vulnerability: CVE-2022-2097

  – CVSS Score: 5

  – Description: AES OCB mode for 32-bit x86 platforms using the AES-NI assembly optimised implementation will not encrypt the entirety of the data under some circumstances. This could reveal sixteen bytes of data that was preexisting in the memory that wasn't written. In the special case of "in place" encryption, sixteen bytes of the plaintext would be revealed. Since OpenSSL does not support OCB based cipher suites for TLS and DTLS, they are both unaffected. Fixed in OpenSSL 3.0.5 (Affected 3.0.0-3.0.4). Fixed in OpenSSL 1.1.1q (Affected 1.1.1-1.1.1p).

- Vulnerability: CVE-2023-27522

  – CVSS Score: N/A

  – Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.Special characters in the origin response header can truncate/split the response forwarded to the client.

- Vulnerability: CVE-2009-1390

  – CVSS Score: 6.8

- Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2)
GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS
certificate in the chain is accepted instead of verifying the entire
chain, which allows remote attackers to spoof trusted servers via a
man-in-the-middle attack.

- Vulnerability: CVE-2012-3526

  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the
Apache HTTP Server allows remote attackers to cause a denial of
service (server or application crash) via multiple X-Forwarded-For
headers in a request.

- Vulnerability: CVE-2020-7059

  - CVSS Score: 6.4
  - Description: When using fgetss() function to read data with stripping tags, in PHP
versions 7.2.x below 7.2.27, 7.3.x below 7.3.14 and 7.4.x below 7.4.2
it is possible to supply data that will cause this function to read
past the allocated buffer. This may lead to information disclosure
or crash.

- Vulnerability: CVE-2023-5678

  - CVSS Score: N/A
  - Description: Issue summary: Generating excessively long X9.42 DH keys or
checkingexcessively long X9.42 DH keys or parameters may be
very slow.Impact summary: Applications that use the functions
DH_generate_key() togenerate an X9.42 DH key may experience
long delays. Likewise, applicationsthat use DH_check_pub_key(),
DH_check_pub_key_ex() or EVP_PKEY_public_check()to check an
X9.42 DH key or X9.42 DH parameters may experience long
delays.Where the key or parameters that are being checked have
been obtained froman untrusted source this may lead to a Denial
of Service.While DH_check() performs all the necessary checks
(as of CVE-2023-3817),DH_check_pub_key() doesn't make any of
these checks, and is thereforevulnerable for excessively large
P and Q parameters.Likewise, while DH_generate_key() performs
a check for an excessively largeP, it doesn't check for an
excessively large Q.An application that calls DH_generate_key() or
DH_check_pub_key() andsupplies a key or parameters obtained from
an untrusted source could bevulnerable to a Denial of Service
attack.DH_generate_key() and DH_check_pub_key() are also called by
a number ofother OpenSSL functions. An application calling any of
those otherfunctions may similarly be affected. The other functions
affected by thisare DH_check_pub_key_ex(), EVP_PKEY_public_check(), and
EVP_PKEY_generate().Also vulnerable are the OpenSSL pkey command line
application when using the"-pubcheck" option, as well as the OpenSSL
genpkey command line application.The OpenSSL SSL/TLS implementation
is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers
are not affected by this issue.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module
before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before
3.1.1-11637, a module for the Apache HTTP Server, allows remote
attackers to cause a denial of service (memory consumption) via an
HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2022-1292

  – CVSS Score: 10

  – Description: The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n). Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).

- Vulnerability: CVE-2019-11048

  – CVSS Score: 5

  – Description: In PHP versions 7.2.x below 7.2.31, 7.3.x below 7.3.18 and 7.4.x below 7.4.6, when HTTP file uploads are allowed, supplying overly long filenames or field names could lead PHP engine to try to allocate oversized memory storage, hit the memory limit and stop processing the request, without cleaning up temporary files created by upload request. This potentially could lead to accumulation of uncleaned temporary files exhausting the disk space on the target server.

- Vulnerability: CVE-2012-4001

  – CVSS Score: 5

  – Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2019-11046

  – CVSS Score: 5

  – Description: In PHP versions 7.2.x below 7.2.26, 7.3.x below 7.3.13 and 7.4.0, PHP bcmath extension functions on some systems, including Windows, can be tricked into reading beyond the allocated space by supplying it with string containing characters that are identified as numeric by the OS but aren't ASCII numbers. This can read to disclosure of the content of some memory locations.

- Vulnerability: CVE-2019-11047

  – CVSS Score: 6.4

  – Description: When PHP EXIF extension is parsing EXIF information from an image, e.g. via exif_read_data() function, in PHP versions 7.2.x below 7.2.26, 7.3.x below 7.3.13 and 7.4.0 it is possible to supply it with data what will cause it to read past the allocated buffer. This may lead to information disclosure or crash.

- Vulnerability: CVE-2019-11044

  – CVSS Score: 5

  – Description: In PHP versions 7.2.x below 7.2.26, 7.3.x below 7.3.13 and 7.4.0 on Windows, PHP link() function accepts filenames with embedded \{}0 byte and treats them as terminating at that byte. This could lead to security vulnerabilities, e.g. in applications checking paths that the code is allowed to access.

- Vulnerability: CVE-2019-11045

245

- CVSS Score: 4.3
- Description: In PHP versions 7.2.x below 7.2.26, 7.3.x below 7.3.13 and 7.4.0, PHP DirectoryIterator class accepts filenames with embedded \{}0 byte and treats them as terminating at that byte. This could lead to security vulnerabilities, e.g. in applications checking paths that the code is allowed to access.

- Vulnerability: CVE-2022-4450

  - CVSS Score: N/A
  - Description: The function PEM_read_bio_ex() reads a PEM file from a BIO and parses anddecodes the "name" (e.g. "CERTIFICATE"), any header data and the payload data.If the function succeeds then the "name_out", "header" and "data" arguments arepopulated with pointers to buffers containing the relevant decoded data. Thecaller is responsible for freeing those buffers. It is possible to construct aPEM file that results in 0 bytes of payload data. In this case PEM_read_bio_ex()will return a failure code but will populate the header argument with a pointerto a buffer that has already been freed. If the caller also frees this bufferthen a double free will occur. This will most likely lead to a crash. Thiscould be exploited by an attacker who has the ability to supply malicious PEMfiles for parsing to achieve a denial of service attack.The functions PEM_read_bio() and PEM_read() are simple wrappers aroundPEM_read_bio_ex() and therefore these functions are also directly affected.These functions are also called indirectly by a number of other OpenSSLfunctions including PEM_X509_INFO_read_bio_ex() andSSL_CTX_use_serverinfo_file() which are also vulnerable. Some OpenSSL internaluses of these functions are not vulnerable because the caller does not free theheader argument if PEM_read_bio_ex() returns a failure code. These locationsinclude the PEM_read_bio_TYPE() functions as well as the decoders introduced inOpenSSL 3.0.The OpenSSL asn1parse command line application is also impacted by this issue.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

– CVSS Score: 4.3

– Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication
Agent 7.1 before 7.1.1 for Web for Internet Information Services,
and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to
inject arbitrary web script or HTML via unspecified vectors.

• Vulnerability: CVE-2019-11050

– CVSS Score: 6.4

– Description: When PHP EXIF extension is parsing EXIF information from an image,
e.g. via exif_read_data() function, in PHP versions 7.2.x below
7.2.26, 7.3.x below 7.3.13 and 7.4.0 it is possible to supply it
with data what will cause it to read past the allocated buffer. This
may lead to information disclosure or crash.

• Vulnerability: CVE-2023-45802

– CVSS Score: N/A

– Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a
time window were the request's memory resources were not reclaimed
immediately. Instead, de-allocation was deferred to connection
close. A client could send new requests and resets, keeping the
connection busy and open and causing the memory footprint to keep
on growing. On connection close, all resources were reclaimed, but
the process might run out of memory before that.This was found by
the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset
Exploit) with their own test client. During "normal" HTTP/2 use, the
probability to hit this bug is very low. The kept memory would not
become noticeable before the connection closes or times out.Users are
recommended to upgrade to version 2.4.58, which fixes the issue.

• Vulnerability: CVE-2022-30556

– CVSS Score: 5

– Description: Apache HTTP Server 2.4.53 and earlier may return lengths to
applications calling r:wsread() that point past the end of the
storage allocated for the buffer.

• Vulnerability: CVE-2022-28615

– CVSS Score: 6.4

– Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose
information due to a read beyond bounds in ap_strcmp_match() when
provided with an extremely large input buffer. While no code
distributed with the server can be coerced into such a call,
third-party modules or lua scripts that use ap_strcmp_match() may
hypothetically be affected.

• Vulnerability: CVE-2022-28614

– CVSS Score: 5

– Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier
may read unintended memory if an attacker can cause the server to
reflect very large input using ap_rwrite() or ap_rputs(), such as
with mod_luas r:puts() function. Modules compiled and distributed
separately from Apache HTTP Server that use the 'ap_rputs' function
and may pass it a very large (INT_MAX or larger) string must be
compiled against current headers to resolve the issue.

• Vulnerability: CVE-2019-0215

– CVSS Score: 6

- Description: In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in mod_ssl when using per-location client certificate verification with TLSv1.3 allowed a client to bypass configured access control restrictions.

- Vulnerability: CVE-2024-4577

  - CVSS Score: N/A
  - Description: In PHP versions8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in command line given toWin32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc.

- Vulnerability: CVE-2013-4365

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2022-28330

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2021-32791

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2021-32792

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.

- Vulnerability: CVE-2020-7070

  - CVSS Score: 5
  - Description: In PHP versions 7.2.x below 7.2.34, 7.3.x below 7.3.23 and 7.4.x below 7.4.11, when PHP is processing incoming HTTP cookie values, the cookie names are url-decoded. This may lead to cookies with prefixes like __Host confused with cookies that decode to such prefix, thus leading to an attacker being able to forge cookie which is supposed to be secure. See also CVE-2020-8184 for more information.

- Vulnerability: CVE-2024-38476

  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-27316

  - CVSS Score: N/A
  - Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

- Vulnerability: CVE-2023-31122

  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2009-0796

  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2024-0727

  - CVSS Score: N/A
  - Description: Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSLto crash leading to a potential Denial of Service attackImpact summary: Applications loading files in the PKCS12 format from untrustedsources might terminate abruptly.A file in PKCS12 format can contain certificates and keys and may come from anuntrusted source. The PKCS12 specification allows certain fields to be NULL, butOpenSSL does not correctly check for this case. This can lead to a NULL pointerdereference that results in OpenSSL crashing. If an application processes PKCS12files from an untrusted source using the OpenSSL APIs then that application willbe vulnerable to this issue.OpenSSL APIs that are vulnerable to this are: PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a similar issue in SMIME_write_PKCS7(). However since thisfunction is related to writing data we do not consider it security significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.

- Vulnerability: CVE-2021-36160

  - CVSS Score: 5
  - Description: A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS). This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48 (inclusive).

- Vulnerability: CVE-2020-7061

  - CVSS Score: 6.4

- Description: In PHP versions 7.3.x below 7.3.15 and 7.4.x below 7.4.3, while
  extracting PHAR files on Windows using phar extension, certain
  content inside PHAR file could lead to one-byte read past the
  allocated buffer. This could potentially lead to information
  disclosure or crash.

- Vulnerability: CVE-2020-1927

  - CVSS Score: 5.8
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with
    mod_rewrite that were intended to be self-referential might be fooled
    by encoded newlines and redirect instead to an an unexpected URL
    within the request URL.

- Vulnerability: CVE-2023-0286

  - CVSS Score: N/A
  - Description: There is a type confusion vulnerability relating to X.400 address
    processinginside an X.509 GeneralName. X.400 addresses were
    parsed as an ASN1_STRING butthe public structure definition for
    GENERAL_NAME incorrectly specified the typeof the x400Address
    field as ASN1_TYPE. This field is subsequently interpreted bythe
    OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than
    anASN1_STRING.When CRL checking is enabled (i.e. the application
    sets theX509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an
    attacker to passarbitrary pointers to a memcmp call, enabling them to
    read memory contents orenact a denial of service. In most cases,
    the attack requires the attacker toprovide both the certificate
    chain and CRL, neither of which need to have avalid signature. If
    the attacker only controls one of these inputs, the otherinput
    must already contain an X.400 address as a CRL distribution point,
    whichis uncommon. As such, this vulnerability is most likely to only
    affectapplications which have implemented their own functionality for
    retrieving CRLsover a network.

- Vulnerability: CVE-2023-3817

  - CVSS Score: N/A
  - Description: Issue summary: Checking excessively long DH keys or parameters may
    be very slow.Impact summary: Applications that use the functions
    DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH
    key or DH parameters may experience longdelays. Where the key or
    parameters that are being checked have been obtainedfrom an untrusted
    source this may lead to a Denial of Service.The function DH_check()
    performs various checks on DH parameters. After fixingCVE-2023-3446
    it was discovered that a large q parameter value can also triggeran
    overly long computation during some of these checks. A correct q
    value,if present, cannot be larger than the modulus p parameter, thus
    it isunnecessary to perform these checks if q is larger than p.An
    application that calls DH_check() and supplies a key or parameters
    obtainedfrom an untrusted source could be vulnerable to a Denial of
    Service attack.The function DH_check() is itself called by a number
    of other OpenSSL functions.An application calling any of those other
    functions may similarly be affected.The other functions affected
    by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable
    are the OpenSSL dhparam and pkeyparam command line applicationswhen
    using the "-check" option.The OpenSSL SSL/TLS implementation is not
    affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not
    affected by this issue.

- Vulnerability: CVE-2021-32786

– CVSS Score: 5.8

– Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, `oidc_validate_redirect_url()` does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring `mod_auth_openidc` to only allow redirection whose destination matches a given regular expression.

• Vulnerability: CVE-2021-32785

– CVSS Score: 4.3

– Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache (`OIDCCacheEncrypt off`, `OIDCSessionType server-cache`, `OIDCCacheType redis`), `mod_auth_openidc` wrongly performed argument interpolation before passing Redis requests to `hiredis`, which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the `hiredis` API. As a workaround, this vulnerability can be mitigated by setting `OIDCCacheEncrypt` to `on`, as cache keys are cryptographically hashed before use when this option is enabled.

• Vulnerability: CVE-2020-9490

– CVSS Score: 5

– Description: Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.

• Vulnerability: CVE-2007-4723

– CVSS Score: 7.5

– Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

• Vulnerability: CVE-2020-7060

– CVSS Score: 6.4

– Description: When using certain mbstring functions to convert multibyte encodings, in PHP versions 7.2.x below 7.2.27, 7.3.x below 7.3.14 and 7.4.x below 7.4.2 it is possible to supply data that will cause function mbfl_filt_conv_big5_wchar to read past the allocated buffer. This may lead to information disclosure or crash.

- Vulnerability: CVE-2021-44790

  – CVSS Score: 7.5

  – Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

- Vulnerability: CVE-2020-7062

  – CVSS Score: 4.3

  – Description: In PHP versions 7.2.x below 7.2.28, 7.3.x below 7.3.15 and 7.4.x below 7.4.3, when using file upload functionality, if upload progress tracking is enabled, but session.upload_progress.cleanup is set to 0 (disabled), and the file upload fails, the upload procedure would try to clean up data that does not exist and encounter null pointer dereference, which would likely lead to a crash.

- Vulnerability: CVE-2020-7063

  – CVSS Score: 5

  – Description: In PHP versions 7.2.x below 7.2.28, 7.3.x below 7.3.15 and 7.4.x below 7.4.3, when creating PHAR archive using PharData::buildFromIterator() function, the files are added with default permissions (0666, or all access) even if the original files on the filesystem were with more restrictive permissions. This may result in files having more lax permissions than intended when such archive is extracted.

- Vulnerability: CVE-2020-7064

  – CVSS Score: 5.8

  – Description: In PHP versions 7.2.x below 7.2.9, 7.3.x below 7.3.16 and 7.4.x below 7.4.4, while parsing EXIF data with exif_read_data() function, it is possible for malicious data to cause PHP to read one byte of uninitialized memory. This could potentially lead to information disclosure or crash.

- Vulnerability: CVE-2020-7066

  – CVSS Score: 4.3

  – Description: In PHP versions 7.2.x below 7.2.29, 7.3.x below 7.3.16 and 7.4.x below 7.4.4, while using get_headers() with user-supplied URL, if the URL contains zero (\{}0) character, the URL will be silently truncated at it. This may cause some software to make incorrect assumptions about the target of the get_headers() and possibly send some information to a wrong server.

- Vulnerability: CVE-2020-7067

  – CVSS Score: 5

  – Description: In PHP versions 7.2.x below 7.2.30, 7.3.x below 7.3.17 and 7.4.x below 7.4.5, if PHP is compiled with EBCDIC support (uncommon), urldecode() function can be made to access locations past the allocated memory, due to erroneously using signed numbers as array indexes.

- Vulnerability: CVE-2020-7068

  – CVSS Score: 3.3

- Description: In PHP versions 7.2.x below 7.2.33, 7.3.x below 7.3.21 and 7.4.x below 7.4.9, while processing PHAR files using phar extension, phar_parse_zipfile could be tricked into accessing freed memory, which could lead to a crash or information disclosure.

- **Vulnerability: CVE-2020-7069**

  - CVSS Score: 6.4
  - Description: In PHP versions 7.2.x below 7.2.34, 7.3.x below 7.3.23 and 7.4.x below 7.4.11, when AES-CCM mode is used with openssl_encrypt() function with 12 bytes IV, only first 7 bytes of the IV is actually used. This can lead to both decreased security and incorrect encryption data.

- **Vulnerability: CVE-2022-37436**

  - CVSS Score: N/A
  - Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- **Vulnerability: CVE-2020-13938**

  - CVSS Score: 2.1
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

- **Vulnerability: CVE-2023-2650**

  - CVSS Score: N/A

- Description: Issue summary: Processing some specially crafted ASN.1 object
  identifiers ordata containing them may be very slow.Impact summary:
  Applications that use OBJ_obj2txt() directly, or use any ofthe
  OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with
  no messagesize limit may experience notable to very long delays
  when processing thosemessages, which may lead to a Denial of
  Service.An OBJECT IDENTIFIER is composed of a series of numbers –
  sub-identifiers -most of which have no size limit. OBJ_obj2txt() may
  be used to translatean ASN.1 OBJECT IDENTIFIER given in DER encoding
  form (using the OpenSSLtype ASN1_OBJECT) to its canonical numeric
  text form, which are thesub-identifiers of the OBJECT IDENTIFIER in
  decimal form, separated byperiods.When one of the sub-identifiers in
  the OBJECT IDENTIFIER is very large(these are sizes that are seen as
  absurdly large, taking up tens or hundredsof KiBs), the translation
  to a decimal number in text may take a very longtime. The time
  complexity is $O(n^2)$ with 'n' being the size of thesub-identifiers
  in bytes (*).With OpenSSL 3.0, support to fetch cryptographic
  algorithms using names /identifiers in string form was introduced.
  This includes using OBJECTIDENTIFIERs in canonical numeric text form
  as identifiers for fetchingalgorithms.Such OBJECT IDENTIFIERs may
  be received through the ASN.1 structureAlgorithmIdentifier, which
  is commonly used in multiple protocols to specifywhat cryptographic
  algorithm should be used to sign or verify, encrypt ordecrypt, or
  digest passed data.Applications that call OBJ_obj2txt() directly
  with untrusted data areaffected, with any version of OpenSSL. If the
  use is for the mere purposeof display, the severity is considered
  low.In OpenSSL 3.0 and newer, this affects the subsystems OCSP,
  PKCS7/SMIME,CMS, CMP/CRMF or TS. It also impacts anything that
  processes X.509certificates, including simple things like verifying
  its signature.The impact on TLS is relatively low, because all
  versions of OpenSSL have a100KiB limit on the peer's certificate
  chain. Additionally, this onlyimpacts clients, or servers that
  have explicitly enabled clientauthentication.In OpenSSL 1.1.1 and
  1.0.2, this only affects displaying diverse objects,such as X.509
  certificates. This is assumed to not happen in such a waythat it
  would cause a Denial of Service, so these versions are considerednot
  affected by this issue in such a way that it would be cause for
  concern,and the severity is therefore considered low.

- Vulnerability: CVE-2023-0215

  - CVSS Score: N/A

- Description: The public API function BIO_new_NDEF is a helper function used for streamingASN.1 data via a BIO. It is primarily used internally to OpenSSL to support theSMIME, CMS and PKCS7 streaming capabilities, but may also be called directly byend user applications.The function receives a BIO from the caller, prepends a new BIO_f_asn1 filterBIO onto the front of it to form a BIO chain, and then returns the new head ofthe BIO chain to the caller. Under certain conditions, for example if a CMSrecipient public key is invalid, the new filter BIO is freed and the functionreturns a NULL result indicating a failure. However, in this case, the BIO chainis not properly cleaned up and the BIO passed by the caller still retainsinternal pointers to the previously freed filter BIO. If the caller then goes onto call BIO_pop() on the BIO then a use-after-free will occur. This will mostlikely result in a crash.This scenario occurs directly in the internal function B64_write_ASN1() whichmay cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() onthe BIO. This internal function is in turn called by the public API functionsPEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream,SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7.Other public API functions that may be impacted by this includei2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream andi2d_PKCS7_bio_stream.The OpenSSL cms and smime command line applications are similarly affected.

- Vulnerability: CVE-2019-9517

  - CVSS Score: 7.8
  - Description: Some HTTP/2 implementations are vulnerable to unconstrained interal data buffering, potentially leading to a denial of service. The attacker opens the HTTP/2 window so the peer can send without constraint; however, they leave the TCP window closed so the peer cannot actually write (many of) the bytes on the wire. The attacker then sends a stream of requests for a large response object. Depending on how the servers queue the responses, this can consume excess memory, CPU, or both.

- Vulnerability: CVE-2020-35452

  - CVSS Score: 6.8
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

- Vulnerability: CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2022-31628

  - CVSS Score: N/A
  - Description: In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the phar uncompressor code would recursively uncompress "quines" gzip files, resulting in an infinite loop.

- Vulnerability: CVE-2022-31629

- CVSS Score: N/A
- Description: In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the vulnerability enables network and same-site attackers to set a standard insecure cookie in the victim's browser which is treated as a '__Host-' or '__Secure-' cookie by PHP applications.

- Vulnerability: CVE-2020-1934

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

- Vulnerability: CVE-2022-36760

  - CVSS Score: N/A
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-4304

  - CVSS Score: N/A
  - Description: A timing based side channel exists in the OpenSSL RSA Decryption implementationwhich could be sufficient to recover a plaintext across a network in aBleichenbacher style attack. To achieve a successful decryption an attackerwould have to be able to send a very large number of trial messages fordecryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5,RSA-OEAP and RSASVE.For example, in a TLS connection, RSA is commonly used by a client to send anencrypted pre-master secret to the server. An attacker that had observed agenuine connection between a client and a server could use this flaw to sendtrial messages to the server and record the time taken to process them. After asufficiently large number of messages the attacker could recover the pre-mastersecret used for the original connection and thus be able to decrypt theapplication data sent over that connection.

- Vulnerability: CVE-2017-8923

  - CVSS Score: 7.5
  - Description: The zend_string_extend function in Zend/zend_string.h in PHP through 7.1.5 does not prevent changes to string objects that result in a negative length, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact by leveraging a script's use of .= with a long string.

- Vulnerability: CVE-2019-0217

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.

- Vulnerability: CVE-2019-0197

  - CVSS Score: 4.9

- Description: A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38.
  When HTTP/2 was enabled for a http: host or H2Upgrade was enabled
  for h2 on a https: host, an Upgrade request from http/1.1 to
  http/2 that was not the first request on a connection could lead
  to a misconfiguration and crash. Server that never enabled the
  h2 protocol or that only enabled it for https: and did not set
  "H2Upgrade on" are unaffected by this issue.

- Vulnerability: CVE-2019-0196

  - CVSS Score: 5

  - Description: A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38.
    Using fuzzed network input, the http/2 request handling could be
    made to access freed memory in string comparison when determining the
    method of a request and thus process the request incorrectly.

- Vulnerability: CVE-2019-0190

  - CVSS Score: 5

  - Description: A bug exists in the way mod_ssl handled client renegotiations. A
    remote attacker could send a carefully crafted request that would
    cause mod_ssl to enter a loop leading to a denial of service. This
    bug can be only triggered with Apache HTTP Server version 2.4.37
    when using OpenSSL version 1.1.1 or later, due to an interaction in
    changes to handling of renegotiation attempts.

- Vulnerability: CVE-2021-33193

  - CVSS Score: 5

  - Description: A crafted method sent through HTTP/2 will bypass validation and be
    forwarded by mod_proxy, which can lead to request splitting or cache
    poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.

- Vulnerability: CVE-2019-0211

  - CVSS Score: 7.2

  - Description: In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event,
    worker or prefork, code executing in less-privileged child processes
    or threads (including scripts executed by an in-process scripting
    interpreter) could execute arbitrary code with the privileges of
    the parent process (usually root) by manipulating the scoreboard.
    Non-Unix systems are not affected.

- Vulnerability: CVE-2019-17567

  - CVSS Score: 5

  - Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel
    configured on an URL that is not necessarily Upgraded by the origin
    server was tunneling the whole connection regardless, thus allowing
    for subsequent requests on the same connection to pass through
    with no HTTP validation, authentication or authorization possibly
    configured.

- Vulnerability: CVE-2022-31813

  - CVSS Score: 7.5

  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-*
    headers to the origin server based on client side Connection
    header hop-by-hop mechanism. This may be used to bypass IP based
    authentication on the origin server/application.

- Vulnerability: CVE-2013-2220

- CVSS Score: 7.5
- Description: Buffer overflow in the radius_get_vendor_attr function in the Radius extension before 1.2.7 for PHP allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a large Vendor Specific Attributes (VSA) length value.

- Vulnerability: CVE-2012-4360

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2023-4807

  - CVSS Score: N/A
  - Description: Issue summary: The POLY1305 MAC (message authentication code) implementationcontains a bug that might corrupt the internal state of applications on theWindows 64 platform when running on newer X86_64 processors supporting theAVX512-IFMA instructions.Impact summary: If in an application that uses the OpenSSL library an attackercan influence whether the POLY1305 MAC algorithm is used, the applicationstate might be corrupted with various application dependent consequences.The POLY1305 MAC (message authentication code) implementation in OpenSSL doesnot save the contents of non-volatile XMM registers on Windows 64 platformwhen calculating the MAC of data larger than 64 bytes. Before returning tothe caller all the XMM registers are set to zero rather than restoring theirprevious content. The vulnerable code is used only on newer x86_64 processorssupporting the AVX512-IFMA instructions.The consequences of this kind of internal application state corruption canbe various – from no consequences, if the calling application does notdepend on the contents of non-volatile XMM registers at all, to the worstconsequences, where the attacker could get complete control of the applicationprocess. However given the contents of the registers are just zeroized sothe attacker cannot put arbitrary values inside, the most likely consequence,if any, would be an incorrect result of some application dependentcalculations or a crash leading to a denial of service.The POLY1305 MAC algorithm is most frequently used as part of theCHACHA20-POLY1305 AEAD (authenticated encryption with associated data)algorithm. The most common usage of this AEAD cipher is with TLS protocolversions 1.2 and 1.3 and a malicious client can influence whether this AEADcipher is used by the server. This implies that server applications usingOpenSSL can be potentially impacted. However we are currently not aware ofany concrete application that would be affected by this issue therefore weconsider this a Low severity security issue.As a workaround the AVX512-IFMA instructions support can be disabled atruntime by setting the environment variable OPENSSL_ia32cap: OPENSSL_ia32cap=:~0x200000The FIPS provider is not affected by this issue.

- Vulnerability: CVE-2009-3767

  - CVSS Score: 4.3
  - Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other versions, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2021-26690

  – CVSS Score: 5
  – Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted
    Cookie header handled by mod_session can cause a NULL pointer
    dereference and crash, leading to a possible Denial Of Service

- Vulnerability: CVE-2021-26691

  – CVSS Score: 7.5
  – Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted
    SessionHeader sent by an origin server could cause a heap overflow

- Vulnerability: CVE-2019-0220

  – CVSS Score: 5
  – Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38.
    When the path component of a request URL contains multiple
    consecutive slashes ('/'), directives such as LocationMatch and
    RewriteRule must account for duplicates in regular expressions while
    other aspects of the servers processing will implicitly collapse
    them.

- Vulnerability: CVE-2024-38477

  – CVSS Score: N/A
  – Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59
    and earlier allows an attacker to crash the server via a malicious
    request.Users are recommended to upgrade to version 2.4.60, which
    fixes this issue.

- Vulnerability: CVE-2024-38474

  – CVSS Score: N/A
  – Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server
    2.4.59 and earlier allows attacker to execute scripts indirectories
    permitted by the configuration but not directly reachable by anyURL
    or source disclosure of scripts meant to only to be executed as
    CGI.Users are recommended to upgrade to version 2.4.60, which fixes
    this issue.Some RewriteRules that capture and substitute unsafely
    will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2021-39275

  – CVSS Score: 7.5
  – Description: ap_escape_quotes() may write beyond the end of a buffer when given
    malicious input. No included modules pass untrusted data to these
    functions, but third-party / external modules may. This issue
    affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2018-17189

  – CVSS Score: 5
  – Description: In Apache HTTP server versions 2.4.37 and prior, by sending request
    bodies in a slow loris way to plain resources, the h2 stream for
    that request unnecessarily occupied a server thread cleaning up that
    incoming data. This affects only HTTP/2 (mod_http2) connections.

- Vulnerability: CVE-2022-29404

  – CVSS Score: 5
  – Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a
    lua script that calls r:parsebody(0) may cause a denial of service
    due to no default limit on possible input size.

- Vulnerability: CVE-2022-37454

  - CVSS Score: N/A
  - Description: The Keccak XKCP SHA-3 reference implementation before fdc6fef has an integer overflow and resultant buffer overflow that allows attackers to execute arbitrary code or eliminate expected cryptographic properties. This occurs in the sponge function interface.

- Vulnerability: CVE-2007-3205

  - CVSS Score: 5
  - Description: The parse_str function in (1) PHP, (2) Hardened-PHP, and (3) Suhosin, when called without a second parameter, might allow remote attackers to overwrite arbitrary variables by specifying variable names and values in the string to be parsed. NOTE: it is not clear whether this is a design limitation of the function or a bug in PHP, although it is likely to be regarded as a bug in Hardened-PHP and Suhosin.

- Vulnerability: CVE-2020-11993

  - CVSS Score: 4.3
  - Description: Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2019-10092

  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

- Vulnerability: CVE-2022-2068

  - CVSS Score: 10
  - Description: In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze).

- Vulnerability: CVE-2009-3766

  - CVSS Score: 6.8

- Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when OpenSSL is used, does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

- Vulnerability: CVE-2021-44224

  - CVSS Score: 6.4
  - Description: A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).

- Vulnerability: CVE-2009-3765

  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2022-22721

  - CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2006-20001

  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2021-3711

  - CVSS Score: 7.5

- Description: In order to decrypt SM2 encrypted data an application is expected to call the API function EVP_PKEY_decrypt(). Typically an application will call this function twice. The first time, on entry, the "out" parameter can be NULL and, on exit, the "outlen" parameter is populated with the buffer size required to hold the decrypted plaintext. The application can then allocate a sufficiently sized buffer and call EVP_PKEY_decrypt() again, but this time passing a non-NULL value for the "out" parameter. A bug in the implementation of the SM2 decryption code means that the calculation of the buffer size required to hold the plaintext returned by the first call to EVP_PKEY_decrypt() can be smaller than the actual size required by the second call. This can lead to a buffer overflow when EVP_PKEY_decrypt() is called by the application a second time with a buffer that is too small. A malicious attacker who is able present SM2 content for decryption to an application could cause attacker chosen data to overflow the buffer by up to a maximum of 62 bytes altering the contents of other data held after the buffer, possibly changing application behaviour or causing the application to crash. The location of the buffer is application dependent but is typically heap allocated. Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k).

- Vulnerability: CVE-2021-3712

  - CVSS Score: 5.8
  - Description: ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own "d2i" functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the "data" and "length" fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the "data" field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). It can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y).

- Vulnerability: CVE-2023-0464

- CVSS Score: N/A
- Description: A security vulnerability has been identified in all supported versionsof OpenSSL related to the verification of X.509 certificate chainsthat include policy constraints. Attackers may be able to exploit thisvulnerability by creating a malicious certificate chain that triggersexponential use of computational resources, leading to a denial-of-service(DoS) attack on affected systems.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0465

  - CVSS Score: N/A
  - Description: Applications that use a non-default option when verifying certificates may bevulnerable to an attack from a malicious CA to circumvent certain checks.Invalid certificate policies in leaf certificates are silently ignored byOpenSSL and other certificate policy checks are skipped for that certificate.A malicious CA could use this to deliberately assert invalid certificate policiesin order to circumvent policy checking on the certificate altogether.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0466

  - CVSS Score: N/A
  - Description: The function X509_VERIFY_PARAM_add0_policy() is documented toimplicitly enable the certificate policy check when doing certificateverification. However the implementation of the function does notenable the check which allows certificates with invalid or incorrectpolicies to pass the certificate verification.As suddenly enabling the policy check could break existing deployments it wasdecided to keep the existing behavior of the X509_VERIFY_PARAM_add0_policy()function.Instead the applications that require OpenSSL to perform certificatepolicy check need to use X509_VERIFY_PARAM_set1_policies() or explicitlyenable the policy check by calling X509_VERIFY_PARAM_set_flags() withthe X509_V_FLAG_POLICY_CHECK flag argument.Certificate policy checks are disabled by default in OpenSSL and are notcommonly used by applications.

- Vulnerability: CVE-2019-10098

  - CVSS Score: 5.8
  - Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.

- Vulnerability: CVE-2019-10097

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4.32-2.4.39, when mod_remoteip was configured to use a trusted intermediary proxy server using the "PROXY" protocol, a specially crafted PROXY header could trigger a stack buffer overflow or NULL pointer deference. This vulnerability could only be triggered by a trusted proxy and not by untrusted HTTP clients.

- Vulnerability: CVE-2021-40438
  - CVSS Score: 6.8
  - Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2011-1176
  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2022-23943
  - CVSS Score: 7.5
  - Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

- Vulnerability: CVE-2018-17199
  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

- Vulnerability: CVE-2022-22720
  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2021-34798
  - CVSS Score: 5
  - Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2023-25690
  - CVSS Score: N/A
  - Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2020-11984

  - CVSS Score: 7.5
  - Description: Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE

- Vulnerability: CVE-2021-4160

  - CVSS Score: 4.3
  - Description: There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that is available to premium support customers only. It will be made available in 1.0.2zc when it is released. The issue only affects OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0). Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL 1.0.2zc-dev (Affected 1.0.2-1.0.2zb).

- Vulnerability: CVE-2022-26377

  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2019-10081

  - CVSS Score: 5
  - Description: HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example configured with "H2PushResource", could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client.

- Vulnerability: CVE-2019-10082

  - CVSS Score: 6.4
  - Description: In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.

- Vulnerability: CVE-2024-40898

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2022-0778

  - CVSS Score: 5
  - Description: The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - TLS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

- Vulnerability: CVE-2022-2097

  - CVSS Score: 5
  - Description: AES OCB mode for 32-bit x86 platforms using the AES-NI assembly optimised implementation will not encrypt the entirety of the data under some circumstances. This could reveal sixteen bytes of data that was preexisting in the memory that wasn't written. In the special case of "in place" encryption, sixteen bytes of the plaintext would be revealed. Since OpenSSL does not support OCB based cipher suites for TLS and DTLS, they are both unaffected. Fixed in OpenSSL 3.0.5 (Affected 3.0.0-3.0.4). Fixed in OpenSSL 1.1.1q (Affected 1.1.1-1.1.1p).

- Vulnerability: CVE-2023-27522

  - CVSS Score: N/A
  - Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.Special characters in the origin response header can truncate/split the response forwarded to the client.

- Vulnerability: CVE-2009-1390

  - CVSS Score: 6.8

- Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2)
  GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS
  certificate in the chain is accepted instead of verifying the entire
  chain, which allows remote attackers to spoof trusted servers via a
  man-in-the-middle attack.

- Vulnerability: CVE-2012-3526

  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the
    Apache HTTP Server allows remote attackers to cause a denial of
    service (server or application crash) via multiple X-Forwarded-For
    headers in a request.

- Vulnerability: CVE-2020-7059

  - CVSS Score: 6.4
  - Description: When using fgetss() function to read data with stripping tags, in PHP
    versions 7.2.x below 7.2.27, 7.3.x below 7.3.14 and 7.4.x below 7.4.2
    it is possible to supply data that will cause this function to read
    past the allocated buffer. This may lead to information disclosure
    or crash.

- Vulnerability: CVE-2023-5678

  - CVSS Score: N/A
  - Description: Issue summary: Generating excessively long X9.42 DH keys or
    checkingexcessively long X9.42 DH keys or parameters may be
    very slow.Impact summary: Applications that use the functions
    DH_generate_key() togenerate an X9.42 DH key may experience
    long delays. Likewise, applicationsthat use DH_check_pub_key(),
    DH_check_pub_key_ex() or EVP_PKEY_public_check()to check an
    X9.42 DH key or X9.42 DH parameters may experience long
    delays.Where the key or parameters that are being checked have
    been obtained froman untrusted source this may lead to a Denial
    of Service.While DH_check() performs all the necessary checks
    (as of CVE-2023-3817),DH_check_pub_key() doesn't make any of
    these checks, and is thereforevulnerable for excessively large
    P and Q parameters.Likewise, while DH_generate_key() performs
    a check for an excessively largeP, it doesn't check for an
    excessively large Q.An application that calls DH_generate_key() or
    DH_check_pub_key() andsupplies a key or parameters obtained from
    an untrusted source could bevulnerable to a Denial of Service
    attack.DH_generate_key() and DH_check_pub_key() are also called by
    a number ofother OpenSSL functions. An application calling any of
    those otherfunctions may similarly be affected. The other functions
    affected by thisare DH_check_pub_key_ex(), EVP_PKEY_public_check(), and
    EVP_PKEY_generate().Also vulnerable are the OpenSSL pkey command line
    application when using the"-pubcheck" option, as well as the OpenSSL
    genpkey command line application.The OpenSSL SSL/TLS implementation
    is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers
    are not affected by this issue.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module
    before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before
    3.1.1-11637, a module for the Apache HTTP Server, allows remote
    attackers to cause a denial of service (memory consumption) via an
    HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2022-1292

  – CVSS Score: 10
  – Description: The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n). Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).

- Vulnerability: CVE-2019-11048

  – CVSS Score: 5
  – Description: In PHP versions 7.2.x below 7.2.31, 7.3.x below 7.3.18 and 7.4.x below 7.4.6, when HTTP file uploads are allowed, supplying overly long filenames or field names could lead PHP engine to try to allocate oversized memory storage, hit the memory limit and stop processing the request, without cleaning up temporary files created by upload request. This potentially could lead to accumulation of uncleaned temporary files exhausting the disk space on the target server.

- Vulnerability: CVE-2012-4001

  – CVSS Score: 5
  – Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2019-11046

  – CVSS Score: 5
  – Description: In PHP versions 7.2.x below 7.2.26, 7.3.x below 7.3.13 and 7.4.0, PHP bcmath extension functions on some systems, including Windows, can be tricked into reading beyond the allocated space by supplying it with string containing characters that are identified as numeric by the OS but aren't ASCII numbers. This can read to disclosure of the content of some memory locations.

- Vulnerability: CVE-2019-11047

  – CVSS Score: 6.4
  – Description: When PHP EXIF extension is parsing EXIF information from an image, e.g. via exif_read_data() function, in PHP versions 7.2.x below 7.2.26, 7.3.x below 7.3.13 and 7.4.0 it is possible to supply it with data what will cause it to read past the allocated buffer. This may lead to information disclosure or crash.

- Vulnerability: CVE-2019-11044

  – CVSS Score: 5
  – Description: In PHP versions 7.2.x below 7.2.26, 7.3.x below 7.3.13 and 7.4.0 on Windows, PHP link() function accepts filenames with embedded \{}0 byte and treats them as terminating at that byte. This could lead to security vulnerabilities, e.g. in applications checking paths that the code is allowed to access.

- Vulnerability: CVE-2019-11045

- CVSS Score: 4.3
- Description: In PHP versions 7.2.x below 7.2.26, 7.3.x below 7.3.13 and 7.4.0, PHP DirectoryIterator class accepts filenames with embedded \{}0 byte and treats them as terminating at that byte. This could lead to security vulnerabilities, e.g. in applications checking paths that the code is allowed to access.

- Vulnerability: CVE-2022-4450

  - CVSS Score: N/A
  - Description: The function PEM_read_bio_ex() reads a PEM file from a BIO and parses anddecodes the "name" (e.g. "CERTIFICATE"), any header data and the payload data.If the function succeeds then the "name_out", "header" and "data" arguments arepopulated with pointers to buffers containing the relevant decoded data. Thecaller is responsible for freeing those buffers. It is possible to construct aPEM file that results in 0 bytes of payload data. In this case PEM_read_bio_ex()will return a failure code but will populate the header argument with a pointerto a buffer that has already been freed. If the caller also frees this bufferthen a double free will occur. This will most likely lead to a crash. Thiscould be exploited by an attacker who has the ability to supply malicious PEMfiles for parsing to achieve a denial of service attack.The functions PEM_read_bio() and PEM_read() are simple wrappers aroundPEM_read_bio_ex() and therefore these functions are also directly affected.These functions are also called indirectly by a number of other OpenSSLfunctions including PEM_X509_INFO_read_bio_ex() andSSL_CTX_use_serverinfo_file() which are also vulnerable. Some OpenSSL internaluses of these functions are not vulnerable because the caller does not free theheader argument if PEM_read_bio_ex() returns a failure code. These locationsinclude the PEM_read_bio_TYPE() functions as well as the decoders introduced inOpenSSL 3.0.The OpenSSL asn1parse command line application is also impacted by this issue.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

- CVSS Score: 4.3

- Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2019-11050

  - CVSS Score: 6.4

  - Description: When PHP EXIF extension is parsing EXIF information from an image, e.g. via exif_read_data() function, in PHP versions 7.2.x below 7.2.26, 7.3.x below 7.3.13 and 7.4.0 it is possible to supply it with data what will cause it to read past the allocated buffer. This may lead to information disclosure or crash.

- Vulnerability: CVE-2023-45802

  - CVSS Score: N/A

  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5

  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- Vulnerability: CVE-2022-28615

  - CVSS Score: 6.4

  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- Vulnerability: CVE-2022-28614

  - CVSS Score: 5

  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

11.4 IP Address: 159.149.133.208

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 5

- High Vulnerabilities: 26

- Medium Vulnerabilities: 110

- Low Vulnerabilities: 7

- Total Vulnerabilities: 148

Services Running on IP Address

- Service: OpenSSH

  – Port: 22
  – Version: 8.0
  – Location:

- Service: Apache httpd

  – Port: 80
  – Version: 2.4.37
  – Location: /

- Service: Apache httpd

  – Port: 443
  – Version: 2.4.37
  – Location: /

- Service: PostgreSQL

  – Port: 5432
  – Version: 10.19 - 10.23
  – Location:

Vulnerabilities Found

- Vulnerability: CVE-2019-16905

  – CVSS Score: 4.4
  – Description: OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an
    experimental key type, has a pre-authentication integer overflow if a
    client or server is configured to use a crafted XMSS key. This leads
    to memory corruption and local code execution because of an error
    in the XMSS key parsing algorithm. NOTE: the XMSS implementation is
    considered experimental in all released OpenSSH versions, and there
    is no supported way to enable it when building portable OpenSSH.

- Vulnerability: CVE-2016-20012

  – CVSS Score: 4.3
  – Description: OpenSSH through 8.7 allows remote attackers, who have a suspicion
    that a certain combination of username and public key is known to
    an SSH server, to test whether this suspicion is correct. This
    occurs because a challenge is sent only when that combination could
    be valid for a login session. NOTE: the vendor does not recognize
    user enumeration as a vulnerability for this product

- Vulnerability: CVE-2021-36368

  – CVSS Score: 2.6
  – Description: An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is "this is not an authentication bypass, since nothing is being bypassed.

- Vulnerability: CVE-2020-14145

  – CVSS Score: 4.3
  – Description: The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.

- Vulnerability: CVE-2023-51767

  – CVSS Score: N/A
  – Description: OpenSSH through 9.6, when common types of DRAM are used, might allow row hammer attacks (for authentication bypass) because the integer value of authenticated in mm_answer_authpassword does not resist flips of a single bit. NOTE: this is applicable to a certain threat model of attacker-victim co-location in which the attacker has user privileges.

- Vulnerability: CVE-2020-15778

  – CVSS Score: 6.8
  – Description: scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."

- Vulnerability: CVE-2023-48795

  – CVSS Score: N/A

- Description: The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.

- Vulnerability: CVE-2023-38408

  - CVSS Score: N/A
  - Description: The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009.

- Vulnerability: CVE-2007-2768

  - CVSS Score: 4.3
  - Description: OpenSSH, when using OPIE (One-Time Passwords in Everything) for PAM, allows remote attackers to determine the existence of certain user accounts, which displays a different response if the user account exists and is configured to use one-time passwords (OTP), a similar issue to CVE-2007-2243.

- Vulnerability: CVE-2021-41617

  - CVSS Score: 4.4
  - Description: sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

- Vulnerability: CVE-2023-51385

- CVSS Score: N/A
- Description: In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.

- Vulnerability: CVE-2008-3844

  - CVSS Score: 9.3
  - Description: Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, as signed in August 2008 using a legitimate Red Hat GPG key, contain an externally introduced modification (Trojan Horse) that allows the package authors to have an unknown impact. NOTE: since the malicious packages were not distributed from any official Red Hat sources, the scope of this issue is restricted to users who may have obtained these packages through unofficial distribution points. As of 20080827, no unofficial distributions of this software are known.

- Vulnerability: CVE-2019-0215

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in mod_ssl when using per-location client certificate verification with TLSv1.3 allowed a client to bypass configured access control restrictions.

- Vulnerability: CVE-2013-4365

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2022-28330

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2021-32791

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2021-32792

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.

- Vulnerability: CVE-2023-31122

  – CVSS Score: N/A
  – Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP
    Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2024-38476

  – CVSS Score: N/A
  – Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are
    vulnerably to information disclosure, SSRF or local script execution
    viabackend applications whose response headers are malicious or
    exploitable.Users are recommended to upgrade to version 2.4.60, which
    fixes this issue.

- Vulnerability: CVE-2024-27316

  – CVSS Score: N/A
  – Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered
    in nghttp2 in order to generate an informative HTTP 413 response.
    If a client does not stop sending headers, this leads to memory
    exhaustion.

- Vulnerability: CVE-2024-38474

  – CVSS Score: N/A
  – Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server
    2.4.59 and earlier allows attacker to execute scripts indirectories
    permitted by the configuration but not directly reachable by anyURL
    or source disclosure of scripts meant to only to be executed as
    CGI.Users are recommended to upgrade to version 2.4.60, which fixes
    this issue.Some RewriteRules that capture and substitute unsafely
    will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2009-0796

  – CVSS Score: 2.6
  – Description: Cross-site scripting (XSS) vulnerability in Status.pm in
    Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the
    Apache HTTP Server, when /perl-status is accessible, allows remote
    attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2022-2068

  – CVSS Score: 10
  – Description: In addition to the c_rehash shell command injection identified in
    CVE-2022-1292, further circumstances where the c_rehash script
    does not properly sanitise shell metacharacters to prevent command
    injection were found by code review. When the CVE-2022-1292 was
    fixed it was not discovered that there are other places in the
    script where the file names of certificates being hashed were
    possibly passed to a command executed through the shell. This
    script is distributed by some operating systems in a manner where
    it is automatically executed. On such operating systems, an
    attacker could execute arbitrary commands with the privileges of
    the script. Use of the c_rehash script is considered obsolete and
    should be replaced by the OpenSSL rehash command line tool. Fixed in
    OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL
    1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected
    1.0.2-1.0.2ze).

- Vulnerability: CVE-2021-36160

- CVSS Score: 5

- Description: A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS). This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48 (inclusive).

- **Vulnerability:** CVE-2020-1927

  - CVSS Score: 5.8

  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.

- **Vulnerability:** CVE-2023-0286

  - CVSS Score: N/A

  - Description: There is a type confusion vulnerability relating to X.400 address processinginside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING butthe public structure definition for GENERAL_NAME incorrectly specified the typeof the x400Address field as ASN1_TYPE. This field is subsequently interpreted bythe OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than anASN1_STRING.When CRL checking is enabled (i.e. the application sets theX509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to passarbitrary pointers to a memcmp call, enabling them to read memory contents orenact a denial of service. In most cases, the attack requires the attacker toprovide both the certificate chain and CRL, neither of which need to have avalid signature. If the attacker only controls one of these inputs, the otherinput must already contain an X.400 address as a CRL distribution point, whichis uncommon. As such, this vulnerability is most likely to only affectapplications which have implemented their own functionality for retrieving CRLsover a network.

- **Vulnerability:** CVE-2023-3817

  - CVSS Score: N/A

  - Description: Issue summary: Checking excessively long DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH key or DH parameters may experience longdelays. Where the key or parameters that are being checked have been obtainedfrom an untrusted source this may lead to a Denial of Service.The function DH_check() performs various checks on DH parameters. After fixingCVE-2023-3446 it was discovered that a large q parameter value can also triggeran overly long computation during some of these checks. A correct q value,if present, cannot be larger than the modulus p parameter, thus it isunnecessary to perform these checks if q is larger than p.An application that calls DH_check() and supplies a key or parameters obtainedfrom an untrusted source could be vulnerable to a Denial of Service attack.The function DH_check() is itself called by a number of other OpenSSL functions.An application calling any of those other functions may similarly be affected.The other functions affected by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable are the OpenSSL dhparam and pkeyparam command line applicationswhen using the "-check" option.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- **Vulnerability:** CVE-2021-32786

- CVSS Score: 5.8
- Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, 'oidc_validate_redirect_url()' does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring 'mod_auth_openidc' to only allow redirection whose destination matches a given regular expression.

- Vulnerability: CVE-2021-32785

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache ('OIDCCacheEncrypt off', 'OIDCSessionType server-cache', 'OIDCCacheType redis'), 'mod_auth_openidc' wrongly performed argument interpolation before passing Redis requests to 'hiredis', which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the 'hiredis' API. As a workaround, this vulnerability can be mitigated by setting 'OIDCCacheEncrypt' to 'on', as cache keys are cryptographically hashed before use when this option is enabled.

- Vulnerability: CVE-2020-9490

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2021-44790

  - CVSS Score: 7.5
  - Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

- Vulnerability: CVE-2020-13938

  – CVSS Score: 2.1
  – Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

- Vulnerability: CVE-2023-2650

  – CVSS Score: N/A
  – Description: Issue summary: Processing some specially crafted ASN.1 object identifiers ordata containing them may be very slow.Impact summary: Applications that use OBJ_obj2txt() directly, or use any ofthe OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no messagesize limit may experience notable to very long delays when processing thosemessages, which may lead to a Denial of Service.An OBJECT IDENTIFIER is composed of a series of numbers – sub-identifiers -most of which have no size limit. OBJ_obj2txt() may be used to translatean ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSLtype ASN1_OBJECT) to its canonical numeric text form, which are thesub-identifiers of the OBJECT IDENTIFIER in decimal form, separated byperiods.When one of the sub-identifiers in the OBJECT IDENTIFIER is very large(these are sizes that are seen as absurdly large, taking up tens or hundredsof KiBs), the translation to a decimal number in text may take a very longtime. The time complexity is $O(n\hat{2})$ with 'n' being the size of thesub-identifiers in bytes (*).With OpenSSL 3.0, support to fetch cryptographic algorithms using names /identifiers in string form was introduced. This includes using OBJECTIDENTIFIERs in canonical numeric text form as identifiers for fetchingalgorithms.Such OBJECT IDENTIFIERs may be received through the ASN.1 structureAlgorithmIdentifier, which is commonly used in multiple protocols to specifywhat cryptographic algorithm should be used to sign or verify, encrypt ordecrypt, or digest passed data.Applications that call OBJ_obj2txt() directly with untrusted data areaffected, with any version of OpenSSL. If the use is for the mere purposeof display, the severity is considered low.In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME,CMS, CMP/CRMF or TS. It also impacts anything that processes X.509certificates, including simple things like verifying its signature.The impact on TLS is relatively low, because all versions of OpenSSL have a100KiB limit on the peer's certificate chain. Additionally, this onlyimpacts clients, or servers that have explicitly enabled clientauthentication.In OpenSSL 1.1.1 and 1.0.2, this only affects displaying diverse objects,such as X.509 certificates. This is assumed to not happen in such a waythat it would cause a Denial of Service, so these versions are considerednot affected by this issue in such a way that it would be cause for concern,and the severity is therefore considered low.

- Vulnerability: CVE-2023-0215

  – CVSS Score: N/A

– Description: The public API function BIO_new_NDEF is a helper function used for streamingASN.1 data via a BIO. It is primarily used internally to OpenSSL to support theSMIME, CMS and PKCS7 streaming capabilities, but may also be called directly byend user applications.The function receives a BIO from the caller, prepends a new BIO_f_asn1 filterBIO onto the front of it to form a BIO chain, and then returns the new head ofthe BIO chain to the caller. Under certain conditions, for example if a CMSrecipient public key is invalid, the new filter BIO is freed and the functionreturns a NULL result indicating a failure. However, in this case, the BIO chainis not properly cleaned up and the BIO passed by the caller still retainsinternal pointers to the previously freed filter BIO. If the caller then goes onto call BIO_pop() on the BIO then a use-after-free will occur. This will mostlikely result in a crash.This scenario occurs directly in the internal function B64_write_ASN1() whichmay cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() onthe BIO. This internal function is in turn called by the public API functionsPEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream,SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7.Other public API functions that may be impacted by this includei2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream andi2d_PKCS7_bio_stream.The OpenSSL cms and smime command line applications are similarly affected.

- Vulnerability: CVE-2020-35452

  – CVSS Score: 6.8
  – Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

- Vulnerability: CVE-2022-22719

  – CVSS Score: 5
  – Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2020-1934

  – CVSS Score: 5
  – Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

- Vulnerability: CVE-2022-36760

  – CVSS Score: N/A
  – Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-4304

  – CVSS Score: N/A

- Description: A timing based side channel exists in the OpenSSL RSA Decryption implementationwhich could be sufficient to recover a plaintext across a network in aBleichenbacher style attack. To achieve a successful decryption an attackerwould have to be able to send a very large number of trial messages fordecryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5,RSA-OEAP and RSASVE.For example, in a TLS connection, RSA is commonly used by a client to send anencrypted pre-master secret to the server. An attacker that had observed agenuine connection between a client and a server could use this flaw to sendtrial messages to the server and record the time taken to process them. After asufficiently large number of messages the attacker could recover the pre-mastersecret used for the original connection and thus be able to decrypt theapplication data sent over that connection.

- Vulnerability: CVE-2019-9517

  - CVSS Score: 7.8
  - Description: Some HTTP/2 implementations are vulnerable to unconstrained interal data buffering, potentially leading to a denial of service. The attacker opens the HTTP/2 window so the peer can send without constraint; however, they leave the TCP window closed so the peer cannot actually write (many of) the bytes on the wire. The attacker then sends a stream of requests for a large response object. Depending on how the servers queue the responses, this can consume excess memory, CPU, or both.

- Vulnerability: CVE-2019-0217

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.

- Vulnerability: CVE-2019-0197

  - CVSS Score: 4.9
  - Description: A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue.

- Vulnerability: CVE-2019-0196

  - CVSS Score: 5
  - Description: A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.

- Vulnerability: CVE-2019-0190

  - CVSS Score: 5
  - Description: A bug exists in the way mod_ssl handled client renegotiations. A remote attacker could send a carefully crafted request that would cause mod_ssl to enter a loop leading to a denial of service. This bug can be only triggered with Apache HTTP Server version 2.4.37 when using OpenSSL version 1.1.1 or later, due to an interaction in changes to handling of renegotiation attempts.

- Vulnerability: CVE-2021-33193

  - CVSS Score: 5
  - Description: A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.

- Vulnerability: CVE-2019-0211

  - CVSS Score: 7.2
  - Description: In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.

- Vulnerability: CVE-2019-17567

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

- Vulnerability: CVE-2022-31813

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

- Vulnerability: CVE-2012-4360

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2023-4807

  - CVSS Score: N/A

– Description: Issue summary: The POLY1305 MAC (message authentication code) implementationcontains a bug that might corrupt the internal state of applications on theWindows 64 platform when running on newer X86_64 processors supporting theAVX512-IFMA instructions.Impact summary: If in an application that uses the OpenSSL library an attackercan influence whether the POLY1305 MAC algorithm is used, the applicationstate might be corrupted with various application dependent consequences.The POLY1305 MAC (message authentication code) implementation in OpenSSL doesnot save the contents of non-volatile XMM registers on Windows 64 platformwhen calculating the MAC of data larger than 64 bytes.   Before returning tothe caller all the XMM registers are set to zero rather than restoring theirprevious content.   The vulnerable code is used only on newer x86_64 processorssupporting the AVX512-IFMA instructions.The consequences of this kind of internal application state corruption canbe various – from no consequences, if the calling application does notdepend on the contents of non-volatile XMM registers at all, to the worstconsequences, where the attacker could get complete control of the applicationprocess.   However given the contents of the registers are just zeroized sothe attacker cannot put arbitrary values inside, the most likely consequence,if any, would be an incorrect result of some application dependentcalculations or a crash leading to a denial of service.The POLY1305 MAC algorithm is most frequently used as part of theCHACHA20-POLY1305 AEAD (authenticated encryption with associated data)algorithm.   The most common usage of this AEAD cipher is with TLS protocolversions 1.2 and 1.3 and a malicious client can influence whether this AEADcipher is used by the server.   This implies that server applications usingOpenSSL can be potentially impacted.   However we are currently not aware ofany concrete application that would be affected by this issue therefore weconsider this a Low severity security issue.As a workaround the AVX512-IFMA instructions support can be disabled atruntime by setting the environment variable OPENSSL_ia32cap: OPENSSL_ia32cap=:~0x200000The FIPS provider is not affected by this issue.

- Vulnerability: CVE-2009-3767

    – CVSS Score: 4.3
    – Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other versions, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2021-26690

    – CVSS Score: 5
    – Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service

- Vulnerability: CVE-2021-26691

    – CVSS Score: 7.5
    – Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow

- Vulnerability: CVE-2019-0220

- CVSS Score: 5
- Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.

- Vulnerability: CVE-2024-38477

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- Vulnerability: CVE-2021-39275

  - CVSS Score: 7.5
  - Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2018-17189

  - CVSS Score: 5
  - Description: In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 (mod_http2) connections.

- Vulnerability: CVE-2022-29404

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2006-20001

  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2020-11993

  - CVSS Score: 4.3
  - Description: Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2021-3711

  – CVSS Score: 7.5

  – Description: In order to decrypt SM2 encrypted data an application is expected to call the API function EVP_PKEY_decrypt(). Typically an application will call this function twice. The first time, on entry, the "out" parameter can be NULL and, on exit, the "outlen" parameter is populated with the buffer size required to hold the decrypted plaintext. The application can then allocate a sufficiently sized buffer and call EVP_PKEY_decrypt() again, but this time passing a non-NULL value for the "out" parameter. A bug in the implementation of the SM2 decryption code means that the calculation of the buffer size required to hold the plaintext returned by the first call to EVP_PKEY_decrypt() can be smaller than the actual size required by the second call. This can lead to a buffer overflow when EVP_PKEY_decrypt() is called by the application a second time with a buffer that is too small. A malicious attacker who is able present SM2 content for decryption to an application could cause attacker chosen data to overflow the buffer by up to a maximum of 62 bytes altering the contents of other data held after the buffer, possibly changing application behaviour or causing the application to crash. The location of the buffer is application dependent but is typically heap allocated. Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k).

- Vulnerability: CVE-2024-0727

  – CVSS Score: N/A

  – Description: Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSLto crash leading to a potential Denial of Service attackImpact summary: Applications loading files in the PKCS12 format from untrustedsources might terminate abruptly.A file in PKCS12 format can contain certificates and keys and may come from anuntrusted source. The PKCS12 specification allows certain fields to be NULL, butOpenSSL does not correctly check for this case. This can lead to a NULL pointerdereference that results in OpenSSL crashing. If an application processes PKCS12files from an untrusted source using the OpenSSL APIs then that application willbe vulnerable to this issue.OpenSSL APIs that are vulnerable to this are: PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a similar issue in SMIME_write_PKCS7(). However since thisfunction is related to writing data we do not consider it security significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.

- Vulnerability: CVE-2009-3766

  – CVSS Score: 6.8

  – Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when OpenSSL is used, does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

- Vulnerability: CVE-2021-44224

  – CVSS Score: 6.4

- Description: A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).

- Vulnerability: CVE-2009-3765

  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2022-22721

  - CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2022-22720

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2019-10092

  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

- Vulnerability: CVE-2021-3712

  - CVSS Score: 5.8

- Description: ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own "d2i" functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the "data" and "length" fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the "data" field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). It can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y).

- Vulnerability: CVE-2023-0464

  - CVSS Score: N/A

  - Description: A security vulnerability has been identified in all supported versionsof OpenSSL related to the verification of X.509 certificate chainsthat include policy constraints. Attackers may be able to exploit thisvulnerability by creating a malicious certificate chain that triggersexponential use of computational resources, leading to a denial-of-service(DoS) attack on affected systems.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0465

  - CVSS Score: N/A

- Description: Applications that use a non-default option when verifying
  certificates may bevulnerable to an attack from a malicious CA
  to circumvent certain checks.Invalid certificate policies in leaf
  certificates are silently ignored byOpenSSL and other certificate
  policy checks are skipped for that certificate.A malicious CA could
  use this to deliberately assert invalid certificate policiesin order
  to circumvent policy checking on the certificate altogether.Policy
  processing is disabled by default but can be enabled by passingthe
  '-policy' argument to the command line utilities or by calling
  the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0466

  - CVSS Score: N/A
  - Description: The function X509_VERIFY_PARAM_add0_policy() is documented
    toimplicitly enable the certificate policy check when doing
    certificateverification. However the implementation of the
    function does notenable the check which allows certificates
    with invalid or incorrectpolicies to pass the certificate
    verification.As suddenly enabling the policy check could break
    existing deployments it wasdecided to keep the existing behavior of
    the X509_VERIFY_PARAM_add0_policy()function.Instead the applications
    that require OpenSSL to perform certificatepolicy check need
    to use X509_VERIFY_PARAM_set1_policies() or explicitlyenable the
    policy check by calling X509_VERIFY_PARAM_set_flags() withthe
    X509_V_FLAG_POLICY_CHECK flag argument.Certificate policy checks
    are disabled by default in OpenSSL and are notcommonly used by
    applications.

- Vulnerability: CVE-2019-10098

  - CVSS Score: 5.8
  - Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with
    mod_rewrite that were intended to be self-referential might be fooled
    by encoded newlines and redirect instead to an unexpected URL within
    the request URL.

- Vulnerability: CVE-2019-10097

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4.32-2.4.39, when mod_remoteip was configured
    to use a trusted intermediary proxy server using the "PROXY"
    protocol, a specially crafted PROXY header could trigger a stack
    buffer overflow or NULL pointer deference. This vulnerability
    could only be triggered by a trusted proxy and not by untrusted HTTP
    clients.

- Vulnerability: CVE-2021-40438

  - CVSS Score: 6.8
  - Description: A crafted request uri-path can cause mod_proxy to forward the request
    to an origin server choosen by the remote user. This issue affects
    Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk
    Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP
    Server does not properly handle certain configuration sections that
    specify NiceValue but not AssignUserID, which might allow remote
    attackers to gain privileges by leveraging the root uid and root gid
    of an mpm-itk process.

- Vulnerability: CVE-2022-23943

  – CVSS Score: 7.5
  – Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

- Vulnerability: CVE-2018-17199

  – CVSS Score: 5
  – Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

- Vulnerability: CVE-2021-34798

  – CVSS Score: 5
  – Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2023-25690

  – CVSS Score: N/A
  – Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2020-11984

  – CVSS Score: 7.5
  – Description: Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE

- Vulnerability: CVE-2021-4160

  – CVSS Score: 4.3

– Description: There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that is available to premium support customers only. It will be made available in 1.0.2zc when it is released. The issue only affects OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0). Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL 1.0.2zc-dev (Affected 1.0.2-1.0.2zb).

- Vulnerability: CVE-2022-26377

  – CVSS Score: 5

  – Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2019-10081

  – CVSS Score: 5

  – Description: HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example configured with "H2PushResource", could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client.

- Vulnerability: CVE-2019-10082

  – CVSS Score: 6.4

  – Description: In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.

- Vulnerability: CVE-2024-40898

  – CVSS Score: N/A

  – Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2022-0778

  – CVSS Score: 5

– Description: The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - TLS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

- Vulnerability: CVE-2022-2097

  – CVSS Score: 5

  – Description: AES OCB mode for 32-bit x86 platforms using the AES-NI assembly optimised implementation will not encrypt the entirety of the data under some circumstances. This could reveal sixteen bytes of data that was preexisting in the memory that wasn't written. In the special case of "in place" encryption, sixteen bytes of the plaintext would be revealed. Since OpenSSL does not support OCB based cipher suites for TLS and DTLS, they are both unaffected. Fixed in OpenSSL 3.0.5 (Affected 3.0.0-3.0.4). Fixed in OpenSSL 1.1.1q (Affected 1.1.1-1.1.1p).

- Vulnerability: CVE-2023-27522

  – CVSS Score: N/A

  – Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.Special characters in the origin response header can truncate/split the response forwarded to the client.

- Vulnerability: CVE-2009-1390

  – CVSS Score: 6.8

  – Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2) GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS certificate in the chain is accepted instead of verifying the entire chain, which allows remote attackers to spoof trusted servers via a man-in-the-middle attack.

- Vulnerability: CVE-2012-3526

  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2023-5678

  - CVSS Score: N/A
  - Description: Issue summary: Generating excessively long X9.42 DH keys or checkingexcessively long X9.42 DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_generate_key() togenerate an X9.42 DH key may experience long delays. Likewise, applicationsthat use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check()to check an X9.42 DH key or X9.42 DH parameters may experience long delays.Where the key or parameters that are being checked have been obtained froman untrusted source this may lead to a Denial of Service.While DH_check() performs all the necessary checks (as of CVE-2023-3817),DH_check_pub_key() doesn't make any of these checks, and is thereforevulnerable for excessively large P and Q parameters.Likewise, while DH_generate_key() performs a check for an excessively largeP, it doesn't check for an excessively large Q.An application that calls DH_generate_key() or DH_check_pub_key() andsupplies a key or parameters obtained from an untrusted source could bevulnerable to a Denial of Service attack.DH_generate_key() and DH_check_pub_key() are also called by a number ofother OpenSSL functions. An application calling any of those otherfunctions may similarly be affected. The other functions affected by thisare DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate().Also vulnerable are the OpenSSL pkey command line application when using the"-pubcheck" option, as well as the OpenSSL genpkey command line application.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2022-1292

  - CVSS Score: 10
  - Description: The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n). Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).

- Vulnerability: CVE-2012-4001

- CVSS Score: 5
- Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2022-37436

  - CVSS Score: N/A
  - Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2022-4450

  - CVSS Score: N/A
  - Description: The function PEM_read_bio_ex() reads a PEM file from a BIO and parses anddecodes the "name" (e.g. "CERTIFICATE"), any header data and the payload data.If the function succeeds then the "name_out", "header" and "data" arguments arepopulated with pointers to buffers containing the relevant decoded data. Thecaller is responsible for freeing those buffers. It is possible to construct aPEM file that results in 0 bytes of payload data. In this case PEM_read_bio_ex()will return a failure code but will populate the header argument with a pointerto a buffer that has already been freed. If the caller also frees this bufferthen a double free will occur. This will most likely lead to a crash. Thiscould be exploited by an attacker who has the ability to supply malicious PEMfiles for parsing to achieve a denial of service attack.The functions PEM_read_bio() and PEM_read() are simple wrappers aroundPEM_read_bio_ex() and therefore these functions are also directly affected.These functions are also called indirectly by a number of other OpenSSLfunctions including PEM_X509_INFO_read_bio_ex() andSSL_CTX_use_serverinfo_file() which are also vulnerable. Some OpenSSL internaluses of these functions are not vulnerable because the caller does not free theheader argument if PEM_read_bio_ex() returns a failure code. These locationsinclude the PEM_read_bio_TYPE() functions as well as the decoders introduced inOpenSSL 3.0.The OpenSSL asn1parse command line application is also impacted by this issue.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1

- Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2023-45802

  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-28615

  - CVSS Score: 6.4
  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- Vulnerability: CVE-2022-28614

  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

- Vulnerability: CVE-2019-0215

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in mod_ssl when using per-location client certificate verification with TLSv1.3 allowed a client to bypass configured access control restrictions.

- Vulnerability: CVE-2013-4365

- CVSS Score: 7.5
- Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2022-28330

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2021-32791

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2021-32792

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.

- Vulnerability: CVE-2023-31122

  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2024-38476

  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-27316

  - CVSS Score: N/A
  - Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

- Vulnerability: CVE-2024-38474

  - CVSS Score: N/A

- Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2009-0796

  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2022-2068

  - CVSS Score: 10
  - Description: In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze).

- Vulnerability: CVE-2021-36160

  - CVSS Score: 5
  - Description: A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS). This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48 (inclusive).

- Vulnerability: CVE-2020-1927

  - CVSS Score: 5.8
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.

- Vulnerability: CVE-2023-0286

  - CVSS Score: N/A

– Description: There is a type confusion vulnerability relating to X.400 address processinginside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING butthe public structure definition for GENERAL_NAME incorrectly specified the typeof the x400Address field as ASN1_TYPE. This field is subsequently interpreted bythe OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than anASN1_STRING.When CRL checking is enabled (i.e. the application sets theX509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to passarbitrary pointers to a memcmp call, enabling them to read memory contents orenact a denial of service. In most cases, the attack requires the attacker toprovide both the certificate chain and CRL, neither of which need to have avalid signature. If the attacker only controls one of these inputs, the otherinput must already contain an X.400 address as a CRL distribution point, whichis uncommon. As such, this vulnerability is most likely to only affectapplications which have implemented their own functionality for retrieving CRLsover a network.

- Vulnerability: CVE-2023-3817

  – CVSS Score: N/A

  – Description: Issue summary: Checking excessively long DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH key or DH parameters may experience longdelays. Where the key or parameters that are being checked have been obtainedfrom an untrusted source this may lead to a Denial of Service.The function DH_check() performs various checks on DH parameters. After fixingCVE-2023-3446 it was discovered that a large q parameter value can also triggeran overly long computation during some of these checks. A correct q value,if present, cannot be larger than the modulus p parameter, thus it isunnecessary to perform these checks if q is larger than p.An application that calls DH_check() and supplies a key or parameters obtainedfrom an untrusted source could be vulnerable to a Denial of Service attack.The function DH_check() is itself called by a number of other OpenSSL functions.An application calling any of those other functions may similarly be affected.The other functions affected by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable are the OpenSSL dhparam and pkeyparam command line applicationswhen using the "-check" option.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2021-32786

  – CVSS Score: 5.8

  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, `oidc_validate_redirect_url()` does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring `mod_auth_openidc` to only allow redirection whose destination matches a given regular expression.

- Vulnerability: CVE-2021-32785

  – CVSS Score: 4.3
  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache ('OIDCCacheEncrypt off', 'OIDCSessionType server-cache', 'OIDCCacheType redis'), 'mod_auth_openidc' wrongly performed argument interpolation before passing Redis requests to 'hiredis', which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the 'hiredis' API. As a workaround, this vulnerability can be mitigated by setting 'OIDCCacheEncrypt' to 'on', as cache keys are cryptographically hashed before use when this option is enabled.

- Vulnerability: CVE-2020-9490

  – CVSS Score: 5
  – Description: Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2007-4723

  – CVSS Score: 7.5
  – Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2021-44790

  – CVSS Score: 7.5
  – Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

- Vulnerability: CVE-2020-13938

  – CVSS Score: 2.1
  – Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

- Vulnerability: CVE-2023-2650

  – CVSS Score: N/A

- Description: Issue summary: Processing some specially crafted ASN.1 object
  identifiers ordata containing them may be very slow.Impact summary:
  Applications that use OBJ_obj2txt() directly, or use any ofthe
  OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with
  no messagesize limit may experience notable to very long delays
  when processing thosemessages, which may lead to a Denial of
  Service.An OBJECT IDENTIFIER is composed of a series of numbers –
  sub-identifiers –most of which have no size limit. OBJ_obj2txt() may
  be used to translatean ASN.1 OBJECT IDENTIFIER given in DER encoding
  form (using the OpenSSLtype ASN1_OBJECT) to its canonical numeric
  text form, which are thesub-identifiers of the OBJECT IDENTIFIER in
  decimal form, separated byperiods.When one of the sub-identifiers in
  the OBJECT IDENTIFIER is very large(these are sizes that are seen as
  absurdly large, taking up tens or hundredsof KiBs), the translation
  to a decimal number in text may take a very longtime. The time
  complexity is $O(n^2)$ with 'n' being the size of thesub-identifiers
  in bytes (*).With OpenSSL 3.0, support to fetch cryptographic
  algorithms using names /identifiers in string form was introduced.
  This includes using OBJECTIDENTIFIERs in canonical numeric text form
  as identifiers for fetchingalgorithms.Such OBJECT IDENTIFIERs may
  be received through the ASN.1 structureAlgorithmIdentifier, which
  is commonly used in multiple protocols to specifywhat cryptographic
  algorithm should be used to sign or verify, encrypt ordecrypt, or
  digest passed data.Applications that call OBJ_obj2txt() directly
  with untrusted data areaffected, with any version of OpenSSL. If the
  use is for the mere purposeof display, the severity is considered
  low.In OpenSSL 3.0 and newer, this affects the subsystems OCSP,
  PKCS7/SMIME,CMS, CMP/CRMF or TS. It also impacts anything that
  processes X.509certificates, including simple things like verifying
  its signature.The impact on TLS is relatively low, because all
  versions of OpenSSL have a100KiB limit on the peer's certificate
  chain. Additionally, this onlyimpacts clients, or servers that
  have explicitly enabled clientauthentication.In OpenSSL 1.1.1 and
  1.0.2, this only affects displaying diverse objects,such as X.509
  certificates. This is assumed to not happen in such a waythat it
  would cause a Denial of Service, so these versions are considerednot
  affected by this issue in such a way that it would be cause for
  concern,and the severity is therefore considered low.
- Vulnerability: CVE-2023-0215
  - CVSS Score: N/A

– Description: The public API function BIO_new_NDEF is a helper function used for streamingASN.1 data via a BIO. It is primarily used internally to OpenSSL to support theSMIME, CMS and PKCS7 streaming capabilities, but may also be called directly byend user applications.The function receives a BIO from the caller, prepends a new BIO_f_asn1 filterBIO onto the front of it to form a BIO chain, and then returns the new head ofthe BIO chain to the caller. Under certain conditions, for example if a CMSrecipient public key is invalid, the new filter BIO is freed and the functionreturns a NULL result indicating a failure. However, in this case, the BIO chainis not properly cleaned up and the BIO passed by the caller still retainsinternal pointers to the previously freed filter BIO. If the caller then goes onto call BIO_pop() on the BIO then a use-after-free will occur. This will mostlikely result in a crash.This scenario occurs directly in the internal function B64_write_ASN1() whichmay cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() onthe BIO. This internal function is in turn called by the public API functionsPEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream,SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7.Other public API functions that may be impacted by this includei2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream andi2d_PKCS7_bio_stream.The OpenSSL cms and smime command line applications are similarly affected.

- Vulnerability: CVE-2020-35452

    – CVSS Score: 6.8
    – Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

- Vulnerability: CVE-2022-22719

    – CVSS Score: 5
    – Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2020-1934

    – CVSS Score: 5
    – Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

- Vulnerability: CVE-2022-36760

    – CVSS Score: N/A
    – Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-4304

    – CVSS Score: N/A

- Description: A timing based side channel exists in the OpenSSL RSA Decryption implementationwhich could be sufficient to recover a plaintext across a network in aBleichenbacher style attack. To achieve a successful decryption an attackerwould have to be able to send a very large number of trial messages fordecryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5,RSA-OEAP and RSASVE.For example, in a TLS connection, RSA is commonly used by a client to send anencrypted pre-master secret to the server. An attacker that had observed agenuine connection between a client and a server could use this flaw to sendtrial messages to the server and record the time taken to process them. After asufficiently large number of messages the attacker could recover the pre-mastersecret used for the original connection and thus be able to decrypt theapplication data sent over that connection.

- Vulnerability: CVE-2019-9517

  - CVSS Score: 7.8
  - Description: Some HTTP/2 implementations are vulnerable to unconstrained interal data buffering, potentially leading to a denial of service. The attacker opens the HTTP/2 window so the peer can send without constraint; however, they leave the TCP window closed so the peer cannot actually write (many of) the bytes on the wire. The attacker then sends a stream of requests for a large response object. Depending on how the servers queue the responses, this can consume excess memory, CPU, or both.

- Vulnerability: CVE-2019-0217

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.

- Vulnerability: CVE-2019-0197

  - CVSS Score: 4.9
  - Description: A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue.

- Vulnerability: CVE-2019-0196

  - CVSS Score: 5
  - Description: A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.

- Vulnerability: CVE-2019-0190

  - CVSS Score: 5
  - Description: A bug exists in the way mod_ssl handled client renegotiations. A remote attacker could send a carefully crafted request that would cause mod_ssl to enter a loop leading to a denial of service. This bug can be only triggered with Apache HTTP Server version 2.4.37 when using OpenSSL version 1.1.1 or later, due to an interaction in changes to handling of renegotiation attempts.

- Vulnerability: CVE-2021-33193

  - CVSS Score: 5
  - Description: A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.

- Vulnerability: CVE-2019-0211

  - CVSS Score: 7.2
  - Description: In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.

- Vulnerability: CVE-2019-17567

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

- Vulnerability: CVE-2022-31813

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

- Vulnerability: CVE-2012-4360

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2023-4807

  - CVSS Score: N/A

- Description: Issue summary: The POLY1305 MAC (message authentication code) implementationcontains a bug that might corrupt the internal state of applications on theWindows 64 platform when running on newer X86_64 processors supporting theAVX512-IFMA instructions.Impact summary: If in an application that uses the OpenSSL library an attackercan influence whether the POLY1305 MAC algorithm is used, the applicationstate might be corrupted with various application dependent consequences.The POLY1305 MAC (message authentication code) implementation in OpenSSL doesnot save the contents of non-volatile XMM registers on Windows 64 platformwhen calculating the MAC of data larger than 64 bytes. Before returning tothe caller all the XMM registers are set to zero rather than restoring theirprevious content. The vulnerable code is used only on newer x86_64 processorssupporting the AVX512-IFMA instructions.The consequences of this kind of internal application state corruption canbe various – from no consequences, if the calling application does notdepend on the contents of non-volatile XMM registers at all, to the worstconsequences, where the attacker could get complete control of the applicationprocess. However given the contents of the registers are just zeroized sothe attacker cannot put arbitrary values inside, the most likely consequence,if any, would be an incorrect result of some application dependentcalculations or a crash leading to a denial of service.The POLY1305 MAC algorithm is most frequently used as part of theCHACHA20-POLY1305 AEAD (authenticated encryption with associated data)algorithm. The most common usage of this AEAD cipher is with TLS protocolversions 1.2 and 1.3 and a malicious client can influence whether this AEADcipher is used by the server. This implies that server applications usingOpenSSL can be potentially impacted. However we are currently not aware ofany concrete application that would be affected by this issue therefore weconsider this a Low severity security issue.As a workaround the AVX512-IFMA instructions support can be disabled atruntime by setting the environment variable OPENSSL_ia32cap: OPENSSL_ia32cap=:~0x200000The FIPS provider is not affected by this issue.

- **Vulnerability: CVE-2009-3767**

  - CVSS Score: 4.3
  - Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other versions, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- **Vulnerability: CVE-2021-26690**

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service

- **Vulnerability: CVE-2021-26691**

  - CVSS Score: 7.5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow

- **Vulnerability: CVE-2019-0220**

- CVSS Score: 5
- Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.

- Vulnerability: CVE-2024-38477

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- Vulnerability: CVE-2021-39275

  - CVSS Score: 7.5
  - Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2018-17189

  - CVSS Score: 5
  - Description: In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 (mod_http2) connections.

- Vulnerability: CVE-2022-29404

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2006-20001

  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2020-11993

  - CVSS Score: 4.3
  - Description: Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2021-3711

  - CVSS Score: 7.5
  - Description: In order to decrypt SM2 encrypted data an application is expected to call the API function EVP_PKEY_decrypt(). Typically an application will call this function twice. The first time, on entry, the "out" parameter can be NULL and, on exit, the "outlen" parameter is populated with the buffer size required to hold the decrypted plaintext. The application can then allocate a sufficiently sized buffer and call EVP_PKEY_decrypt() again, but this time passing a non-NULL value for the "out" parameter. A bug in the implementation of the SM2 decryption code means that the calculation of the buffer size required to hold the plaintext returned by the first call to EVP_PKEY_decrypt() can be smaller than the actual size required by the second call. This can lead to a buffer overflow when EVP_PKEY_decrypt() is called by the application a second time with a buffer that is too small. A malicious attacker who is able present SM2 content for decryption to an application could cause attacker chosen data to overflow the buffer by up to a maximum of 62 bytes altering the contents of other data held after the buffer, possibly changing application behaviour or causing the application to crash. The location of the buffer is application dependent but is typically heap allocated. Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k).

- Vulnerability: CVE-2024-0727

  - CVSS Score: N/A
  - Description: Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSLto crash leading to a potential Denial of Service attackImpact summary: Applications loading files in the PKCS12 format from untrustedsources might terminate abruptly.A file in PKCS12 format can contain certificates and keys and may come from anuntrusted source. The PKCS12 specification allows certain fields to be NULL, butOpenSSL does not correctly check for this case. This can lead to a NULL pointerdereference that results in OpenSSL crashing. If an application processes PKCS12files from an untrusted source using the OpenSSL APIs then that application willbe vulnerable to this issue.OpenSSL APIs that are vulnerable to this are: PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a similar issue in SMIME_write_PKCS7(). However since thisfunction is related to writing data we do not consider it security significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.

- Vulnerability: CVE-2009-3766

  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when OpenSSL is used, does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

- Vulnerability: CVE-2021-44224

  - CVSS Score: 6.4

- Description: A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).

- Vulnerability: CVE-2009-3765

  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2022-22721

  - CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2022-22720

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2019-10092

  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

- Vulnerability: CVE-2021-3712

  - CVSS Score: 5.8

- Description: ASN.1 strings are represented internally within OpenSSL as an
  ASN1_STRING structure which contains a buffer holding the string
  data and a field holding the buffer length. This contrasts with
  normal C strings which are repesented as a buffer for the string
  data which is terminated with a NUL (0) byte. Although not a
  strict requirement, ASN.1 strings that are parsed using OpenSSL's
  own "d2i" functions (and other similar parsing functions) as well
  as any string whose value has been set with the ASN1_STRING_set()
  function will additionally NUL terminate the byte array in the
  ASN1_STRING structure. However, it is possible for applications
  to directly construct valid ASN1_STRING structures which do not NUL
  terminate the byte array by directly setting the "data" and "length"
  fields in the ASN1_STRING array. This can also happen by using
  the ASN1_STRING_set0() function. Numerous OpenSSL functions that
  print ASN.1 data have been found to assume that the ASN1_STRING byte
  array will be NUL terminated, even though this is not guaranteed for
  strings that have been directly constructed. Where an application
  requests an ASN.1 structure to be printed, and where that ASN.1
  structure contains ASN1_STRINGs that have been directly constructed
  by the application without NUL terminating the "data" field, then
  a read buffer overrun can occur. The same thing can also occur
  during name constraints processing of certificates (for example
  if a certificate has been directly constructed by the application
  instead of loading it via the OpenSSL parsing functions, and the
  certificate contains non NUL terminated ASN1_STRING structures).
  It can also occur in the X509_get1_email(), X509_REQ_get1_email()
  and X509_get1_ocsp() functions. If a malicious actor can cause an
  application to directly construct an ASN1_STRING and then process it
  through one of the affected OpenSSL functions then this issue could
  be hit. This might result in a crash (causing a Denial of Service
  attack). It could also result in the disclosure of private memory
  contents (such as private keys, or sensitive plaintext). Fixed in
  OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za
  (Affected 1.0.2-1.0.2y).

- Vulnerability: CVE-2023-0464

  - CVSS Score: N/A

  - Description: A security vulnerability has been identified in all supported
    versionsof OpenSSL related to the verification of X.509 certificate
    chainsthat include policy constraints. Attackers may be able to
    exploit thisvulnerability by creating a malicious certificate chain
    that triggersexponential use of computational resources, leading
    to a denial-of-service(DoS) attack on affected systems.Policy
    processing is disabled by default but can be enabled by passingthe
    '-policy' argument to the command line utilities or by calling
    the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0465

  - CVSS Score: N/A

- Description: Applications that use a non-default option when verifying
  certificates may bevulnerable to an attack from a malicious CA
  to circumvent certain checks.Invalid certificate policies in leaf
  certificates are silently ignored byOpenSSL and other certificate
  policy checks are skipped for that certificate.A malicious CA could
  use this to deliberately assert invalid certificate policiesin order
  to circumvent policy checking on the certificate altogether.Policy
  processing is disabled by default but can be enabled by passingthe
  '-policy' argument to the command line utilities or by calling
  the'X509_VERIFY_PARAM_set1_policies()' function.

- **Vulnerability:** CVE-2023-0466

  - CVSS Score: N/A
  - Description: The function X509_VERIFY_PARAM_add0_policy() is documented
    toimplicitly enable the certificate policy check when doing
    certificateverification. However the implementation of the
    function does notenable the check which allows certificates
    with invalid or incorrectpolicies to pass the certificate
    verification.As suddenly enabling the policy check could break
    existing deployments it wasdecided to keep the existing behavior of
    the X509_VERIFY_PARAM_add0_policy()function.Instead the applications
    that require OpenSSL to perform certificatepolicy check need
    to use X509_VERIFY_PARAM_set1_policies() or explicitlyenable the
    policy check by calling X509_VERIFY_PARAM_set_flags() withthe
    X509_V_FLAG_POLICY_CHECK flag argument.Certificate policy checks
    are disabled by default in OpenSSL and are notcommonly used by
    applications.

- **Vulnerability:** CVE-2019-10098

  - CVSS Score: 5.8
  - Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with
    mod_rewrite that were intended to be self-referential might be fooled
    by encoded newlines and redirect instead to an unexpected URL within
    the request URL.

- **Vulnerability:** CVE-2019-10097

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4.32-2.4.39, when mod_remoteip was configured
    to use a trusted intermediary proxy server using the "PROXY"
    protocol, a specially crafted PROXY header could trigger a stack
    buffer overflow or NULL pointer deference. This vulnerability
    could only be triggered by a trusted proxy and not by untrusted HTTP
    clients.

- **Vulnerability:** CVE-2021-40438

  - CVSS Score: 6.8
  - Description: A crafted request uri-path can cause mod_proxy to forward the request
    to an origin server choosen by the remote user. This issue affects
    Apache HTTP Server 2.4.48 and earlier.

- **Vulnerability:** CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk
    Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP
    Server does not properly handle certain configuration sections that
    specify NiceValue but not AssignUserID, which might allow remote
    attackers to gain privileges by leveraging the root uid and root gid
    of an mpm-itk process.

- Vulnerability: CVE-2022-23943

  – CVSS Score: 7.5
  – Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

- Vulnerability: CVE-2018-17199

  – CVSS Score: 5
  – Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

- Vulnerability: CVE-2021-34798

  – CVSS Score: 5
  – Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2023-25690

  – CVSS Score: N/A
  – Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2020-11984

  – CVSS Score: 7.5
  – Description: Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE

- Vulnerability: CVE-2021-4160

  – CVSS Score: 4.3

– Description: There is a carry propagation bug in the MIPS32 and MIPS64 squaring
procedure. Many EC algorithms are affected, including some of the
TLS 1.3 default curves. Impact was not analyzed in detail, because
the pre-requisites for attack are considered unlikely and include
reusing private keys. Analysis suggests that attacks against RSA and
DSA as a result of this defect would be very difficult to perform
and are not believed likely. Attacks against DH are considered
just feasible (although very difficult) because most of the work
necessary to deduce information about a private key may be performed
offline. The amount of resources required for such an attack would
be significant. However, for an attack on TLS to be meaningful, the
server would have to share the DH private key among multiple clients,
which is no longer an option since CVE-2016-0701. This issue affects
OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the
releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For
the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that
is available to premium support customers only. It will be made
available in 1.0.2zc when it is released. The issue only affects
OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0).
Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL
1.0.2zc-dev (Affected 1.0.2-1.0.2zb).

- Vulnerability: CVE-2022-26377

  – CVSS Score: 5
  – Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request
  Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server
  allows an attacker to smuggle requests to the AJP server it forwards
  requests to. This issue affects Apache HTTP Server Apache HTTP
  Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2019-10081

  – CVSS Score: 5
  – Description: HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example
  configured with "H2PushResource", could lead to an overwrite of
  memory in the pushing request's pool, leading to crashes. The memory
  copied is that of the configured push link header values, not data
  supplied by the client.

- Vulnerability: CVE-2019-10082

  – CVSS Score: 6.4
  – Description: In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input,
  the http/2 session handling could be made to read memory after being
  freed, during connection shutdown.

- Vulnerability: CVE-2024-40898

  – CVSS Score: N/A
  – Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in
  server/vhost context, allows to potentially leak NTML hashes to
  a malicious server via SSRF and malicious requests.Users are
  recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2022-0778

  – CVSS Score: 5

- Description: The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - TLS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

- Vulnerability: CVE-2022-2097

  - CVSS Score: 5
  - Description: AES OCB mode for 32-bit x86 platforms using the AES-NI assembly optimised implementation will not encrypt the entirety of the data under some circumstances. This could reveal sixteen bytes of data that was preexisting in the memory that wasn't written. In the special case of "in place" encryption, sixteen bytes of the plaintext would be revealed. Since OpenSSL does not support OCB based cipher suites for TLS and DTLS, they are both unaffected. Fixed in OpenSSL 3.0.5 (Affected 3.0.0-3.0.4). Fixed in OpenSSL 1.1.1q (Affected 1.1.1-1.1.1p).

- Vulnerability: CVE-2023-27522

  - CVSS Score: N/A
  - Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.Special characters in the origin response header can truncate/split the response forwarded to the client.

- Vulnerability: CVE-2009-1390

  - CVSS Score: 6.8
  - Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2) GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS certificate in the chain is accepted instead of verifying the entire chain, which allows remote attackers to spoof trusted servers via a man-in-the-middle attack.

- Vulnerability: CVE-2012-3526

  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2023-5678

  - CVSS Score: N/A
  - Description: Issue summary: Generating excessively long X9.42 DH keys or checkingexcessively long X9.42 DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_generate_key() togenerate an X9.42 DH key may experience long delays. Likewise, applicationsthat use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check()to check an X9.42 DH key or X9.42 DH parameters may experience long delays.Where the key or parameters that are being checked have been obtained froman untrusted source this may lead to a Denial of Service.While DH_check() performs all the necessary checks (as of CVE-2023-3817),DH_check_pub_key() doesn't make any of these checks, and is thereforevulnerable for excessively large P and Q parameters.Likewise, while DH_generate_key() performs a check for an excessively largeP, it doesn't check for an excessively large Q.An application that calls DH_generate_key() or DH_check_pub_key() andsupplies a key or parameters obtained from an untrusted source could bevulnerable to a Denial of Service attack.DH_generate_key() and DH_check_pub_key() are also called by a number ofother OpenSSL functions. An application calling any of those otherfunctions may similarly be affected. The other functions affected by thisare DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate().Also vulnerable are the OpenSSL pkey command line application when using the"-pubcheck" option, as well as the OpenSSL genpkey command line application.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2022-1292

  - CVSS Score: 10
  - Description: The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n). Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).

- Vulnerability: CVE-2012-4001

- CVSS Score: 5
- Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2022-37436

  - CVSS Score: N/A
  - Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2022-4450

  - CVSS Score: N/A
  - Description: The function PEM_read_bio_ex() reads a PEM file from a BIO and parses anddecodes the "name" (e.g. "CERTIFICATE"), any header data and the payload data.If the function succeeds then the "name_out", "header" and "data" arguments arepopulated with pointers to buffers containing the relevant decoded data. Thecaller is responsible for freeing those buffers. It is possible to construct aPEM file that results in 0 bytes of payload data. In this case PEM_read_bio_ex()will return a failure code but will populate the header argument with a pointerto a buffer that has already been freed. If the caller also frees this bufferthen a double free will occur. This will most likely lead to a crash. Thiscould be exploited by an attacker who has the ability to supply malicious PEMfiles for parsing to achieve a denial of service attack.The functions PEM_read_bio() and PEM_read() are simple wrappers aroundPEM_read_bio_ex() and therefore these functions are also directly affected.These functions are also called indirectly by a number of other OpenSSLfunctions including PEM_X509_INFO_read_bio_ex() andSSL_CTX_use_serverinfo_file() which are also vulnerable. Some OpenSSL internaluses of these functions are not vulnerable because the caller does not free theheader argument if PEM_read_bio_ex() returns a failure code. These locationsinclude the PEM_read_bio_TYPE() functions as well as the decoders introduced inOpenSSL 3.0.The OpenSSL asn1parse command line application is also impacted by this issue.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1

- Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2023-45802

  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-28615

  - CVSS Score: 6.4
  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- Vulnerability: CVE-2022-28614

  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

11.5   IP Address: 159.149.133.149

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 5

- High Vulnerabilities: 24

- Medium Vulnerabilities: 177

- Low Vulnerabilities: 18

- Total Vulnerabilities: 224

Services Running on IP Address

- Service: OpenSSH

    – Port: 22
    – Version: 7.4
    – Location:

- Service: Apache httpd

    – Port: 80
    – Version: 2.4.6
    – Location: /

- Service: Apache httpd

    – Port: 443
    – Version: 2.4.6
    – Location: /

Vulnerabilities Found

- Vulnerability: CVE-2008-3844

    – CVSS Score: 9.3
    – Description: Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, as signed in August 2008 using a legitimate Red Hat GPG key, contain an externally introduced modification (Trojan Horse) that allows the package authors to have an unknown impact. NOTE: since the malicious packages were not distributed from any official Red Hat sources, the scope of this issue is restricted to users who may have obtained these packages through unofficial distribution points. As of 20080827, no unofficial distributions of this software are known.

- Vulnerability: CVE-2019-6110

    – CVSS Score: 4
    – Description: In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.

- Vulnerability: CVE-2016-20012

    – CVSS Score: 4.3

- Description: OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product

- Vulnerability: CVE-2018-15919

  - CVSS Score: 5
  - Description: Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'

- Vulnerability: CVE-2018-15473

  - CVSS Score: 5
  - Description: OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.

- Vulnerability: CVE-2021-36368

  - CVSS Score: 2.6
  - Description: An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is "this is not an authentication bypass, since nothing is being bypassed.

- Vulnerability: CVE-2017-15906

  - CVSS Score: 5
  - Description: The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.

- Vulnerability: CVE-2018-20685

  - CVSS Score: 2.6
  - Description: In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.

- Vulnerability: CVE-2020-14145

  - CVSS Score: 4.3
  - Description: The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.

- Vulnerability: CVE-2023-51767

- CVSS Score: N/A
  - Description: OpenSSH through 9.6, when common types of DRAM are used, might allow
                 row hammer attacks (for authentication bypass) because the integer
                 value of authenticated in mm_answer_authpassword does not resist
                 flips of a single bit. NOTE: this is applicable to a certain threat
                 model of attacker-victim co-location in which the attacker has user
                 privileges.

- Vulnerability: CVE-2020-15778

  - CVSS Score: 6.8
  - Description: scp in OpenSSH through 8.3p1 allows command injection in the scp.c
                 toremote function, as demonstrated by backtick characters in the
                 destination argument. NOTE: the vendor reportedly has stated that
                 they intentionally omit validation of "anomalous argument transfers"
                 because that could "stand a great chance of breaking existing
                 workflows."

- Vulnerability: CVE-2023-48795

  - CVSS Score: N/A
  - Description: The SSH transport protocol with certain OpenSSH extensions,
                 found in OpenSSH before 9.6 and other products, allows remote
                 attackers to bypass integrity checks such that some packets are
                 omitted (from the extension negotiation message), and a client and
                 server may consequently end up with a connection for which some
                 security features have been downgraded or disabled, aka a Terrapin
                 attack. This occurs because the SSH Binary Packet Protocol (BPP),
                 implemented by these extensions, mishandles the handshake phase
                 and mishandles use of sequence numbers. For example, there is an
                 effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with
                 Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com
                 and (if CBC is used) the -etm@openssh.com MAC algorithms. This also
                 affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear
                 through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80,
                 AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh
                 before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway
                 before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch
                 before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through
                 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0,
                 ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before
                 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0,
                 ConnectBot SSH library before 2.2.22, Apache MINA sshd through
                 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2
                 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before
                 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before
                 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2,
                 Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY
                 through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2
                 module before 1.15.0 for Node.js, the thrussh library before 0.35.1
                 for Rust, and the Russh crate before 0.40.2 for Rust.

- Vulnerability: CVE-2023-38408

  - CVSS Score: N/A
  - Description: The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an
                 insufficiently trustworthy search path, leading to remote code
                 execution if an agent is forwarded to an attacker-controlled
                 system. (Code in /usr/lib is not necessarily safe for loading into
                 ssh-agent.) NOTE: this issue exists because of an incomplete fix for
                 CVE-2016-10009.

- Vulnerability: CVE-2007-2768

  – CVSS Score: 4.3
  – Description: OpenSSH, when using OPIE (One-Time Passwords in Everything) for PAM, allows remote attackers to determine the existence of certain user accounts, which displays a different response if the user account exists and is configured to use one-time passwords (OTP), a similar issue to CVE-2007-2243.

- Vulnerability: CVE-2021-41617

  – CVSS Score: 4.4
  – Description: sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

- Vulnerability: CVE-2019-6111

  – CVSS Score: 5.8
  – Description: An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).

- Vulnerability: CVE-2023-51385

  – CVSS Score: N/A
  – Description: In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.

- Vulnerability: CVE-2019-6109

  – CVSS Score: 4
  – Description: An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.

- Vulnerability: CVE-2014-0117

  – CVSS Score: 4.3
  – Description: The mod_proxy module in the Apache HTTP Server 2.4.x before 2.4.10, when a reverse proxy is enabled, allows remote attackers to cause a denial of service (child-process crash) via a crafted HTTP Connection header.

- Vulnerability: CVE-2017-7679

  – CVSS Score: 7.5

- Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

- **Vulnerability:** CVE-2017-9798

  - CVSS Score: 5
  - Description: Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.

- **Vulnerability:** CVE-2015-3185

  - CVSS Score: 4.3
  - Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

- **Vulnerability:** CVE-2015-3184

  - CVSS Score: 5
  - Description: mod_authz_svn in Apache Subversion 1.7.x before 1.7.21 and 1.8.x before 1.8.14, when using Apache httpd 2.4.x, does not properly restrict anonymous access, which allows remote anonymous users to read hidden files via the path name.

- **Vulnerability:** CVE-2024-4577

  - CVSS Score: N/A
  - Description: In PHP versions8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in command line given toWin32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc.

- **Vulnerability:** CVE-2013-4365

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- **Vulnerability:** CVE-2018-5407

  - CVSS Score: 1.9
  - Description: Simultaneous Multi-threading (SMT) in processors can enable local users to exploit software vulnerable to timing attacks via a side-channel timing attack on 'port contention'.

- Vulnerability: CVE-2022-28330

  – CVSS Score: 5
  – Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond
                  bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2021-32791

  – CVSS Score: 4.3
  – Description: mod_auth_openidc is an authentication/authorization module for the
                  Apache 2.x HTTP server that functions as an OpenID Connect Relying
                  Party, authenticating users against an OpenID Connect Provider.
                  In mod_auth_openidc before version 2.4.9, the AES GCM encryption in
                  mod_auth_openidc uses a static IV and AAD. It is important to fix
                  because this creates a static nonce and since aes-gcm is a stream
                  cipher, this can lead to known cryptographic issues, since the same
                  key is being reused. From 2.4.9 onwards this has been patched to use
                  dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2021-32792

  – CVSS Score: 4.3
  – Description: mod_auth_openidc is an authentication/authorization module for the
                  Apache 2.x HTTP server that functions as an OpenID Connect Relying
                  Party, authenticating users against an OpenID Connect Provider. In
                  mod_auth_openidc before version 2.4.9, there is an XSS vulnerability
                  in when using 'OIDCPreservePost On'.

- Vulnerability: CVE-2024-38476

  – CVSS Score: N/A
  – Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are
                  vulnerably to information disclosure, SSRF or local script execution
                  viabackend applications whose response headers are malicious or
                  exploitable.Users are recommended to upgrade to version 2.4.60, which
                  fixes this issue.

- Vulnerability: CVE-2024-38477

  – CVSS Score: N/A
  – Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59
                  and earlier allows an attacker to crash the server via a malicious
                  request.Users are recommended to upgrade to version 2.4.60, which
                  fixes this issue.

- Vulnerability: CVE-2023-31122

  – CVSS Score: N/A
  – Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP
                  Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2009-0796

  – CVSS Score: 2.6
  – Description: Cross-site scripting (XSS) vulnerability in Status.pm in
                  Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the
                  Apache HTTP Server, when /perl-status is accessible, allows remote
                  attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2024-0727

  – CVSS Score: N/A

- Description: Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSLto crash leading to a potential Denial of Service attackImpact summary: Applications loading files in the PKCS12 format from untrustedsources might terminate abruptly.A file in PKCS12 format can contain certificates and keys and may come from anuntrusted source. The PKCS12 specification allows certain fields to be NULL, butOpenSSL does not correctly check for this case. This can lead to a NULL pointerdereference that results in OpenSSL crashing. If an application processes PKCS12files from an untrusted source using the OpenSSL APIs then that application willbe vulnerable to this issue.OpenSSL APIs that are vulnerable to this are: PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a similar issue in SMIME_write_PKCS7(). However since thisfunction is related to writing data we do not consider it security significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.

- Vulnerability: CVE-2014-0118

  - CVSS Score: 4.3
  - Description: The deflate_in_filter function in mod_deflate.c in the mod_deflate module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.

- Vulnerability: CVE-2013-6438

  - CVSS Score: 5
  - Description: The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.

- Vulnerability: CVE-2020-1927

  - CVSS Score: 5.8
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.

- Vulnerability: CVE-2023-0286

  - CVSS Score: N/A

    – Description: There is a type confusion vulnerability relating to X.400 address processinginside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING butthe public structure definition for GENERAL_NAME incorrectly specified the typeof the x400Address field as ASN1_TYPE. This field is subsequently interpreted bythe OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than anASN1_STRING.When CRL checking is enabled (i.e. the application sets theX509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to passarbitrary pointers to a memcmp call, enabling them to read memory contents orenact a denial of service. In most cases, the attack requires the attacker toprovide both the certificate chain and CRL, neither of which need to have avalid signature. If the attacker only controls one of these inputs, the otherinput must already contain an X.400 address as a CRL distribution point, whichis uncommon. As such, this vulnerability is most likely to only affectapplications which have implemented their own functionality for retrieving CRLsover a network.

- Vulnerability: CVE-2023-3817

    – CVSS Score: N/A

    – Description: Issue summary: Checking excessively long DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH key or DH parameters may experience longdelays. Where the key or parameters that are being checked have been obtainedfrom an untrusted source this may lead to a Denial of Service.The function DH_check() performs various checks on DH parameters. After fixingCVE-2023-3446 it was discovered that a large q parameter value can also triggeran overly long computation during some of these checks. A correct q value,if present, cannot be larger than the modulus p parameter, thus it isunnecessary to perform these checks if q is larger than p.An application that calls DH_check() and supplies a key or parameters obtainedfrom an untrusted source could be vulnerable to a Denial of Service attack.The function DH_check() is itself called by a number of other OpenSSL functions.An application calling any of those other functions may similarly be affected.The other functions affected by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable are the OpenSSL dhparam and pkeyparam command line applicationswhen using the "-check" option.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2017-3167

    – CVSS Score: 7.5

    – Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.

- Vulnerability: CVE-2021-32786

    – CVSS Score: 5.8

– Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, `oidc_validate_redirect_url()` does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring `mod_auth_openidc` to only allow redirection whose destination matches a given regular expression.

• Vulnerability: CVE-2021-32785

– CVSS Score: 4.3

– Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache (`OIDCCacheEncrypt off`, `OIDCSessionType server-cache`, `OIDCCacheType redis`), `mod_auth_openidc` wrongly performed argument interpolation before passing Redis requests to `hiredis`, which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the `hiredis` API. As a workaround, this vulnerability can be mitigated by setting `OIDCCacheEncrypt` to `on`, as cache keys are cryptographically hashed before use when this option is enabled.

• Vulnerability: CVE-2007-4723

– CVSS Score: 7.5

– Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

• Vulnerability: CVE-2021-44790

– CVSS Score: 7.5

– Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

• Vulnerability: CVE-2016-4975

– CVSS Score: 4.3

– Description: Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).

- Vulnerability: CVE-2020-13938

  - CVSS Score: 2.1
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

- Vulnerability: CVE-2023-2650

  - CVSS Score: N/A
  - Description: Issue summary: Processing some specially crafted ASN.1 object identifiers ordata containing them may be very slow.Impact summary: Applications that use OBJ_obj2txt() directly, or use any ofthe OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no messagesize limit may experience notable to very long delays when processing thosemessages, which may lead to a Denial of Service.An OBJECT IDENTIFIER is composed of a series of numbers - sub-identifiers -most of which have no size limit. OBJ_obj2txt() may be used to translatean ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSLtype ASN1_OBJECT) to its canonical numeric text form, which are thesub-identifiers of the OBJECT IDENTIFIER in decimal form, separated byperiods.When one of the sub-identifiers in the OBJECT IDENTIFIER is very large(these are sizes that are seen as absurdly large, taking up tens or hundredsof KiBs), the translation to a decimal number in text may take a very longtime. The time complexity is O(n$\hat{2}$) with 'n' being the size of thesub-identifiers in bytes (*).With OpenSSL 3.0, support to fetch cryptographic algorithms using names /identifiers in string form was introduced. This includes using OBJECTIDENTIFIERs in canonical numeric text form as identifiers for fetchingalgorithms.Such OBJECT IDENTIFIERs may be received through the ASN.1 structureAlgorithmIdentifier, which is commonly used in multiple protocols to specifywhat cryptographic algorithm should be used to sign or verify, encrypt ordecrypt, or digest passed data.Applications that call OBJ_obj2txt() directly with untrusted data areaffected, with any version of OpenSSL. If the use is for the mere purposeof display, the severity is considered low.In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME,CMS, CMP/CRMF or TS. It also impacts anything that processes X.509certificates, including simple things like verifying its signature.The impact on TLS is relatively low, because all versions of OpenSSL have a100KiB limit on the peer's certificate chain. Additionally, this onlyimpacts clients, or servers that have explicitly enabled clientauthentication.In OpenSSL 1.1.1 and 1.0.2, this only affects displaying diverse objects,such as X.509 certificates. This is assumed to not happen in such a waythat it would cause a Denial of Service, so these versions are considerednot affected by this issue in such a way that it would be cause for concern,and the severity is therefore considered low.

- Vulnerability: CVE-2023-0215

  - CVSS Score: N/A

- Description: The public API function BIO_new_NDEF is a helper function used for streamingASN.1 data via a BIO. It is primarily used internally to OpenSSL to support theSMIME, CMS and PKCS7 streaming capabilities, but may also be called directly byend user applications.The function receives a BIO from the caller, prepends a new BIO_f_asn1 filterBIO onto the front of it to form a BIO chain, and then returns the new head ofthe BIO chain to the caller. Under certain conditions, for example if a CMSrecipient public key is invalid, the new filter BIO is freed and the functionreturns a NULL result indicating a failure. However, in this case, the BIO chainis not properly cleaned up and the BIO passed by the caller still retainsinternal pointers to the previously freed filter BIO. If the caller then goes onto call BIO_pop() on the BIO then a use-after-free will occur. This will mostlikely result in a crash.This scenario occurs directly in the internal function B64_write_ASN1() whichmay cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() onthe BIO. This internal function is in turn called by the public API functionsPEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream,SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7.Other public API functions that may be impacted by this includei2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream andi2d_PKCS7_bio_stream.The OpenSSL cms and smime command line applications are similarly affected.

- Vulnerability: CVE-2015-3183

  - CVSS Score: 5
  - Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

- Vulnerability: CVE-2020-35452

  - CVSS Score: 6.8
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

- Vulnerability: CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2020-1934

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

- Vulnerability: CVE-2022-36760

  - CVSS Score: N/A

- Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- **Vulnerability: CVE-2022-4304**

  - CVSS Score: N/A

  - Description: A timing based side channel exists in the OpenSSL RSA Decryption implementationwhich could be sufficient to recover a plaintext across a network in aBleichenbacher style attack. To achieve a successful decryption an attackerwould have to be able to send a very large number of trial messages fordecryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5,RSA-OEAP and RSASVE.For example, in a TLS connection, RSA is commonly used by a client to send anencrypted pre-master secret to the server. An attacker that had observed agenuine connection between a client and a server could use this flaw to sendtrial messages to the server and record the time taken to process them. After asufficiently large number of messages the attacker could recover the pre-mastersecret used for the original connection and thus be able to decrypt theapplication data sent over that connection.

- **Vulnerability: CVE-2019-1563**

  - CVSS Score: 4.3

  - Description: In situations where an attacker receives automated notification of the success or failure of a decryption attempt an attacker, after sending a very large number of messages to be decrypted, can recover a CMS/PKCS7 transported encryption key or decrypt any RSA encrypted message that was encrypted with the public RSA key, using a Bleichenbacher padding oracle attack. Applications are not affected if they use a certificate together with the private RSA key to the CMS_decrypt or PKCS7_decrypt functions to select the correct recipient info to decrypt. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).

- **Vulnerability: CVE-2014-3523**

  - CVSS Score: 5

  - Description: Memory leak in the winnt_accept function in server/mpm/winnt/child.c in the WinNT MPM in the Apache HTTP Server 2.4.x before 2.4.10 on Windows, when the default AcceptFilter is enabled, allows remote attackers to cause a denial of service (memory consumption) via crafted requests.

- **Vulnerability: CVE-2013-5704**

  - CVSS Score: 5

  - Description: The mod_headers module in the Apache HTTP Server 2.2.22 allows remote attackers to bypass "RequestHeader unset" directives by placing a header in the trailer portion of data sent with chunked transfer coding. NOTE: the vendor states "this is not a security issue in httpd as such."

- **Vulnerability: CVE-2019-17567**

  - CVSS Score: 5

- Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

• Vulnerability: CVE-2022-31813

  – CVSS Score: 7.5
  – Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

• Vulnerability: CVE-2013-2220

  – CVSS Score: 7.5
  – Description: Buffer overflow in the radius_get_vendor_attr function in the Radius extension before 1.2.7 for PHP allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a large Vendor Specific Attributes (VSA) length value.

• Vulnerability: CVE-2012-4360

  – CVSS Score: 4.3
  – Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

• Vulnerability: CVE-2014-0231

  – CVSS Score: 5
  – Description: The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.

• Vulnerability: CVE-2021-26690

  – CVSS Score: 5
  – Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service

• Vulnerability: CVE-2021-26691

  – CVSS Score: 7.5
  – Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow

• Vulnerability: CVE-2019-0220

  – CVSS Score: 5
  – Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.

• Vulnerability: CVE-2022-30556

    – CVSS Score: 5

    – Description: Apache HTTP Server 2.4.53 and earlier may return lengths to
                    applications calling r:wsread() that point past the end of the
                    storage allocated for the buffer.

- Vulnerability: CVE-2021-39275

    – CVSS Score: 7.5

    – Description: ap_escape_quotes() may write beyond the end of a buffer when given
                    malicious input. No included modules pass untrusted data to these
                    functions, but third-party / external modules may. This issue
                    affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2014-3581

    – CVSS Score: 5

    – Description: The cache_merge_headers_out function in modules/cache/cache_util.c
                    in the mod_cache module in the Apache HTTP Server before 2.4.11
                    allows remote attackers to cause a denial of service (NULL pointer
                    dereference and application crash) via an empty HTTP Content-Type
                    header.

- Vulnerability: CVE-2016-0736

    – CVSS Score: 5

    – Description: In Apache HTTP Server versions 2.4.0 to 2.4.23, mod_session_crypto was
                    encrypting its data/cookie using the configured ciphers with possibly
                    either CBC or ECB modes of operation (AES256-CBC by default), hence
                    no selectable or builtin authenticated encryption. This made it
                    vulnerable to padding oracle attacks, particularly with CBC.

- Vulnerability: CVE-2022-29404

    – CVSS Score: 5

    – Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a
                    lua script that calls r:parsebody(0) may cause a denial of service
                    due to no default limit on possible input size.

- Vulnerability: CVE-2018-1312

    – CVSS Score: 6.8

    – Description: In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest
                    authentication challenge, the nonce sent to prevent reply attacks
                    was not correctly generated using a pseudo-random seed. In a cluster
                    of servers using a common Digest authentication configuration, HTTP
                    requests could be replayed across servers by an attacker without
                    detection.

- Vulnerability: CVE-2022-22720

    – CVSS Score: 7.5

    – Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound
                    connection when errors are encountered discarding the request body,
                    exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2007-3205

    – CVSS Score: 5

    – Description: The parse_str function in (1) PHP, (2) Hardened-PHP, and (3) Suhosin,
                    when called without a second parameter, might allow remote attackers
                    to overwrite arbitrary variables by specifying variable names and
                    values in the string to be parsed. NOTE: it is not clear whether
                    this is a design limitation of the function or a bug in PHP, although
                    it is likely to be regarded as a bug in Hardened-PHP and Suhosin.

- Vulnerability: CVE-2017-15710

  – CVSS Score: 5

  – Description: In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.

- Vulnerability: CVE-2014-0226

  – CVSS Score: 6.8

  – Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

- Vulnerability: CVE-2022-2068

  – CVSS Score: 10

  – Description: In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze).

- Vulnerability: CVE-2009-3766

  – CVSS Score: 6.8

  – Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when OpenSSL is used, does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

- Vulnerability: CVE-2009-3767

  – CVSS Score: 4.3

- Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other versions, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2009-3765

  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2022-22721

  - CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2006-20001

  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2019-10092

  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

- Vulnerability: CVE-2021-3712

  - CVSS Score: 5.8

- Description: ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own "d2i" functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the "data" and "length" fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the "data" field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). It can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y).

- Vulnerability: CVE-2023-0464

  - CVSS Score: N/A

  - Description: A security vulnerability has been identified in all supported versionsof OpenSSL related to the verification of X.509 certificate chainsthat include policy constraints. Attackers may be able to exploit thisvulnerability by creating a malicious certificate chain that triggersexponential use of computational resources, leading to a denial-of-service(DoS) attack on affected systems.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0465

  - CVSS Score: N/A

- Description: Applications that use a non-default option when verifying
  certificates may bevulnerable to an attack from a malicious CA
  to circumvent certain checks.Invalid certificate policies in leaf
  certificates are silently ignored byOpenSSL and other certificate
  policy checks are skipped for that certificate.A malicious CA could
  use this to deliberately assert invalid certificate policiesin order
  to circumvent policy checking on the certificate altogether.Policy
  processing is disabled by default but can be enabled by passingthe
  '-policy' argument to the command line utilities or by calling
  the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0466

  - CVSS Score: N/A
  - Description: The function X509_VERIFY_PARAM_add0_policy() is documented
    toimplicitly enable the certificate policy check when doing
    certificateverification. However the implementation of the
    function does notenable the check which allows certificates
    with invalid or incorrectpolicies to pass the certificate
    verification.As suddenly enabling the policy check could break
    existing deployments it wasdecided to keep the existing behavior of
    the X509_VERIFY_PARAM_add0_policy()function.Instead the applications
    that require OpenSSL to perform certificatepolicy check need
    to use X509_VERIFY_PARAM_set1_policies() or explicitlyenable the
    policy check by calling X509_VERIFY_PARAM_set_flags() withthe
    X509_V_FLAG_POLICY_CHECK flag argument.Certificate policy checks
    are disabled by default in OpenSSL and are notcommonly used by
    applications.

- Vulnerability: CVE-2019-10098

  - CVSS Score: 5.8
  - Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with
    mod_rewrite that were intended to be self-referential might be fooled
    by encoded newlines and redirect instead to an unexpected URL within
    the request URL.

- Vulnerability: CVE-2015-0228

  - CVSS Score: 5
  - Description: The lua_websocket_read function in lua_request.c in the mod_lua module
    in the Apache HTTP Server through 2.4.12 allows remote attackers to
    cause a denial of service (child-process crash) by sending a crafted
    WebSocket Ping frame after a Lua script has called the wsupgrade
    function.

- Vulnerability: CVE-2016-5387

  - CVSS Score: 6.8
  - Description: The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18
    and therefore does not protect applications from the presence of
    untrusted client data in the HTTP_PROXY environment variable, which
    might allow remote attackers to redirect an application's outbound
    HTTP traffic to an arbitrary proxy server via a crafted Proxy header
    in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states
    "This mitigation has been assigned the identifier CVE-2016-5387"; in
    other words, this is not a CVE ID for a vulnerability.

- Vulnerability: CVE-2017-15715

  - CVSS Score: 6.8

- Description: In Apache httpd 2.4.0 to 2.4.29, the expression specified in
  <FilesMatch> could match '$' to a newline character in a malicious
  filename, rather than matching only the end of the filename. This
  could be exploited in environments where uploads of some files are
  are externally blocked, but only by matching the trailing portion of
  the filename.

- Vulnerability: CVE-2021-40438

  - CVSS Score: 6.8
  - Description: A crafted request uri-path can cause mod_proxy to forward the request
    to an origin server choosen by the remote user. This issue affects
    Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk
    Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP
    Server does not properly handle certain configuration sections that
    specify NiceValue but not AssignUserID, which might allow remote
    attackers to gain privileges by leveraging the root uid and root gid
    of an mpm-itk process.

- Vulnerability: CVE-2022-23943

  - CVSS Score: 7.5
  - Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server
    allows an attacker to overwrite heap memory with possibly attacker
    provided data. This issue affects Apache HTTP Server 2.4 version
    2.4.52 and prior versions.

- Vulnerability: CVE-2018-17199

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session
    checks the session expiry time before decoding the session. This
    causes session expiry time to be ignored for mod_session_cookie
    sessions since the expiry time is loaded when the session is decoded.

- Vulnerability: CVE-2021-23841

  - CVSS Score: 4.3
  - Description: The OpenSSL public API function X509_issuer_and_serial_hash() attempts
    to create a unique hash value based on the issuer and serial number
    data contained within an X509 certificate. However it fails to
    correctly handle any errors that may occur while parsing the
    issuer field (which might occur if the issuer field is maliciously
    constructed). This may subsequently result in a NULL pointer deref
    and a crash leading to a potential denial of service attack. The
    function X509_issuer_and_serial_hash() is never directly called by
    OpenSSL itself so applications are only vulnerable if they use this
    function directly and they use it on certificates that may have been
    obtained from untrusted sources. OpenSSL versions 1.1.1i and below
    are affected by this issue. Users of these versions should upgrade
    to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected
    by this issue. However OpenSSL 1.0.2 is out of support and no longer
    receiving public updates. Premium support customers of OpenSSL 1.0.2
    should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j.
    Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL
    1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2018-1301

  - CVSS Score: 4.3
  - Description: A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.

- Vulnerability: CVE-2018-1302

  - CVSS Score: 4.3
  - Description: When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.

- Vulnerability: CVE-2020-1968

  - CVSS Score: 4.3
  - Description: The Raccoon attack exploits a flaw in the TLS specification which can lead to an attacker being able to compute the pre-master secret in connections which have used a Diffie-Hellman (DH) based ciphersuite. In such a case this would result in the attacker being able to eavesdrop on all encrypted communications sent over that TLS connection. The attack can only be exploited if an implementation re-uses a DH secret across multiple TLS connections. Note that this issue only impacts DH ciphersuites and not ECDH ciphersuites. This issue affects OpenSSL 1.0.2 which is out of support and no longer receiving public updates. OpenSSL 1.1.1 is not vulnerable to this issue. Fixed in OpenSSL 1.0.2w (Affected 1.0.2-1.0.2v).

- Vulnerability: CVE-2021-34798

  - CVSS Score: 5
  - Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2023-25690

  - CVSS Score: N/A
  - Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2020-11985

  - CVSS Score: 4.3

- Description: IP address spoofing when proxying using mod_remoteip and mod_rewrite
  For configurations using proxying with mod_remoteip and certain
  mod_rewrite rules, an attacker could spoof their IP address for
  logging and PHP scripts. Note this issue was fixed in Apache HTTP
  Server 2.4.24 but was retrospectively allocated a low severity CVE in
  2020.

- **Vulnerability:** CVE-2021-4160

  - CVSS Score: 4.3
  - Description: There is a carry propagation bug in the MIPS32 and MIPS64 squaring
    procedure. Many EC algorithms are affected, including some of the
    TLS 1.3 default curves. Impact was not analyzed in detail, because
    the pre-requisites for attack are considered unlikely and include
    reusing private keys. Analysis suggests that attacks against RSA and
    DSA as a result of this defect would be very difficult to perform
    and are not believed likely. Attacks against DH are considered
    just feasible (although very difficult) because most of the work
    necessary to deduce information about a private key may be performed
    offline. The amount of resources required for such an attack would
    be significant. However, for an attack on TLS to be meaningful, the
    server would have to share the DH private key among multiple clients,
    which is no longer an option since CVE-2016-0701. This issue affects
    OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the
    releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For
    the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that
    is available to premium support customers only. It will be made
    available in 1.0.2zc when it is released. The issue only affects
    OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0).
    Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL
    1.0.2zc-dev (Affected 1.0.2-1.0.2zb).

- **Vulnerability:** CVE-2013-4352

  - CVSS Score: 4.3
  - Description: The cache_invalidate function in modules/cache/cache_storage.c in the
    mod_cache module in the Apache HTTP Server 2.4.6, when a caching
    forward proxy is enabled, allows remote HTTP servers to cause a
    denial of service (NULL pointer dereference and daemon crash) via
    vectors that trigger a missing hostname value.

- **Vulnerability:** CVE-2022-26377

  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request
    Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server
    allows an attacker to smuggle requests to the AJP server it forwards
    requests to. This issue affects Apache HTTP Server Apache HTTP
    Server 2.4 version 2.4.53 and prior versions.

- **Vulnerability:** CVE-2014-0098

  - CVSS Score: 5
  - Description: The log_cookie function in mod_log_config.c in the mod_log_config
    module in the Apache HTTP Server before 2.4.8 allows remote attackers
    to cause a denial of service (segmentation fault and daemon crash)
    via a crafted cookie that is not properly handled during truncation.

- **Vulnerability:** CVE-2016-8743

  - CVSS Score: 5

- Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

- **Vulnerability:** CVE-2024-40898

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- **Vulnerability:** CVE-2024-38474

  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- **Vulnerability:** CVE-2022-0778

  - CVSS Score: 5
  - Description: The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - TLS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

- Vulnerability: CVE-2020-1971

  – CVSS Score: 4.3

  – Description: The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s_server, s_client and verify tools have support for the "-crl_download" option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue. Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w).

- Vulnerability: CVE-2009-1390

  – CVSS Score: 6.8

  – Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2) GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS certificate in the chain is accepted instead of verifying the entire chain, which allows remote attackers to spoof trusted servers via a man-in-the-middle attack.

- Vulnerability: CVE-2012-3526

  – CVSS Score: 5

  – Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2024-5458

  – CVSS Score: N/A

  – Description: In PHP versions8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, due to a code logic error, filtering functions such as filter_var when validating URLs(FILTER_VALIDATE_URL) for certain types of URLs the function will result in invalid user information (username + password part of URLs) being treated as valid user information. This may lead to the downstream code accepting invalid URLs as valid and parsing them incorrectly.

- Vulnerability: CVE-2023-5678

  - CVSS Score: N/A

  - Description: Issue summary: Generating excessively long X9.42 DH keys or checkingexcessively long X9.42 DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_generate_key() togenerate an X9.42 DH key may experience long delays. Likewise, applicationsthat use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check()to check an X9.42 DH key or X9.42 DH parameters may experience long delays.Where the key or parameters that are being checked have been obtained froman untrusted source this may lead to a Denial of Service.While DH_check() performs all the necessary checks (as of CVE-2023-3817),DH_check_pub_key() doesn't make any of these checks, and is thereforevulnerable for excessively large P and Q parameters.Likewise, while DH_generate_key() performs a check for an excessively largeP, it doesn't check for an excessively large Q.An application that calls DH_generate_key() or DH_check_pub_key() andsupplies a key or parameters obtained from an untrusted source could bevulnerable to a Denial of Service attack.DH_generate_key() and DH_check_pub_key() are also called by a number ofother OpenSSL functions. An application calling any of those otherfunctions may similarly be affected. The other functions affected by thisare DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate().Also vulnerable are the OpenSSL pkey command line application when using the"-pubcheck" option, as well as the OpenSSL genpkey command line application.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2017-3736

  - CVSS Score: 4

  - Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

- Vulnerability: CVE-2017-3737

  - CVSS Score: 4.3

- Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

- **Vulnerability:** CVE-2019-1547

  - CVSS Score: 1.9

  - Description: Normally in OpenSSL EC groups always have a co-factor present and this is used in side channel resistant code paths. However, in some cases, it is possible to construct a group using explicit parameters (instead of using a named curve). In those cases it is possible that such a group does not have the cofactor present. This can occur even where all the parameters match a known named curve. If such a curve is used then OpenSSL falls back to non-side channel resistant code paths which may result in full key recovery during an ECDSA signature operation. In order to be vulnerable an attacker would have to have the ability to time the creation of a large number of signatures where explicit parameters with no co-factor present are in use by an application using libcrypto. For the avoidance of doubt libssl is not vulnerable because explicit parameters are never used. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).

- **Vulnerability:** CVE-2017-3735

  - CVSS Score: 5

  - Description: While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL before 1.0.2m and 1.1.0g.

- **Vulnerability:** CVE-2009-2299

  - CVSS Score: 5

  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- **Vulnerability:** CVE-2022-1292

  - CVSS Score: 10

- Description: The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n). Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).

- Vulnerability: CVE-2017-3738

  - CVSS Score: 4.3
  - Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

- Vulnerability: CVE-2012-4001

  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2022-37436

  - CVSS Score: N/A
  - Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2021-23840

  - CVSS Score: 5

- Description: Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissable length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2018-0737

  - CVSS Score: 4.3
  - Description: The OpenSSL RSA Key generation algorithm has been shown to be vulnerable to a cache timing side channel attack. An attacker with sufficient access to mount cache timing attacks during the RSA key generation process could recover the private key. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2b-1.0.2o).

- Vulnerability: CVE-2018-0734

  - CVSS Score: 4.3
  - Description: The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.1a (Affected 1.1.1). Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.0.2q (Affected 1.0.2-1.0.2p).

- Vulnerability: CVE-2018-0732

  - CVSS Score: 5
  - Description: During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime value to the client. This will cause the client to spend an unreasonably long period of time generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2-1.0.2o).

- Vulnerability: CVE-2017-9788

  - CVSS Score: 6.4
  - Description: In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.

- Vulnerability: CVE-2018-0739

  - CVSS Score: 4.3

- Description: Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o (Affected 1.0.2b-1.0.2n).

- Vulnerability: CVE-2014-8109

  - CVSS Score: 4.3
  - Description: mod_lua.c in the mod_lua module in the Apache HTTP Server 2.3.x and 2.4.x through 2.4.10 does not support an httpd configuration in which the same Lua authorization provider is used with different arguments within different contexts, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives, as demonstrated by a configuration that specifies authorization for one group to access a certain directory, and authorization for a second group to access a second directory.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2016-2161

  - CVSS Score: 5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.23, malicious input to mod_auth_digest can cause the server to crash, and each instance continues to crash even for subsequently valid requests.

- Vulnerability: CVE-2016-8612

  - CVSS Score: 3.3
  - Description: Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.

- Vulnerability: CVE-2019-1552

  - CVSS Score: 1.9

- Description: OpenSSL has internal defaults for a directory tree where it
  can find a configuration file as well as certificates used for
  verification in TLS. This directory is most commonly referred to
  as OPENSSLDIR, and is configurable with the --prefix / --openssldir
  configuration options. For OpenSSL versions 1.1.0 and 1.1.1, the
  mingw configuration targets assume that resulting programs and
  libraries are installed in a Unix-like environment and the default
  prefix for program installation as well as for OPENSSLDIR should be
  '/usr/local'. However, mingw programs are Windows programs, and as
  such, find themselves looking at sub-directories of 'C:/usr/local',
  which may be world writable, which enables untrusted users to modify
  OpenSSL's default configuration, insert CA certificates, modify (or
  even replace) existing engine modules, etc. For OpenSSL 1.0.2,
  '/usr/local/ssl' is used as default for OPENSSLDIR on all Unix and
  Windows targets, including Visual C builds. However, some build
  instructions for the diverse Windows targets on 1.0.2 encourage
  you to specify your own --prefix. OpenSSL versions 1.1.1, 1.1.0
  and 1.0.2 are affected by this issue. Due to the limited scope
  of affected deployments this has been assessed as low severity and
  therefore we are not creating new releases at this time. Fixed
  in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL
  1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected
  1.0.2-1.0.2s).

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5
    for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM
    Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows
    use an improper encryption algorithm and a weak key for maintaining
    the stored data of the node secret for the SecurID Authentication
    API, which allows local users to obtain sensitive information via
    cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication
    Agent 7.1 before 7.1.1 for Web for Internet Information Services,
    and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to
    inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2019-1551

  - CVSS Score: 5
  - Description: There is an overflow bug in the x64_64 Montgomery squaring procedure
    used in exponentiation with 512-bit moduli. No EC algorithms are
    affected. Analysis suggests that attacks against 2-prime RSA1024,
    3-prime RSA1536, and DSA1024 as a result of this defect would be
    very difficult to perform and are not believed likely. Attacks
    against DH512 are considered just feasible. However, for an attack
    the target would have to re-use the DH512 private key, which is not
    recommended anyway. Also applications directly using the low level
    API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME. Fixed
    in OpenSSL 1.1.1e (Affected 1.1.1-1.1.1d). Fixed in OpenSSL 1.0.2u
    (Affected 1.0.2-1.0.2t).

- Vulnerability: CVE-2019-1559

  - CVSS Score: 4.3

- Description: If an application encounters a fatal protocol error and then calls
  SSL_shutdown() twice (once to send a close_notify, and once to
  receive one) then OpenSSL can respond differently to the calling
  application if a 0 byte record is received with invalid padding
  compared to if a 0 byte record is received with an invalid MAC. If
  the application then behaves differently based on that in a way that
  is detectable to the remote peer, then this amounts to a padding
  oracle that could be used to decrypt data. In order for this to be
  exploitable "non-stitched" ciphersuites must be in use. Stitched
  ciphersuites are optimised implementations of certain commonly
  used ciphersuites. Also the application must call SSL_shutdown()
  twice even if a protocol error has occurred (applications should
  not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected
  1.0.2-1.0.2q).

- **Vulnerability:** CVE-2023-45802

  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a
    time window were the request's memory resources were not reclaimed
    immediately. Instead, de-allocation was deferred to connection
    close. A client could send new requests and resets, keeping the
    connection busy and open and causing the memory footprint to keep
    on growing. On connection close, all resources were reclaimed, but
    the process might run out of memory before that.This was found by
    the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset
    Exploit) with their own test client. During "normal" HTTP/2 use, the
    probability to hit this bug is very low. The kept memory would not
    become noticeable before the connection closes or times out.Users are
    recommended to upgrade to version 2.4.58, which fixes the issue.

- **Vulnerability:** CVE-2018-1283

  - CVSS Score: 3.5
  - Description: In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to
    forward its session data to CGI applications (SessionEnv on, not
    the default), a remote user may influence their content by using a
    "Session" header. This comes from the "HTTP_SESSION" variable name
    used by mod_session to forward its data to CGIs, since the prefix
    "HTTP_" is also used by the Apache HTTP Server to pass HTTP header
    fields, per CGI specifications.

- **Vulnerability:** CVE-2018-1303

  - CVSS Score: 5
  - Description: A specially crafted HTTP request header could have crashed the Apache
    HTTP Server prior to version 2.4.30 due to an out of bound read while
    preparing data to be cached in shared memory. It could be used as
    a Denial of Service attack against users of mod_cache_socache. The
    vulnerability is considered as low risk since mod_cache_socache is not
    widely used, mod_cache_disk is not concerned by this vulnerability.

- **Vulnerability:** CVE-2019-0217

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition
    in mod_auth_digest when running in a threaded server could allow a
    user with valid credentials to authenticate using another username,
    bypassing configured access control restrictions.

- **Vulnerability:** CVE-2022-28615

- CVSS Score: 6.4
- Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- Vulnerability: CVE-2022-28614

  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

- Vulnerability: CVE-2014-0117

  - CVSS Score: 4.3
  - Description: The mod_proxy module in the Apache HTTP Server 2.4.x before 2.4.10, when a reverse proxy is enabled, allows remote attackers to cause a denial of service (child-process crash) via a crafted HTTP Connection header.

- Vulnerability: CVE-2017-7679

  - CVSS Score: 7.5
  - Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

- Vulnerability: CVE-2017-9798

  - CVSS Score: 5
  - Description: Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.

- Vulnerability: CVE-2015-3185

  - CVSS Score: 4.3
  - Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

- Vulnerability: CVE-2015-3184

  - CVSS Score: 5

- Description: mod_authz_svn in Apache Subversion 1.7.x before 1.7.21 and 1.8.x before 1.8.14, when using Apache httpd 2.4.x, does not properly restrict anonymous access, which allows remote anonymous users to read hidden files via the path name.

- **Vulnerability:** CVE-2024-4577

  - CVSS Score: N/A
  - Description: In PHP versions8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in command line given toWin32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc.

- **Vulnerability:** CVE-2013-4365

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- **Vulnerability:** CVE-2018-5407

  - CVSS Score: 1.9
  - Description: Simultaneous Multi-threading (SMT) in processors can enable local users to exploit software vulnerable to timing attacks via a side-channel timing attack on 'port contention'.

- **Vulnerability:** CVE-2022-28330

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- **Vulnerability:** CVE-2021-32791

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

- **Vulnerability:** CVE-2021-32792

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.

- **Vulnerability:** CVE-2024-38476

  - CVSS Score: N/A

- Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- **Vulnerability: CVE-2024-38477**

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- **Vulnerability: CVE-2023-31122**

  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- **Vulnerability: CVE-2009-0796**

  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- **Vulnerability: CVE-2024-0727**

  - CVSS Score: N/A
  - Description: Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSLto crash leading to a potential Denial of Service attackImpact summary: Applications loading files in the PKCS12 format from untrustedsources might terminate abruptly.A file in PKCS12 format can contain certificates and keys and may come from anuntrusted source. The PKCS12 specification allows certain fields to be NULL, butOpenSSL does not correctly check for this case. This can lead to a NULL pointerdereference that results in OpenSSL crashing. If an application processes PKCS12files from an untrusted source using the OpenSSL APIs then that application willbe vulnerable to this issue.OpenSSL APIs that are vulnerable to this are: PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a similar issue in SMIME_write_PKCS7(). However since thisfunction is related to writing data we do not consider it security significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.

- **Vulnerability: CVE-2014-0118**

  - CVSS Score: 4.3
  - Description: The deflate_in_filter function in mod_deflate.c in the mod_deflate module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.

- **Vulnerability: CVE-2013-6438**

  - CVSS Score: 5

- Description: The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.

- Vulnerability: CVE-2020-1927

  - CVSS Score: 5.8
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.

- Vulnerability: CVE-2023-0286

  - CVSS Score: N/A
  - Description: There is a type confusion vulnerability relating to X.400 address processinginside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING butthe public structure definition for GENERAL_NAME incorrectly specified the typeof the x400Address field as ASN1_TYPE. This field is subsequently interpreted bythe OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than anASN1_STRING.When CRL checking is enabled (i.e. the application sets theX509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to passarbitrary pointers to a memcmp call, enabling them to read memory contents orenact a denial of service. In most cases, the attack requires the attacker toprovide both the certificate chain and CRL, neither of which need to have avalid signature. If the attacker only controls one of these inputs, the otherinput must already contain an X.400 address as a CRL distribution point, whichis uncommon. As such, this vulnerability is most likely to only affectapplications which have implemented their own functionality for retrieving CRLsover a network.

- Vulnerability: CVE-2023-3817

  - CVSS Score: N/A
  - Description: Issue summary: Checking excessively long DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH key or DH parameters may experience longdelays. Where the key or parameters that are being checked have been obtainedfrom an untrusted source this may lead to a Denial of Service.The function DH_check() performs various checks on DH parameters. After fixingCVE-2023-3446 it was discovered that a large q parameter value can also triggeran overly long computation during some of these checks. A correct q value,if present, cannot be larger than the modulus p parameter, thus it isunnecessary to perform these checks if q is larger than p.An application that calls DH_check() and supplies a key or parameters obtainedfrom an untrusted source could be vulnerable to a Denial of Service attack.The function DH_check() is itself called by a number of other OpenSSL functions.An application calling any of those other functions may similarly be affected.The other functions affected by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable are the OpenSSL dhparam and pkeyparam command line applicationswhen using the "-check" option.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2017-3167

- CVSS Score: 7.5
- Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.

- Vulnerability: CVE-2021-32786

  - CVSS Score: 5.8
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, `oidc_validate_redirect_url()` does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring `mod_auth_openidc` to only allow redirection whose destination matches a given regular expression.

- Vulnerability: CVE-2021-32785

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache (`OIDCCacheEncrypt off`, `OIDCSessionType server-cache`, `OIDCCacheType redis`), `mod_auth_openidc` wrongly performed argument interpolation before passing Redis requests to `hiredis`, which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the `hiredis` API. As a workaround, this vulnerability can be mitigated by setting `OIDCCacheEncrypt` to `on`, as cache keys are cryptographically hashed before use when this option is enabled.

- Vulnerability: CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2021-44790

  - CVSS Score: 7.5
  - Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

- Vulnerability: CVE-2016-4975

  – CVSS Score: 4.3

  – Description: Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).

- Vulnerability: CVE-2020-13938

  – CVSS Score: 2.1

  – Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

- Vulnerability: CVE-2023-2650

  – CVSS Score: N/A

  – Description: Issue summary: Processing some specially crafted ASN.1 object identifiers ordata containing them may be very slow.Impact summary: Applications that use OBJ_obj2txt() directly, or use any ofthe OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no messagesize limit may experience notable to very long delays when processing thosemessages, which may lead to a Denial of Service.An OBJECT IDENTIFIER is composed of a series of numbers – sub-identifiers -most of which have no size limit. OBJ_obj2txt() may be used to translatean ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSLtype ASN1_OBJECT) to its canonical numeric text form, which are thesub-identifiers of the OBJECT IDENTIFIER in decimal form, separated byperiods.When one of the sub-identifiers in the OBJECT IDENTIFIER is very large(these are sizes that are seen as absurdly large, taking up tens or hundredsof KiBs), the translation to a decimal number in text may take a very longtime. The time complexity is O(n$\hat{2}$) with 'n' being the size of thesub-identifiers in bytes (*).With OpenSSL 3.0, support to fetch cryptographic algorithms using names /identifiers in string form was introduced. This includes using OBJECTIDENTIFIERs in canonical numeric text form as identifiers for fetchingalgorithms.Such OBJECT IDENTIFIERs may be received through the ASN.1 structureAlgorithmIdentifier, which is commonly used in multiple protocols to specifywhat cryptographic algorithm should be used to sign or verify, encrypt ordecrypt, or digest passed data.Applications that call OBJ_obj2txt() directly with untrusted data areaffected, with any version of OpenSSL. If the use is for the mere purposeof display, the severity is considered low.In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME,CMS, CMP/CRMF or TS. It also impacts anything that processes X.509certificates, including simple things like verifying its signature.The impact on TLS is relatively low, because all versions of OpenSSL have a100KiB limit on the peer's certificate chain. Additionally, this onlyimpacts clients, or servers that have explicitly enabled clientauthentication.In OpenSSL 1.1.1 and 1.0.2, this only affects displaying diverse objects,such as X.509 certificates. This is assumed to not happen in such a waythat it would cause a Denial of Service, so these versions are considerednot affected by this issue in such a way that it would be cause for concern,and the severity is therefore considered low.

- Vulnerability: CVE-2023-0215

  – CVSS Score: N/A

- Description: The public API function BIO_new_NDEF is a helper function used for streamingASN.1 data via a BIO. It is primarily used internally to OpenSSL to support theSMIME, CMS and PKCS7 streaming capabilities, but may also be called directly byend user applications.The function receives a BIO from the caller, prepends a new BIO_f_asn1 filterBIO onto the front of it to form a BIO chain, and then returns the new head ofthe BIO chain to the caller. Under certain conditions, for example if a CMSrecipient public key is invalid, the new filter BIO is freed and the functionreturns a NULL result indicating a failure. However, in this case, the BIO chainis not properly cleaned up and the BIO passed by the caller still retainsinternal pointers to the previously freed filter BIO. If the caller then goes onto call BIO_pop() on the BIO then a use-after-free will occur. This will mostlikely result in a crash.This scenario occurs directly in the internal function B64_write_ASN1() whichmay cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() onthe BIO. This internal function is in turn called by the public API functionsPEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream,SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7.Other public API functions that may be impacted by this includei2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream andi2d_PKCS7_bio_stream.The OpenSSL cms and smime command line applications are similarly affected.

- Vulnerability: CVE-2015-3183

  - CVSS Score: 5
  - Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

- Vulnerability: CVE-2020-35452

  - CVSS Score: 6.8
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

- Vulnerability: CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2020-1934

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

- Vulnerability: CVE-2022-36760

  - CVSS Score: N/A

- Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-4304

  - CVSS Score: N/A

  - Description: A timing based side channel exists in the OpenSSL RSA Decryption implementationwhich could be sufficient to recover a plaintext across a network in aBleichenbacher style attack. To achieve a successful decryption an attackerwould have to be able to send a very large number of trial messages fordecryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5,RSA-OEAP and RSASVE.For example, in a TLS connection, RSA is commonly used by a client to send anencrypted pre-master secret to the server. An attacker that had observed agenuine connection between a client and a server could use this flaw to sendtrial messages to the server and record the time taken to process them. After asufficiently large number of messages the attacker could recover the pre-mastersecret used for the original connection and thus be able to decrypt theapplication data sent over that connection.

- Vulnerability: CVE-2019-1563

  - CVSS Score: 4.3

  - Description: In situations where an attacker receives automated notification of the success or failure of a decryption attempt an attacker, after sending a very large number of messages to be decrypted, can recover a CMS/PKCS7 transported encryption key or decrypt any RSA encrypted message that was encrypted with the public RSA key, using a Bleichenbacher padding oracle attack. Applications are not affected if they use a certificate together with the private RSA key to the CMS_decrypt or PKCS7_decrypt functions to select the correct recipient info to decrypt. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).

- Vulnerability: CVE-2014-3523

  - CVSS Score: 5

  - Description: Memory leak in the winnt_accept function in server/mpm/winnt/child.c in the WinNT MPM in the Apache HTTP Server 2.4.x before 2.4.10 on Windows, when the default AcceptFilter is enabled, allows remote attackers to cause a denial of service (memory consumption) via crafted requests.

- Vulnerability: CVE-2013-5704

  - CVSS Score: 5

  - Description: The mod_headers module in the Apache HTTP Server 2.2.22 allows remote attackers to bypass "RequestHeader unset" directives by placing a header in the trailer portion of data sent with chunked transfer coding. NOTE: the vendor states "this is not a security issue in httpd as such."

- Vulnerability: CVE-2019-17567

  - CVSS Score: 5

- Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

- **Vulnerability: CVE-2022-31813**

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

- **Vulnerability: CVE-2013-2220**

  - CVSS Score: 7.5
  - Description: Buffer overflow in the radius_get_vendor_attr function in the Radius extension before 1.2.7 for PHP allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a large Vendor Specific Attributes (VSA) length value.

- **Vulnerability: CVE-2012-4360**

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- **Vulnerability: CVE-2014-0231**

  - CVSS Score: 5
  - Description: The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.

- **Vulnerability: CVE-2021-26690**

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service

- **Vulnerability: CVE-2021-26691**

  - CVSS Score: 7.5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow

- **Vulnerability: CVE-2019-0220**

  - CVSS Score: 5
  - Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.

- **Vulnerability: CVE-2022-30556**

- CVSS Score: 5
- Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- Vulnerability: CVE-2021-39275

  - CVSS Score: 7.5
  - Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2014-3581

  - CVSS Score: 5
  - Description: The cache_merge_headers_out function in modules/cache/cache_util.c in the mod_cache module in the Apache HTTP Server before 2.4.11 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty HTTP Content-Type header.

- Vulnerability: CVE-2016-0736

  - CVSS Score: 5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.23, mod_session_crypto was encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This made it vulnerable to padding oracle attacks, particularly with CBC.

- Vulnerability: CVE-2022-29404

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2018-1312

  - CVSS Score: 6.8
  - Description: In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

- Vulnerability: CVE-2022-22720

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2007-3205

  - CVSS Score: 5
  - Description: The parse_str function in (1) PHP, (2) Hardened-PHP, and (3) Suhosin, when called without a second parameter, might allow remote attackers to overwrite arbitrary variables by specifying variable names and values in the string to be parsed. NOTE: it is not clear whether this is a design limitation of the function or a bug in PHP, although it is likely to be regarded as a bug in Hardened-PHP and Suhosin.

- Vulnerability: CVE-2017-15710

  – CVSS Score: 5

  – Description: In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.

- Vulnerability: CVE-2014-0226

  – CVSS Score: 6.8

  – Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

- Vulnerability: CVE-2022-2068

  – CVSS Score: 10

  – Description: In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze).

- Vulnerability: CVE-2009-3766

  – CVSS Score: 6.8

  – Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when OpenSSL is used, does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

- Vulnerability: CVE-2009-3767

  – CVSS Score: 4.3

- Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other versions, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2009-3765

  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2022-22721

  - CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2006-20001

  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2019-10092

  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

- Vulnerability: CVE-2021-3712

  - CVSS Score: 5.8

- Description: ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own "d2i" functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the "data" and "length" fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the "data" field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). It can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y).

- Vulnerability: CVE-2023-0464

  - CVSS Score: N/A

  - Description: A security vulnerability has been identified in all supported versionsof OpenSSL related to the verification of X.509 certificate chainsthat include policy constraints. Attackers may be able to exploit thisvulnerability by creating a malicious certificate chain that triggersexponential use of computational resources, leading to a denial-of-service(DoS) attack on affected systems.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0465

  - CVSS Score: N/A

– Description: Applications that use a non-default option when verifying
certificates may bevulnerable to an attack from a malicious CA
to circumvent certain checks.Invalid certificate policies in leaf
certificates are silently ignored byOpenSSL and other certificate
policy checks are skipped for that certificate.A malicious CA could
use this to deliberately assert invalid certificate policiesin order
to circumvent policy checking on the certificate altogether.Policy
processing is disabled by default but can be enabled by passingthe
'-policy' argument to the command line utilities or by calling
the'X509_VERIFY_PARAM_set1_policies()' function.

• Vulnerability: CVE-2023-0466

   – CVSS Score: N/A

   – Description: The function X509_VERIFY_PARAM_add0_policy() is documented
toimplicitly enable the certificate policy check when doing
certificateverification. However the implementation of the
function does notenable the check which allows certificates
with invalid or incorrectpolicies to pass the certificate
verification.As suddenly enabling the policy check could break
existing deployments it wasdecided to keep the existing behavior of
the X509_VERIFY_PARAM_add0_policy()function.Instead the applications
that require OpenSSL to perform certificatepolicy check need
to use X509_VERIFY_PARAM_set1_policies() or explicitlyenable the
policy check by calling X509_VERIFY_PARAM_set_flags() withthe
X509_V_FLAG_POLICY_CHECK flag argument.Certificate policy checks
are disabled by default in OpenSSL and are notcommonly used by
applications.

• Vulnerability: CVE-2019-10098

   – CVSS Score: 5.8

   – Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with
mod_rewrite that were intended to be self-referential might be fooled
by encoded newlines and redirect instead to an unexpected URL within
the request URL.

• Vulnerability: CVE-2015-0228

   – CVSS Score: 5

   – Description: The lua_websocket_read function in lua_request.c in the mod_lua module
in the Apache HTTP Server through 2.4.12 allows remote attackers to
cause a denial of service (child-process crash) by sending a crafted
WebSocket Ping frame after a Lua script has called the wsupgrade
function.

• Vulnerability: CVE-2016-5387

   – CVSS Score: 6.8

   – Description: The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18
and therefore does not protect applications from the presence of
untrusted client data in the HTTP_PROXY environment variable, which
might allow remote attackers to redirect an application's outbound
HTTP traffic to an arbitrary proxy server via a crafted Proxy header
in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states
"This mitigation has been assigned the identifier CVE-2016-5387"; in
other words, this is not a CVE ID for a vulnerability.

• Vulnerability: CVE-2017-15715

   – CVSS Score: 6.8

- Description: In Apache httpd 2.4.0 to 2.4.29, the expression specified in
  <FilesMatch> could match '$' to a newline character in a malicious
  filename, rather than matching only the end of the filename. This
  could be exploited in environments where uploads of some files are
  are externally blocked, but only by matching the trailing portion of
  the filename.

- Vulnerability: CVE-2021-40438

  - CVSS Score: 6.8
  - Description: A crafted request uri-path can cause mod_proxy to forward the request
    to an origin server choosen by the remote user. This issue affects
    Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk
    Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP
    Server does not properly handle certain configuration sections that
    specify NiceValue but not AssignUserID, which might allow remote
    attackers to gain privileges by leveraging the root uid and root gid
    of an mpm-itk process.

- Vulnerability: CVE-2022-23943

  - CVSS Score: 7.5
  - Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server
    allows an attacker to overwrite heap memory with possibly attacker
    provided data. This issue affects Apache HTTP Server 2.4 version
    2.4.52 and prior versions.

- Vulnerability: CVE-2018-17199

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session
    checks the session expiry time before decoding the session. This
    causes session expiry time to be ignored for mod_session_cookie
    sessions since the expiry time is loaded when the session is decoded.

- Vulnerability: CVE-2021-23841

  - CVSS Score: 4.3
  - Description: The OpenSSL public API function X509_issuer_and_serial_hash() attempts
    to create a unique hash value based on the issuer and serial number
    data contained within an X509 certificate. However it fails to
    correctly handle any errors that may occur while parsing the
    issuer field (which might occur if the issuer field is maliciously
    constructed). This may subsequently result in a NULL pointer deref
    and a crash leading to a potential denial of service attack. The
    function X509_issuer_and_serial_hash() is never directly called by
    OpenSSL itself so applications are only vulnerable if they use this
    function directly and they use it on certificates that may have been
    obtained from untrusted sources. OpenSSL versions 1.1.1i and below
    are affected by this issue. Users of these versions should upgrade
    to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected
    by this issue. However OpenSSL 1.0.2 is out of support and no longer
    receiving public updates. Premium support customers of OpenSSL 1.0.2
    should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j.
    Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL
    1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2018-1301

  – CVSS Score: 4.3
  – Description: A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.

- Vulnerability: CVE-2018-1302

  – CVSS Score: 4.3
  – Description: When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.

- Vulnerability: CVE-2020-1968

  – CVSS Score: 4.3
  – Description: The Raccoon attack exploits a flaw in the TLS specification which can lead to an attacker being able to compute the pre-master secret in connections which have used a Diffie-Hellman (DH) based ciphersuite. In such a case this would result in the attacker being able to eavesdrop on all encrypted communications sent over that TLS connection. The attack can only be exploited if an implementation re-uses a DH secret across multiple TLS connections. Note that this issue only impacts DH ciphersuites and not ECDH ciphersuites. This issue affects OpenSSL 1.0.2 which is out of support and no longer receiving public updates. OpenSSL 1.1.1 is not vulnerable to this issue. Fixed in OpenSSL 1.0.2w (Affected 1.0.2-1.0.2v).

- Vulnerability: CVE-2021-34798

  – CVSS Score: 5
  – Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2023-25690

  – CVSS Score: N/A
  – Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2020-11985

  – CVSS Score: 4.3

- Description: IP address spoofing when proxying using mod_remoteip and mod_rewrite
  For configurations using proxying with mod_remoteip and certain
  mod_rewrite rules, an attacker could spoof their IP address for
  logging and PHP scripts. Note this issue was fixed in Apache HTTP
  Server 2.4.24 but was retrospectively allocated a low severity CVE in
  2020.

- **Vulnerability: CVE-2021-4160**

  - CVSS Score: 4.3
  - Description: There is a carry propagation bug in the MIPS32 and MIPS64 squaring
    procedure. Many EC algorithms are affected, including some of the
    TLS 1.3 default curves. Impact was not analyzed in detail, because
    the pre-requisites for attack are considered unlikely and include
    reusing private keys. Analysis suggests that attacks against RSA and
    DSA as a result of this defect would be very difficult to perform
    and are not believed likely. Attacks against DH are considered
    just feasible (although very difficult) because most of the work
    necessary to deduce information about a private key may be performed
    offline. The amount of resources required for such an attack would
    be significant. However, for an attack on TLS to be meaningful, the
    server would have to share the DH private key among multiple clients,
    which is no longer an option since CVE-2016-0701. This issue affects
    OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the
    releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For
    the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that
    is available to premium support customers only. It will be made
    available in 1.0.2zc when it is released. The issue only affects
    OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0).
    Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL
    1.0.2zc-dev (Affected 1.0.2-1.0.2zb).

- **Vulnerability: CVE-2013-4352**

  - CVSS Score: 4.3
  - Description: The cache_invalidate function in modules/cache/cache_storage.c in the
    mod_cache module in the Apache HTTP Server 2.4.6, when a caching
    forward proxy is enabled, allows remote HTTP servers to cause a
    denial of service (NULL pointer dereference and daemon crash) via
    vectors that trigger a missing hostname value.

- **Vulnerability: CVE-2022-26377**

  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request
    Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server
    allows an attacker to smuggle requests to the AJP server it forwards
    requests to. This issue affects Apache HTTP Server Apache HTTP
    Server 2.4 version 2.4.53 and prior versions.

- **Vulnerability: CVE-2014-0098**

  - CVSS Score: 5
  - Description: The log_cookie function in mod_log_config.c in the mod_log_config
    module in the Apache HTTP Server before 2.4.8 allows remote attackers
    to cause a denial of service (segmentation fault and daemon crash)
    via a crafted cookie that is not properly handled during truncation.

- **Vulnerability: CVE-2016-8743**

  - CVSS Score: 5

- Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

- **Vulnerability:** CVE-2024-40898

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- **Vulnerability:** CVE-2024-38474

  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- **Vulnerability:** CVE-2022-0778

  - CVSS Score: 5
  - Description: The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - TLS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

- Vulnerability: CVE-2020-1971

  - CVSS Score: 4.3
  - Description: The X.509 GeneralName type is a generic type for representing
                 different types of names. One of those name types is known as
                 EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which
                 compares different instances of a GENERAL_NAME to see if they
                 are equal or not. This function behaves incorrectly when both
                 GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference
                 and a crash may occur leading to a possible denial of service
                 attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two
                 purposes: 1) Comparing CRL distribution point names between an
                 available CRL and a CRL distribution point embedded in an X509
                 certificate 2) When verifying that a timestamp response token signer
                 matches the timestamp authority name (exposed via the API functions
                 TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can
                 control both items being compared then that attacker could trigger
                 a crash. For example if the attacker can trick a client or server
                 into checking a malicious certificate against a malicious CRL then
                 this may occur. Note that some applications automatically download
                 CRLs based on a URL embedded in a certificate. This checking happens
                 prior to the signatures on the certificate and CRL being verified.
                 OpenSSL's s_server, s_client and verify tools have support for the
                 "-crl_download" option which implements automatic CRL downloading and
                 this attack has been demonstrated to work against those tools. Note
                 that an unrelated bug means that affected versions of OpenSSL cannot
                 parse or construct correct encodings of EDIPARTYNAME. However it is
                 possible to construct a malformed EDIPARTYNAME that OpenSSL's parser
                 will accept and hence trigger this attack. All OpenSSL 1.1.1 and
                 1.0.2 versions are affected by this issue. Other OpenSSL releases
                 are out of support and have not been checked. Fixed in OpenSSL
                 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected
                 1.0.2-1.0.2w).

- Vulnerability: CVE-2009-1390

  - CVSS Score: 6.8
  - Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2)
                 GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS
                 certificate in the chain is accepted instead of verifying the entire
                 chain, which allows remote attackers to spoof trusted servers via a
                 man-in-the-middle attack.

- Vulnerability: CVE-2012-3526

  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the
                 Apache HTTP Server allows remote attackers to cause a denial of
                 service (server or application crash) via multiple X-Forwarded-For
                 headers in a request.

- Vulnerability: CVE-2024-5458

  - CVSS Score: N/A
  - Description: In PHP versions8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.*
                 before 8.3.8, due to a code logic error, filtering functions such
                 as filter_var when validating URLs(FILTER_VALIDATE_URL) for certain
                 types of URLs the function will result in invalid user information
                 (username + password part of URLs) being treated as valid user
                 information. This may lead to the downstream code accepting invalid
                 URLs as valid and parsing them incorrectly.

- Vulnerability: CVE-2023-5678

    – CVSS Score: N/A

    – Description: Issue summary: Generating excessively long X9.42 DH keys or checkingexcessively long X9.42 DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_generate_key() togenerate an X9.42 DH key may experience long delays. Likewise, applicationsthat use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check()to check an X9.42 DH key or X9.42 DH parameters may experience long delays.Where the key or parameters that are being checked have been obtained froman untrusted source this may lead to a Denial of Service.While DH_check() performs all the necessary checks (as of CVE-2023-3817),DH_check_pub_key() doesn't make any of these checks, and is thereforevulnerable for excessively large P and Q parameters.Likewise, while DH_generate_key() performs a check for an excessively largeP, it doesn't check for an excessively large Q.An application that calls DH_generate_key() or DH_check_pub_key() andsupplies a key or parameters obtained from an untrusted source could bevulnerable to a Denial of Service attack.DH_generate_key() and DH_check_pub_key() are also called by a number ofother OpenSSL functions. An application calling any of those otherfunctions may similarly be affected. The other functions affected by thisare DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate().Also vulnerable are the OpenSSL pkey command line application when using the"-pubcheck" option, as well as the OpenSSL genpkey command line application.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2017-3736

    – CVSS Score: 4

    – Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

- Vulnerability: CVE-2017-3737

    – CVSS Score: 4.3

- Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

- Vulnerability: CVE-2019-1547

  - CVSS Score: 1.9

  - Description: Normally in OpenSSL EC groups always have a co-factor present and this is used in side channel resistant code paths. However, in some cases, it is possible to construct a group using explicit parameters (instead of using a named curve). In those cases it is possible that such a group does not have the cofactor present. This can occur even where all the parameters match a known named curve. If such a curve is used then OpenSSL falls back to non-side channel resistant code paths which may result in full key recovery during an ECDSA signature operation. In order to be vulnerable an attacker would have to have the ability to time the creation of a large number of signatures where explicit parameters with no co-factor present are in use by an application using libcrypto. For the avoidance of doubt libssl is not vulnerable because explicit parameters are never used. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).

- Vulnerability: CVE-2017-3735

  - CVSS Score: 5

  - Description: While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL before 1.0.2m and 1.1.0g.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5

  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2022-1292

  - CVSS Score: 10

– Description: The c_rehash script does not properly sanitise shell metacharacters
to prevent command injection. This script is distributed by
some operating systems in a manner where it is automatically
executed. On such operating systems, an attacker could execute
arbitrary commands with the privileges of the script. Use of the
c_rehash script is considered obsolete and should be replaced by the
OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected
3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n).
Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).

- Vulnerability: CVE-2017-3738

  – CVSS Score: 4.3

  – Description: There is an overflow bug in the AVX2 Montgomery multiplication
procedure used in exponentiation with 1024-bit moduli. No EC
algorithms are affected. Analysis suggests that attacks against
RSA and DSA as a result of this defect would be very difficult to
perform and are not believed likely. Attacks against DH1024 are
considered just feasible, because most of the work necessary to
deduce information about a private key may be performed offline. The
amount of resources required for such an attack would be significant.
However, for an attack on TLS to be meaningful, the server would have
to share the DH1024 private key among multiple clients, which is no
longer an option since CVE-2016-0701. This only affects processors
that support the AVX2 but not ADX extensions like Intel Haswell
(4th generation). Note: The impact from this issue is similar to
CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version
1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n.
Due to the low severity of this issue we are not issuing a new
release of OpenSSL 1.1.0 at this time. The fix will be included in
OpenSSL 1.1.0h when it becomes available. The fix is also available
in commit e502cc86d in the OpenSSL git repository.

- Vulnerability: CVE-2012-4001

  – CVSS Score: 5

  – Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server
does not properly verify its host name, which allows remote attackers
to trigger HTTP requests to arbitrary hosts via unspecified vectors,
as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2022-37436

  – CVSS Score: N/A

  – Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause
the response headers to be truncated early, resulting in some headers
being incorporated into the response body. If the later headers have
any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2021-23840

  – CVSS Score: 5

- Description: Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissable length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2018-0737

  - CVSS Score: 4.3
  - Description: The OpenSSL RSA Key generation algorithm has been shown to be vulnerable to a cache timing side channel attack. An attacker with sufficient access to mount cache timing attacks during the RSA key generation process could recover the private key. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2b-1.0.2o).

- Vulnerability: CVE-2018-0734

  - CVSS Score: 4.3
  - Description: The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.1a (Affected 1.1.1). Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.0.2q (Affected 1.0.2-1.0.2p).

- Vulnerability: CVE-2018-0732

  - CVSS Score: 5
  - Description: During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime value to the client. This will cause the client to spend an unreasonably long period of time generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2-1.0.2o).

- Vulnerability: CVE-2017-9788

  - CVSS Score: 6.4
  - Description: In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.

- Vulnerability: CVE-2018-0739

  - CVSS Score: 4.3

- Description: Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o (Affected 1.0.2b-1.0.2n).

- Vulnerability: CVE-2014-8109

  - CVSS Score: 4.3
  - Description: mod_lua.c in the mod_lua module in the Apache HTTP Server 2.3.x and 2.4.x through 2.4.10 does not support an httpd configuration in which the same Lua authorization provider is used with different arguments within different contexts, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives, as demonstrated by a configuration that specifies authorization for one group to access a certain directory, and authorization for a second group to access a second directory.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2016-2161

  - CVSS Score: 5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.23, malicious input to mod_auth_digest can cause the server to crash, and each instance continues to crash even for subsequently valid requests.

- Vulnerability: CVE-2016-8612

  - CVSS Score: 3.3
  - Description: Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.

- Vulnerability: CVE-2019-1552

  - CVSS Score: 1.9

- Description: OpenSSL has internal defaults for a directory tree where it
  can find a configuration file as well as certificates used for
  verification in TLS. This directory is most commonly referred to
  as OPENSSLDIR, and is configurable with the --prefix / --openssldir
  configuration options. For OpenSSL versions 1.1.0 and 1.1.1, the
  mingw configuration targets assume that resulting programs and
  libraries are installed in a Unix-like environment and the default
  prefix for program installation as well as for OPENSSLDIR should be
  '/usr/local'. However, mingw programs are Windows programs, and as
  such, find themselves looking at sub-directories of 'C:/usr/local',
  which may be world writable, which enables untrusted users to modify
  OpenSSL's default configuration, insert CA certificates, modify (or
  even replace) existing engine modules, etc. For OpenSSL 1.0.2,
  '/usr/local/ssl' is used as default for OPENSSLDIR on all Unix and
  Windows targets, including Visual C builds. However, some build
  instructions for the diverse Windows targets on 1.0.2 encourage
  you to specify your own --prefix. OpenSSL versions 1.1.1, 1.1.0
  and 1.0.2 are affected by this issue. Due to the limited scope
  of affected deployments this has been assessed as low severity and
  therefore we are not creating new releases at this time. Fixed
  in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL
  1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected
  1.0.2-1.0.2s).

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5
    for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM
    Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows
    use an improper encryption algorithm and a weak key for maintaining
    the stored data of the node secret for the SecurID Authentication
    API, which allows local users to obtain sensitive information via
    cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication
    Agent 7.1 before 7.1.1 for Web for Internet Information Services,
    and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to
    inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2019-1551

  - CVSS Score: 5
  - Description: There is an overflow bug in the x64_64 Montgomery squaring procedure
    used in exponentiation with 512-bit moduli. No EC algorithms are
    affected. Analysis suggests that attacks against 2-prime RSA1024,
    3-prime RSA1536, and DSA1024 as a result of this defect would be
    very difficult to perform and are not believed likely. Attacks
    against DH512 are considered just feasible. However, for an attack
    the target would have to re-use the DH512 private key, which is not
    recommended anyway. Also applications directly using the low level
    API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME. Fixed
    in OpenSSL 1.1.1e (Affected 1.1.1-1.1.1d). Fixed in OpenSSL 1.0.2u
    (Affected 1.0.2-1.0.2t).

- Vulnerability: CVE-2019-1559

  - CVSS Score: 4.3

- Description: If an application encounters a fatal protocol error and then calls
  SSL_shutdown() twice (once to send a close_notify, and once to
  receive one) then OpenSSL can respond differently to the calling
  application if a 0 byte record is received with invalid padding
  compared to if a 0 byte record is received with an invalid MAC. If
  the application then behaves differently based on that in a way that
  is detectable to the remote peer, then this amounts to a padding
  oracle that could be used to decrypt data. In order for this to be
  exploitable "non-stitched" ciphersuites must be in use. Stitched
  ciphersuites are optimised implementations of certain commonly
  used ciphersuites. Also the application must call SSL_shutdown()
  twice even if a protocol error has occurred (applications should
  not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected
  1.0.2-1.0.2q).

- **Vulnerability:** CVE-2023-45802

  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a
    time window were the request's memory resources were not reclaimed
    immediately. Instead, de-allocation was deferred to connection
    close. A client could send new requests and resets, keeping the
    connection busy and open and causing the memory footprint to keep
    on growing. On connection close, all resources were reclaimed, but
    the process might run out of memory before that.This was found by
    the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset
    Exploit) with their own test client. During "normal" HTTP/2 use, the
    probability to hit this bug is very low. The kept memory would not
    become noticeable before the connection closes or times out.Users are
    recommended to upgrade to version 2.4.58, which fixes the issue.

- **Vulnerability:** CVE-2018-1283

  - CVSS Score: 3.5
  - Description: In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to
    forward its session data to CGI applications (SessionEnv on, not
    the default), a remote user may influence their content by using a
    "Session" header. This comes from the "HTTP_SESSION" variable name
    used by mod_session to forward its data to CGIs, since the prefix
    "HTTP_" is also used by the Apache HTTP Server to pass HTTP header
    fields, per CGI specifications.

- **Vulnerability:** CVE-2018-1303

  - CVSS Score: 5
  - Description: A specially crafted HTTP request header could have crashed the Apache
    HTTP Server prior to version 2.4.30 due to an out of bound read while
    preparing data to be cached in shared memory. It could be used as
    a Denial of Service attack against users of mod_cache_socache. The
    vulnerability is considered as low risk since mod_cache_socache is not
    widely used, mod_cache_disk is not concerned by this vulnerability.

- **Vulnerability:** CVE-2019-0217

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition
    in mod_auth_digest when running in a threaded server could allow a
    user with valid credentials to authenticate using another username,
    bypassing configured access control restrictions.

- **Vulnerability:** CVE-2022-28615

- CVSS Score: 6.4
- Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- Vulnerability: CVE-2022-28614

  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

11.6   IP Address: 159.149.53.224

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 4

- High Vulnerabilities: 28

- Medium Vulnerabilities: 184

- Low Vulnerabilities: 16

- Total Vulnerabilities: 232

Services Running on IP Address

- Service: Apache httpd

    – Port: 80
    – Version: 2.4.6
    – Location: https://www.sedutedilaurea.veterinaria.unimi.it/

- Service: Apache httpd

    – Port: 443
    – Version: 2.4.6
    – Location: http://www.sedutedilaurea.veterinaria.unimi.it/login.php

Vulnerabilities Found

- Vulnerability: CVE-2014-0117

    – CVSS Score: 4.3
    – Description: The mod_proxy module in the Apache HTTP Server 2.4.x before 2.4.10, when a reverse proxy is enabled, allows remote attackers to cause a denial of service (child-process crash) via a crafted HTTP Connection header.

- Vulnerability: CVE-2017-7679

    – CVSS Score: 7.5
    – Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

- Vulnerability: CVE-2017-7272

    – CVSS Score: 5.8
    – Description: PHP through 7.1.11 enables potential SSRF in applications that accept an fsockopen or pfsockopen hostname argument with an expectation that the port number is constrained. Because a :port syntax is recognized, fsockopen will use the port number that is specified in the hostname argument, instead of the port number in the second argument of the function.

- Vulnerability: CVE-2017-9798

    – CVSS Score: 5

– Description: Apache httpd allows remote attackers to read secret data from process
   memory if the Limit directive can be set in a user's .htaccess file,
   or if httpd.conf has certain misconfigurations, aka Optionsbleed.
   This affects the Apache HTTP Server through 2.2.34 and 2.4.x through
   2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request
   when attempting to read secret data. This is a use-after-free
   issue and thus secret data is not always sent, and the specific data
   depends on many factors including configuration. Exploitation with
   .htaccess can be blocked with a patch to the ap_limit_section function
   in server/core.c.

- Vulnerability: CVE-2015-3185

   – CVSS Score: 4.3

   – Description: The ap_some_auth_required function in server/request.c in the Apache
      HTTP Server 2.4.x before 2.4.14 does not consider that a Require
      directive may be associated with an authorization setting rather
      than an authentication setting, which allows remote attackers to
      bypass intended access restrictions in opportunistic circumstances
      by leveraging the presence of a module that relies on the 2.2 API
      behavior.

- Vulnerability: CVE-2015-3184

   – CVSS Score: 5

   – Description: mod_authz_svn in Apache Subversion 1.7.x before 1.7.21 and 1.8.x
      before 1.8.14, when using Apache httpd 2.4.x, does not properly
      restrict anonymous access, which allows remote anonymous users to
      read hidden files via the path name.

- Vulnerability: CVE-2024-4577

   – CVSS Score: N/A

   – Description: In PHP versions8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before
      8.3.8, when using Apache and PHP-CGI on Windows, if the system is set
      up to use certain code pages, Windows may use "Best-Fit" behavior to
      replace characters in command line given toWin32 API functions. PHP
      CGI module may misinterpret those characters as PHP options, which
      may allow a malicious user to pass options to PHP binary being run,
      and thus reveal the source code of scripts, run arbitrary PHP code on
      the server, etc.

- Vulnerability: CVE-2013-4365

   – CVSS Score: 7.5

   – Description: Heap-based buffer overflow in the fcgid_header_bucket_read function
      in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache
      HTTP Server allows remote attackers to have an unspecified impact via
      unknown vectors.

- Vulnerability: CVE-2018-5407

   – CVSS Score: 1.9

   – Description: Simultaneous Multi-threading (SMT) in processors can enable local
      users to exploit software vulnerable to timing attacks via a
      side-channel timing attack on 'port contention'.

- Vulnerability: CVE-2022-28330

   – CVSS Score: 5

   – Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond
      bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2021-32791

  – CVSS Score: 4.3
  – Description: mod_auth_openidc is an authentication/authorization module for the
                 Apache 2.x HTTP server that functions as an OpenID Connect Relying
                 Party, authenticating users against an OpenID Connect Provider.
                 In mod_auth_openidc before version 2.4.9, the AES GCM encryption in
                 mod_auth_openidc uses a static IV and AAD. It is important to fix
                 because this creates a static nonce and since aes-gcm is a stream
                 cipher, this can lead to known cryptographic issues, since the same
                 key is being reused. From 2.4.9 onwards this has been patched to use
                 dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2021-32792

  – CVSS Score: 4.3
  – Description: mod_auth_openidc is an authentication/authorization module for the
                 Apache 2.x HTTP server that functions as an OpenID Connect Relying
                 Party, authenticating users against an OpenID Connect Provider. In
                 mod_auth_openidc before version 2.4.9, there is an XSS vulnerability
                 in when using 'OIDCPreservePost On'.

- Vulnerability: CVE-2024-38476

  – CVSS Score: N/A
  – Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are
                 vulnerably to information disclosure, SSRF or local script execution
                 viabackend applications whose response headers are malicious or
                 exploitable.Users are recommended to upgrade to version 2.4.60, which
                 fixes this issue.

- Vulnerability: CVE-2024-38477

  – CVSS Score: N/A
  – Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59
                 and earlier allows an attacker to crash the server via a malicious
                 request.Users are recommended to upgrade to version 2.4.60, which
                 fixes this issue.

- Vulnerability: CVE-2023-31122

  – CVSS Score: N/A
  – Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP
                 Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2009-0796

  – CVSS Score: 2.6
  – Description: Cross-site scripting (XSS) vulnerability in Status.pm in
                 Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the
                 Apache HTTP Server, when /perl-status is accessible, allows remote
                 attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2024-0727

  – CVSS Score: N/A

- Description: Issue summary: Processing a maliciously formatted PKCS12 file
  may lead OpenSSLto crash leading to a potential Denial of Service
  attackImpact summary: Applications loading files in the PKCS12
  format from untrustedsources might terminate abruptly.A file in
  PKCS12 format can contain certificates and keys and may come from
  anuntrusted source. The PKCS12 specification allows certain fields
  to be NULL, butOpenSSL does not correctly check for this case.
  This can lead to a NULL pointerdereference that results in OpenSSL
  crashing. If an application processes PKCS12files from an untrusted
  source using the OpenSSL APIs then that application willbe vulnerable
  to this issue.OpenSSL APIs that are vulnerable to this are:
  PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(),
  PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a
  similar issue in SMIME_write_PKCS7(). However since thisfunction
  is related to writing data we do not consider it security
  significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected
  by this issue.

- **Vulnerability:** CVE-2014-0118

  - CVSS Score: 4.3
  - Description: The deflate_in_filter function in mod_deflate.c in the mod_deflate
    module in the Apache HTTP Server before 2.4.10, when request body
    decompression is enabled, allows remote attackers to cause a denial
    of service (resource consumption) via crafted request data that
    decompresses to a much larger size.

- **Vulnerability:** CVE-2013-6438

  - CVSS Score: 5
  - Description: The dav_xml_get_cdata function in main/util.c in the mod_dav module
    in the Apache HTTP Server before 2.4.8 does not properly remove
    whitespace characters from CDATA sections, which allows remote
    attackers to cause a denial of service (daemon crash) via a crafted
    DAV WRITE request.

- **Vulnerability:** CVE-2020-1927

  - CVSS Score: 5.8
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with
    mod_rewrite that were intended to be self-referential might be fooled
    by encoded newlines and redirect instead to an an unexpected URL
    within the request URL.

- **Vulnerability:** CVE-2023-0286

  - CVSS Score: N/A

- Description: There is a type confusion vulnerability relating to X.400 address processinginside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING butthe public structure definition for GENERAL_NAME incorrectly specified the typeof the x400Address field as ASN1_TYPE. This field is subsequently interpreted bythe OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than anASN1_STRING.When CRL checking is enabled (i.e. the application sets theX509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to passarbitrary pointers to a memcmp call, enabling them to read memory contents orenact a denial of service. In most cases, the attack requires the attacker toprovide both the certificate chain and CRL, neither of which need to have avalid signature. If the attacker only controls one of these inputs, the otherinput must already contain an X.400 address as a CRL distribution point, whichis uncommon. As such, this vulnerability is most likely to only affectapplications which have implemented their own functionality for retrieving CRLsover a network.

- Vulnerability: CVE-2023-3817

  - CVSS Score: N/A

  - Description: Issue summary: Checking excessively long DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH key or DH parameters may experience longdelays. Where the key or parameters that are being checked have been obtainedfrom an untrusted source this may lead to a Denial of Service.The function DH_check() performs various checks on DH parameters. After fixingCVE-2023-3446 it was discovered that a large q parameter value can also triggeran overly long computation during some of these checks. A correct q value,if present, cannot be larger than the modulus p parameter, thus it isunnecessary to perform these checks if q is larger than p.An application that calls DH_check() and supplies a key or parameters obtainedfrom an untrusted source could be vulnerable to a Denial of Service attack.The function DH_check() is itself called by a number of other OpenSSL functions.An application calling any of those other functions may similarly be affected.The other functions affected by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable are the OpenSSL dhparam and pkeyparam command line applicationswhen using the "-check" option.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2017-3167

  - CVSS Score: 7.5

  - Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.

- Vulnerability: CVE-2021-32786

  - CVSS Score: 5.8

- Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, `oidc_validate_redirect_url()` does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring `mod_auth_openidc` to only allow redirection whose destination matches a given regular expression.

- Vulnerability: CVE-2021-32785

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache (`OIDCCacheEncrypt off`, `OIDCSessionType server-cache`, `OIDCCacheType redis`), `mod_auth_openidc` wrongly performed argument interpolation before passing Redis requests to `hiredis`, which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the `hiredis` API. As a workaround, this vulnerability can be mitigated by setting `OIDCCacheEncrypt` to `on`, as cache keys are cryptographically hashed before use when this option is enabled.

- Vulnerability: CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2021-44790

  - CVSS Score: 7.5
  - Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

- Vulnerability: CVE-2016-4975

  - CVSS Score: 4.3
  - Description: Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).

- **Vulnerability:** CVE-2020-13938

  – CVSS Score: 2.1

  – Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

- **Vulnerability:** CVE-2023-2650

  – CVSS Score: N/A

  – Description: Issue summary: Processing some specially crafted ASN.1 object identifiers ordata containing them may be very slow.Impact summary: Applications that use OBJ_obj2txt() directly, or use any ofthe OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no messagesize limit may experience notable to very long delays when processing thosemessages, which may lead to a Denial of Service.An OBJECT IDENTIFIER is composed of a series of numbers – sub-identifiers -most of which have no size limit. OBJ_obj2txt() may be used to translatean ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSLtype ASN1_OBJECT) to its canonical numeric text form, which are thesub-identifiers of the OBJECT IDENTIFIER in decimal form, separated byperiods.When one of the sub-identifiers in the OBJECT IDENTIFIER is very large(these are sizes that are seen as absurdly large, taking up tens or hundredsof KiBs), the translation to a decimal number in text may take a very longtime. The time complexity is $O(n^2)$ with 'n' being the size of thesub-identifiers in bytes (*).With OpenSSL 3.0, support to fetch cryptographic algorithms using names /identifiers in string form was introduced. This includes using OBJECTIDENTIFIERs in canonical numeric text form as identifiers for fetchingalgorithms.Such OBJECT IDENTIFIERs may be received through the ASN.1 structureAlgorithmIdentifier, which is commonly used in multiple protocols to specifywhat cryptographic algorithm should be used to sign or verify, encrypt ordecrypt, or digest passed data.Applications that call OBJ_obj2txt() directly with untrusted data areaffected, with any version of OpenSSL. If the use is for the mere purposeof display, the severity is considered low.In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME,CMS, CMP/CRMF or TS. It also impacts anything that processes X.509certificates, including simple things like verifying its signature.The impact on TLS is relatively low, because all versions of OpenSSL have a100KiB limit on the peer's certificate chain. Additionally, this onlyimpacts clients, or servers that have explicitly enabled clientauthentication.In OpenSSL 1.1.1 and 1.0.2, this only affects displaying diverse objects,such as X.509 certificates. This is assumed to not happen in such a waythat it would cause a Denial of Service, so these versions are considerednot affected by this issue in such a way that it would be cause for concern,and the severity is therefore considered low.

- **Vulnerability:** CVE-2023-0215

  – CVSS Score: N/A

- Description: The public API function BIO_new_NDEF is a helper function used for streamingASN.1 data via a BIO. It is primarily used internally to OpenSSL to support theSMIME, CMS and PKCS7 streaming capabilities, but may also be called directly byend user applications.The function receives a BIO from the caller, prepends a new BIO_f_asn1 filterBIO onto the front of it to form a BIO chain, and then returns the new head ofthe BIO chain to the caller. Under certain conditions, for example if a CMSrecipient public key is invalid, the new filter BIO is freed and the functionreturns a NULL result indicating a failure. However, in this case, the BIO chainis not properly cleaned up and the BIO passed by the caller still retainsinternal pointers to the previously freed filter BIO. If the caller then goes onto call BIO_pop() on the BIO then a use-after-free will occur. This will mostlikely result in a crash.This scenario occurs directly in the internal function B64_write_ASN1() whichmay cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() onthe BIO. This internal function is in turn called by the public API functionsPEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream,SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7.Other public API functions that may be impacted by this includei2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream andi2d_PKCS7_bio_stream.The OpenSSL cms and smime command line applications are similarly affected.

- **Vulnerability:** CVE-2015-3183

  - CVSS Score: 5
  - Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

- **Vulnerability:** CVE-2020-35452

  - CVSS Score: 6.8
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

- **Vulnerability:** CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- **Vulnerability:** CVE-2022-31628

  - CVSS Score: N/A
  - Description: In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the phar uncompressor code would recursively uncompress "quines" gzip files, resulting in an infinite loop.

- **Vulnerability:** CVE-2022-31629

  - CVSS Score: N/A

– Description: In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the vulnerability enables network and same-site attackers to set a standard insecure cookie in the victim's browser which is treated as a '__Host-' or '__Secure-' cookie by PHP applications.

- Vulnerability: CVE-2020-1934

  – CVSS Score: 5
  – Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

- Vulnerability: CVE-2022-36760

  – CVSS Score: N/A
  – Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-4304

  – CVSS Score: N/A
  – Description: A timing based side channel exists in the OpenSSL RSA Decryption implementationwhich could be sufficient to recover a plaintext across a network in aBleichenbacher style attack. To achieve a successful decryption an attackerwould have to be able to send a very large number of trial messages fordecryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5,RSA-OEAP and RSASVE.For example, in a TLS connection, RSA is commonly used by a client to send anencrypted pre-master secret to the server. An attacker that had observed agenuine connection between a client and a server could use this flaw to sendtrial messages to the server and record the time taken to process them. After asufficiently large number of messages the attacker could recover the pre-mastersecret used for the original connection and thus be able to decrypt theapplication data sent over that connection.

- Vulnerability: CVE-2018-19396

  – CVSS Score: 5
  – Description: ext/standard/var_unserializer.c in PHP 5.x through 7.1.24 allows attackers to cause a denial of service (application crash) via an unserialize call for the com, dotnet, or variant class.

- Vulnerability: CVE-2018-19395

  – CVSS Score: 5
  – Description: ext/standard/var.c in PHP 5.x through 7.1.24 on Windows allows attackers to cause a denial of service (NULL pointer dereference and application crash) because com and com_safearray_proxy return NULL in com_properties_get in ext/com_dotnet/com_handlers.c, as demonstrated by a serialize call on COM("WScript.Shell").

- Vulnerability: CVE-2017-8923

  – CVSS Score: 7.5
  – Description: The zend_string_extend function in Zend/zend_string.h in PHP through 7.1.5 does not prevent changes to string objects that result in a negative length, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact by leveraging a script's use of .= with a long string.

- Vulnerability: CVE-2019-1563

  – CVSS Score: 4.3
  – Description: In situations where an attacker receives automated notification
    of the success or failure of a decryption attempt an attacker,
    after sending a very large number of messages to be decrypted, can
    recover a CMS/PKCS7 transported encryption key or decrypt any RSA
    encrypted message that was encrypted with the public RSA key, using a
    Bleichenbacher padding oracle attack. Applications are not affected
    if they use a certificate together with the private RSA key to the
    CMS_decrypt or PKCS7_decrypt functions to select the correct recipient
    info to decrypt. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c).
    Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL
    1.0.2t (Affected 1.0.2-1.0.2s).

- Vulnerability: CVE-2014-3523

  – CVSS Score: 5
  – Description: Memory leak in the winnt_accept function in server/mpm/winnt/child.c
    in the WinNT MPM in the Apache HTTP Server 2.4.x before 2.4.10 on
    Windows, when the default AcceptFilter is enabled, allows remote
    attackers to cause a denial of service (memory consumption) via
    crafted requests.

- Vulnerability: CVE-2013-5704

  – CVSS Score: 5
  – Description: The mod_headers module in the Apache HTTP Server 2.2.22 allows remote
    attackers to bypass "RequestHeader unset" directives by placing a
    header in the trailer portion of data sent with chunked transfer
    coding. NOTE: the vendor states "this is not a security issue in
    httpd as such."

- Vulnerability: CVE-2019-9639

  – CVSS Score: 5
  – Description: An issue was discovered in the EXIF component in PHP before
    7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is
    an uninitialized read in exif_process_IFD_in_MAKERNOTE because of
    mishandling the data_len variable.

- Vulnerability: CVE-2019-9638

  – CVSS Score: 5
  – Description: An issue was discovered in the EXIF component in PHP before
    7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is
    an uninitialized read in exif_process_IFD_in_MAKERNOTE because of
    mishandling the maker_note->offset relationship to value_len.

- Vulnerability: CVE-2019-17567

  – CVSS Score: 5
  – Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel
    configured on an URL that is not necessarily Upgraded by the origin
    server was tunneling the whole connection regardless, thus allowing
    for subsequent requests on the same connection to pass through
    with no HTTP validation, authentication or authorization possibly
    configured.

- Vulnerability: CVE-2022-31813

  – CVSS Score: 7.5

- Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

- Vulnerability: CVE-2013-2220

  - CVSS Score: 7.5
  - Description: Buffer overflow in the radius_get_vendor_attr function in the Radius extension before 1.2.7 for PHP allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a large Vendor Specific Attributes (VSA) length value.

- Vulnerability: CVE-2019-9637

  - CVSS Score: 5
  - Description: An issue was discovered in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. Due to the way rename() across filesystems is implemented, it is possible that file being renamed is briefly available with wrong permissions while the rename is ongoing, thus enabling unauthorized users to access the data.

- Vulnerability: CVE-2012-4360

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2014-0231

  - CVSS Score: 5
  - Description: The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.

- Vulnerability: CVE-2021-26690

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service

- Vulnerability: CVE-2021-26691

  - CVSS Score: 7.5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow

- Vulnerability: CVE-2019-0220

  - CVSS Score: 5
  - Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.

- Vulnerability: CVE-2017-7963

  - CVSS Score: 5

- Description: The GNU Multiple Precision Arithmetic Library (GMP) interfaces for PHP through 7.1.4 allow attackers to cause a denial of service (memory consumption and application crash) via operations on long strings. NOTE: the vendor disputes this, stating "There is no security issue here, because GMP safely aborts in case of an OOM condition. The only attack vector here is denial of service. However, if you allow attacker-controlled, unbounded allocations you have a DoS vector regardless of GMP's OOM behavior.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- Vulnerability: CVE-2021-39275

  - CVSS Score: 7.5
  - Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2014-3581

  - CVSS Score: 5
  - Description: The cache_merge_headers_out function in modules/cache/cache_util.c in the mod_cache module in the Apache HTTP Server before 2.4.11 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty HTTP Content-Type header.

- Vulnerability: CVE-2016-0736

  - CVSS Score: 5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.23, mod_session_crypto was encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This made it vulnerable to padding oracle attacks, particularly with CBC.

- Vulnerability: CVE-2022-29404

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2018-1312

  - CVSS Score: 6.8
  - Description: In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

- Vulnerability: CVE-2022-22720

  - CVSS Score: 7.5

- Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2007-3205

  - CVSS Score: 5
  - Description: The parse_str function in (1) PHP, (2) Hardened-PHP, and (3) Suhosin, when called without a second parameter, might allow remote attackers to overwrite arbitrary variables by specifying variable names and values in the string to be parsed. NOTE: it is not clear whether this is a design limitation of the function or a bug in PHP, although it is likely to be regarded as a bug in Hardened-PHP and Suhosin.

- Vulnerability: CVE-2017-15710

  - CVSS Score: 5
  - Description: In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.

- Vulnerability: CVE-2014-0226

  - CVSS Score: 6.8
  - Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

- Vulnerability: CVE-2022-2068

  - CVSS Score: 10
  - Description: In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze).

- Vulnerability: CVE-2009-3766

- CVSS Score: 6.8
- Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when OpenSSL is used, does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

- Vulnerability: CVE-2009-3767

  - CVSS Score: 4.3
  - Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other versions, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2009-3765

  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2022-22721

  - CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2006-20001

  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2019-10092

  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

- Vulnerability: CVE-2021-3712

  - CVSS Score: 5.8

– Description: ASN.1 strings are represented internally within OpenSSL as an ASN1 STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own "d2i" functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1 STRING set() function will additionally NUL terminate the byte array in the ASN1 STRING structure. However, it is possible for applications to directly construct valid ASN1 STRING structures which do not NUL terminate the byte array by directly setting the "data" and "length" fields in the ASN1 STRING array. This can also happen by using the ASN1 STRING set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1 STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1 STRINGs that have been directly constructed by the application without NUL terminating the "data" field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1 STRING structures). It can also occur in the X509 get1 email(), X509 REQ get1 email() and X509 get1 ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1 STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y).

- Vulnerability: CVE-2023-0464

  – CVSS Score: N/A

  – Description: A security vulnerability has been identified in all supported versionsof OpenSSL related to the verification of X.509 certificate chainsthat include policy constraints. Attackers may be able to exploit thisvulnerability by creating a malicious certificate chain that triggersexponential use of computational resources, leading to a denial-of-service(DoS) attack on affected systems.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509 VERIFY PARAM set1 policies()' function.

- Vulnerability: CVE-2023-0465

  – CVSS Score: N/A

- Description: Applications that use a non-default option when verifying
                certificates may bevulnerable to an attack from a malicious CA
                to circumvent certain checks.Invalid certificate policies in leaf
                certificates are silently ignored byOpenSSL and other certificate
                policy checks are skipped for that certificate.A malicious CA could
                use this to deliberately assert invalid certificate policiesin order
                to circumvent policy checking on the certificate altogether.Policy
                processing is disabled by default but can be enabled by passingthe
                '-policy' argument to the command line utilities or by calling
                the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0466

  - CVSS Score: N/A

  - Description: The function X509_VERIFY_PARAM_add0_policy() is documented
                  toimplicitly enable the certificate policy check when doing
                  certificateverification. However the implementation of the
                  function does notenable the check which allows certificates
                  with invalid or incorrectpolicies to pass the certificate
                  verification.As suddenly enabling the policy check could break
                  existing deployments it wasdecided to keep the existing behavior of
                  the X509_VERIFY_PARAM_add0_policy()function.Instead the applications
                  that require OpenSSL to perform certificatepolicy check need
                  to use X509_VERIFY_PARAM_set1_policies() or explicitlyenable the
                  policy check by calling X509_VERIFY_PARAM_set_flags() withthe
                  X509_V_FLAG_POLICY_CHECK flag argument.Certificate policy checks
                  are disabled by default in OpenSSL and are notcommonly used by
                  applications.

- Vulnerability: CVE-2015-9253

  - CVSS Score: 6.8

  - Description: An issue was discovered in PHP 7.3.x before 7.3.0alpha3, 7.2.x before
                  7.2.8, and before 7.1.20. The php-fpm master process restarts
                  a child process in an endless loop when using program execution
                  functions (e.g., passthru, exec, shell_exec, or system) with a
                  non-blocking STDIN stream, causing this master process to consume
                  100% of the CPU, and consume disk space with a large volume of error
                  logs, as demonstrated by an attack by a customer of a shared-hosting
                  facility.

- Vulnerability: CVE-2015-0228

  - CVSS Score: 5

  - Description: The lua_websocket_read function in lua_request.c in the mod_lua module
                  in the Apache HTTP Server through 2.4.12 allows remote attackers to
                  cause a denial of service (child-process crash) by sending a crafted
                  WebSocket Ping frame after a Lua script has called the wsupgrade
                  function.

- Vulnerability: CVE-2016-5387

  - CVSS Score: 6.8

  - Description: The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18
                  and therefore does not protect applications from the presence of
                  untrusted client data in the HTTP_PROXY environment variable, which
                  might allow remote attackers to redirect an application's outbound
                  HTTP traffic to an arbitrary proxy server via a crafted Proxy header
                  in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states
                  "This mitigation has been assigned the identifier CVE-2016-5387"; in
                  other words, this is not a CVE ID for a vulnerability.

- Vulnerability: CVE-2017-15715

  – CVSS Score: 6.8
  – Description: In Apache httpd 2.4.0 to 2.4.29, the expression specified in
    <FilesMatch> could match '$' to a newline character in a malicious
    filename, rather than matching only the end of the filename. This
    could be exploited in environments where uploads of some files are
    are externally blocked, but only by matching the trailing portion of
    the filename.

- Vulnerability: CVE-2021-40438

  – CVSS Score: 6.8
  – Description: A crafted request uri-path can cause mod_proxy to forward the request
    to an origin server choosen by the remote user. This issue affects
    Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2011-1176

  – CVSS Score: 4.3
  – Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk
    Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP
    Server does not properly handle certain configuration sections that
    specify NiceValue but not AssignUserID, which might allow remote
    attackers to gain privileges by leveraging the root uid and root gid
    of an mpm-itk process.

- Vulnerability: CVE-2022-23943

  – CVSS Score: 7.5
  – Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server
    allows an attacker to overwrite heap memory with possibly attacker
    provided data. This issue affects Apache HTTP Server 2.4 version
    2.4.52 and prior versions.

- Vulnerability: CVE-2021-23840

  – CVSS Score: 5
  – Description: Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate
    may overflow the output length argument in some cases where the input
    length is close to the maximum permissable length for an integer on
    the platform. In such cases the return value from the function call
    will be 1 (indicating success), but the output length value will be
    negative. This could cause applications to behave incorrectly or
    crash. OpenSSL versions 1.1.1i and below are affected by this issue.
    Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL
    versions 1.0.2x and below are affected by this issue. However
    OpenSSL 1.0.2 is out of support and no longer receiving public
    updates. Premium support customers of OpenSSL 1.0.2 should upgrade
    to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL
    1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected
    1.0.2-1.0.2x).

- Vulnerability: CVE-2021-23841

  – CVSS Score: 4.3

– Description: The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack. The function X509_issuer_and_serial_hash() is never directly called by OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on certificates that may have been obtained from untrusted sources. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2018-1301

  – CVSS Score: 4.3
  – Description: A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.

- Vulnerability: CVE-2018-1302

  – CVSS Score: 4.3
  – Description: When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.

- Vulnerability: CVE-2020-1968

  – CVSS Score: 4.3
  – Description: The Raccoon attack exploits a flaw in the TLS specification which can lead to an attacker being able to compute the pre-master secret in connections which have used a Diffie-Hellman (DH) based ciphersuite. In such a case this would result in the attacker being able to eavesdrop on all encrypted communications sent over that TLS connection. The attack can only be exploited if an implementation re-uses a DH secret across multiple TLS connections. Note that this issue only impacts DH ciphersuites and not ECDH ciphersuites. This issue affects OpenSSL 1.0.2 which is out of support and no longer receiving public updates. OpenSSL 1.1.1 is not vulnerable to this issue. Fixed in OpenSSL 1.0.2w (Affected 1.0.2-1.0.2v).

- Vulnerability: CVE-2021-34798

  – CVSS Score: 5
  – Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2023-25690

- CVSS Score: N/A
- Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2019-10098

  - CVSS Score: 5.8
  - Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.

- Vulnerability: CVE-2020-11985

  - CVSS Score: 4.3
  - Description: IP address spoofing when proxying using mod_remoteip and mod_rewrite For configurations using proxying with mod_remoteip and certain mod_rewrite rules, an attacker could spoof their IP address for logging and PHP scripts. Note this issue was fixed in Apache HTTP Server 2.4.24 but was retrospectively allocated a low severity CVE in 2020.

- Vulnerability: CVE-2021-4160

  - CVSS Score: 4.3
  - Description: There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that is available to premium support customers only. It will be made available in 1.0.2zc when it is released. The issue only affects OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0). Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL 1.0.2zc-dev (Affected 1.0.2-1.0.2zb).

- Vulnerability: CVE-2013-4352

  - CVSS Score: 4.3

- Description: The cache_invalidate function in modules/cache/cache_storage.c in the mod_cache module in the Apache HTTP Server 2.4.6, when a caching forward proxy is enabled, allows remote HTTP servers to cause a denial of service (NULL pointer dereference and daemon crash) via vectors that trigger a missing hostname value.

- **Vulnerability:** CVE-2022-26377

  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- **Vulnerability:** CVE-2014-0098

  - CVSS Score: 5
  - Description: The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.

- **Vulnerability:** CVE-2019-9641

  - CVSS Score: 7.5
  - Description: An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_TIFF.

- **Vulnerability:** CVE-2016-8743

  - CVSS Score: 5
  - Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

- **Vulnerability:** CVE-2024-40898

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- **Vulnerability:** CVE-2024-38474

  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- **Vulnerability:** CVE-2022-0778

  - CVSS Score: 5

– Description: The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - TLS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

- Vulnerability: CVE-2020-1971

  – CVSS Score: 4.3

— Description: The X.509 GeneralName type is a generic type for representing
different types of names. One of those name types is known as
EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which
compares different instances of a GENERAL_NAME to see if they
are equal or not. This function behaves incorrectly when both
GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference
and a crash may occur leading to a possible denial of service
attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two
purposes: 1) Comparing CRL distribution point names between an
available CRL and a CRL distribution point embedded in an X509
certificate 2) When verifying that a timestamp response token signer
matches the timestamp authority name (exposed via the API functions
TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can
control both items being compared then that attacker could trigger
a crash. For example if the attacker can trick a client or server
into checking a malicious certificate against a malicious CRL then
this may occur. Note that some applications automatically download
CRLs based on a URL embedded in a certificate. This checking happens
prior to the signatures on the certificate and CRL being verified.
OpenSSL's s_server, s_client and verify tools have support for the
"-crl_download" option which implements automatic CRL downloading and
this attack has been demonstrated to work against those tools. Note
that an unrelated bug means that affected versions of OpenSSL cannot
parse or construct correct encodings of EDIPARTYNAME. However it is
possible to construct a malformed EDIPARTYNAME that OpenSSL's parser
will accept and hence trigger this attack. All OpenSSL 1.1.1 and
1.0.2 versions are affected by this issue. Other OpenSSL releases
are out of support and have not been checked. Fixed in OpenSSL
1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected
1.0.2-1.0.2w).

- Vulnerability: CVE-2009-1390

  — CVSS Score: 6.8

  — Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2)
GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS
certificate in the chain is accepted instead of verifying the entire
chain, which allows remote attackers to spoof trusted servers via a
man-in-the-middle attack.

- Vulnerability: CVE-2012-3526

  — CVSS Score: 5

  — Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the
Apache HTTP Server allows remote attackers to cause a denial of
service (server or application crash) via multiple X-Forwarded-For
headers in a request.

- Vulnerability: CVE-2023-5678

  — CVSS Score: N/A

- Description: Issue summary: Generating excessively long X9.42 DH keys or checkingexcessively long X9.42 DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_generate_key() togenerate an X9.42 DH key may experience long delays. Likewise, applicationsthat use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check()to check an X9.42 DH key or X9.42 DH parameters may experience long delays.Where the key or parameters that are being checked have been obtained froman untrusted source this may lead to a Denial of Service.While DH_check() performs all the necessary checks (as of CVE-2023-3817),DH_check_pub_key() doesn't make any of these checks, and is thereforevulnerable for excessively large P and Q parameters.Likewise, while DH_generate_key() performs a check for an excessively largeP, it doesn't check for an excessively large Q.An application that calls DH_generate_key() or DH_check_pub_key() andsupplies a key or parameters obtained from an untrusted source could bevulnerable to a Denial of Service attack.DH_generate_key() and DH_check_pub_key() are also called by a number ofother OpenSSL functions. An application calling any of those otherfunctions may similarly be affected. The other functions affected by thisare DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate().Also vulnerable are the OpenSSL pkey command line application when using the"-pubcheck" option, as well as the OpenSSL genpkey command line application.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2017-3736

  - CVSS Score: 4

  - Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

- Vulnerability: CVE-2017-3737

  - CVSS Score: 4.3

- Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

- **Vulnerability:** CVE-2019-1547

  - CVSS Score: 1.9

  - Description: Normally in OpenSSL EC groups always have a co-factor present and this is used in side channel resistant code paths. However, in some cases, it is possible to construct a group using explicit parameters (instead of using a named curve). In those cases it is possible that such a group does not have the cofactor present. This can occur even where all the parameters match a known named curve. If such a curve is used then OpenSSL falls back to non-side channel resistant code paths which may result in full key recovery during an ECDSA signature operation. In order to be vulnerable an attacker would have to have the ability to time the creation of a large number of signatures where explicit parameters with no co-factor present are in use by an application using libcrypto. For the avoidance of doubt libssl is not vulnerable because explicit parameters are never used. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).

- **Vulnerability:** CVE-2017-3735

  - CVSS Score: 5

  - Description: While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL before 1.0.2m and 1.1.0g.

- **Vulnerability:** CVE-2009-2299

  - CVSS Score: 5

  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- **Vulnerability:** CVE-2022-1292

  - CVSS Score: 10

- Description: The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n). Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).

- Vulnerability: CVE-2017-3738

  - CVSS Score: 4.3
  - Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

- Vulnerability: CVE-2020-11579

  - CVSS Score: 5
  - Description: An issue was discovered in Chadha PHPKB 9.0 Enterprise Edition. installer/test-connection.php (part of the installation process) allows a remote unauthenticated attacker to disclose local files on hosts running PHP before 7.2.16, or on hosts where the MySQL ALLOW LOCAL DATA INFILE option is enabled.

- Vulnerability: CVE-2012-4001

  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2022-37436

  - CVSS Score: N/A
  - Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2018-17199

  - CVSS Score: 5

- Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

- Vulnerability: CVE-2018-0737

  - CVSS Score: 4.3
  - Description: The OpenSSL RSA Key generation algorithm has been shown to be vulnerable to a cache timing side channel attack. An attacker with sufficient access to mount cache timing attacks during the RSA key generation process could recover the private key. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2b-1.0.2o).

- Vulnerability: CVE-2018-0734

  - CVSS Score: 4.3
  - Description: The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.1a (Affected 1.1.1). Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.0.2q (Affected 1.0.2-1.0.2p).

- Vulnerability: CVE-2018-0732

  - CVSS Score: 5
  - Description: During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime value to the client. This will cause the client to spend an unreasonably long period of time generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2-1.0.2o).

- Vulnerability: CVE-2017-9788

  - CVSS Score: 6.4
  - Description: In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.

- Vulnerability: CVE-2018-0739

  - CVSS Score: 4.3
  - Description: Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o (Affected 1.0.2b-1.0.2n).

- Vulnerability: CVE-2014-8109

  - CVSS Score: 4.3

– Description: mod_lua.c in the mod_lua module in the Apache HTTP Server 2.3.x and 2.4.x through 2.4.10 does not support an httpd configuration in which the same Lua authorization provider is used with different arguments within different contexts, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives, as demonstrated by a configuration that specifies authorization for one group to access a certain directory, and authorization for a second group to access a second directory.

- Vulnerability: CVE-2013-2765

  – CVSS Score: 5

  – Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2011-2688

  – CVSS Score: 7.5

  – Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2016-2161

  – CVSS Score: 5

  – Description: In Apache HTTP Server versions 2.4.0 to 2.4.23, malicious input to mod_auth_digest can cause the server to crash, and each instance continues to crash even for subsequently valid requests.

- Vulnerability: CVE-2016-8612

  – CVSS Score: 3.3

  – Description: Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.

- Vulnerability: CVE-2019-1552

  – CVSS Score: 1.9

- Description: OpenSSL has internal defaults for a directory tree where it
               can find a configuration file as well as certificates used for
               verification in TLS. This directory is most commonly referred to
               as OPENSSLDIR, and is configurable with the --prefix / --openssldir
               configuration options. For OpenSSL versions 1.1.0 and 1.1.1, the
               mingw configuration targets assume that resulting programs and
               libraries are installed in a Unix-like environment and the default
               prefix for program installation as well as for OPENSSLDIR should be
               '/usr/local'. However, mingw programs are Windows programs, and as
               such, find themselves looking at sub-directories of 'C:/usr/local',
               which may be world writable, which enables untrusted users to modify
               OpenSSL's default configuration, insert CA certificates, modify (or
               even replace) existing engine modules, etc. For OpenSSL 1.0.2,
               '/usr/local/ssl' is used as default for OPENSSLDIR on all Unix and
               Windows targets, including Visual C builds. However, some build
               instructions for the diverse Windows targets on 1.0.2 encourage
               you to specify your own --prefix. OpenSSL versions 1.1.1, 1.1.0
               and 1.0.2 are affected by this issue. Due to the limited scope
               of affected deployments this has been assessed as low severity and
               therefore we are not creating new releases at this time. Fixed
               in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL
               1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected
               1.0.2-1.0.2s).

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5
                 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM
                 Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows
                 use an improper encryption algorithm and a weak key for maintaining
                 the stored data of the node secret for the SecurID Authentication
                 API, which allows local users to obtain sensitive information via
                 cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication
                 Agent 7.1 before 7.1.1 for Web for Internet Information Services,
                 and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to
                 inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2019-1551

  - CVSS Score: 5
  - Description: There is an overflow bug in the x64_64 Montgomery squaring procedure
                 used in exponentiation with 512-bit moduli. No EC algorithms are
                 affected. Analysis suggests that attacks against 2-prime RSA1024,
                 3-prime RSA1536, and DSA1024 as a result of this defect would be
                 very difficult to perform and are not believed likely. Attacks
                 against DH512 are considered just feasible. However, for an attack
                 the target would have to re-use the DH512 private key, which is not
                 recommended anyway. Also applications directly using the low level
                 API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME. Fixed
                 in OpenSSL 1.1.1e (Affected 1.1.1-1.1.1d). Fixed in OpenSSL 1.0.2u
                 (Affected 1.0.2-1.0.2t).

- Vulnerability: CVE-2019-1559

  - CVSS Score: 4.3

- Description: If an application encounters a fatal protocol error and then calls
  SSL_shutdown() twice (once to send a close_notify, and once to
  receive one) then OpenSSL can respond differently to the calling
  application if a 0 byte record is received with invalid padding
  compared to if a 0 byte record is received with an invalid MAC. If
  the application then behaves differently based on that in a way that
  is detectable to the remote peer, then this amounts to a padding
  oracle that could be used to decrypt data. In order for this to be
  exploitable "non-stitched" ciphersuites must be in use. Stitched
  ciphersuites are optimised implementations of certain commonly
  used ciphersuites. Also the application must call SSL_shutdown()
  twice even if a protocol error has occurred (applications should
  not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected
  1.0.2-1.0.2q).

- Vulnerability: CVE-2023-45802

  - CVSS Score: N/A

  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a
    time window were the request's memory resources were not reclaimed
    immediately. Instead, de-allocation was deferred to connection
    close. A client could send new requests and resets, keeping the
    connection busy and open and causing the memory footprint to keep
    on growing. On connection close, all resources were reclaimed, but
    the process might run out of memory before that.This was found by
    the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset
    Exploit) with their own test client. During "normal" HTTP/2 use, the
    probability to hit this bug is very low. The kept memory would not
    become noticeable before the connection closes or times out.Users are
    recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2018-1283

  - CVSS Score: 3.5

  - Description: In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to
    forward its session data to CGI applications (SessionEnv on, not
    the default), a remote user may influence their content by using a
    "Session" header. This comes from the "HTTP_SESSION" variable name
    used by mod_session to forward its data to CGIs, since the prefix
    "HTTP_" is also used by the Apache HTTP Server to pass HTTP header
    fields, per CGI specifications.

- Vulnerability: CVE-2018-1303

  - CVSS Score: 5

  - Description: A specially crafted HTTP request header could have crashed the Apache
    HTTP Server prior to version 2.4.30 due to an out of bound read while
    preparing data to be cached in shared memory. It could be used as
    a Denial of Service attack against users of mod_cache_socache. The
    vulnerability is considered as low risk since mod_cache_socache is not
    widely used, mod_cache_disk is not concerned by this vulnerability.

- Vulnerability: CVE-2019-0217

  - CVSS Score: 6

  - Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition
    in mod_auth_digest when running in a threaded server could allow a
    user with valid credentials to authenticate using another username,
    bypassing configured access control restrictions.

- Vulnerability: CVE-2022-28615

- CVSS Score: 6.4
- Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- **Vulnerability: CVE-2022-28614**

  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

- **Vulnerability: CVE-2014-0117**

  - CVSS Score: 4.3
  - Description: The mod_proxy module in the Apache HTTP Server 2.4.x before 2.4.10, when a reverse proxy is enabled, allows remote attackers to cause a denial of service (child-process crash) via a crafted HTTP Connection header.

- **Vulnerability: CVE-2017-7679**

  - CVSS Score: 7.5
  - Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

- **Vulnerability: CVE-2017-7272**

  - CVSS Score: 5.8
  - Description: PHP through 7.1.11 enables potential SSRF in applications that accept an fsockopen or pfsockopen hostname argument with an expectation that the port number is constrained. Because a :port syntax is recognized, fsockopen will use the port number that is specified in the hostname argument, instead of the port number in the second argument of the function.

- **Vulnerability: CVE-2017-9798**

  - CVSS Score: 5
  - Description: Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.

- **Vulnerability: CVE-2015-3185**

  - CVSS Score: 4.3

- Description: The ap_some_auth_required function in server/request.c in the Apache
  HTTP Server 2.4.x before 2.4.14 does not consider that a Require
  directive may be associated with an authorization setting rather
  than an authentication setting, which allows remote attackers to
  bypass intended access restrictions in opportunistic circumstances
  by leveraging the presence of a module that relies on the 2.2 API
  behavior.

- Vulnerability: CVE-2015-3184

  - CVSS Score: 5
  - Description: mod_authz_svn in Apache Subversion 1.7.x before 1.7.21 and 1.8.x
    before 1.8.14, when using Apache httpd 2.4.x, does not properly
    restrict anonymous access, which allows remote anonymous users to
    read hidden files via the path name.

- Vulnerability: CVE-2024-4577

  - CVSS Score: N/A
  - Description: In PHP versions8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before
    8.3.8, when using Apache and PHP-CGI on Windows, if the system is set
    up to use certain code pages, Windows may use "Best-Fit" behavior to
    replace characters in command line given toWin32 API functions. PHP
    CGI module may misinterpret those characters as PHP options, which
    may allow a malicious user to pass options to PHP binary being run,
    and thus reveal the source code of scripts, run arbitrary PHP code on
    the server, etc.

- Vulnerability: CVE-2013-4365

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function
    in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache
    HTTP Server allows remote attackers to have an unspecified impact via
    unknown vectors.

- Vulnerability: CVE-2018-5407

  - CVSS Score: 1.9
  - Description: Simultaneous Multi-threading (SMT) in processors can enable local
    users to exploit software vulnerable to timing attacks via a
    side-channel timing attack on 'port contention'.

- Vulnerability: CVE-2022-28330

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond
    bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2021-32791

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the
    Apache 2.x HTTP server that functions as an OpenID Connect Relying
    Party, authenticating users against an OpenID Connect Provider.
    In mod_auth_openidc before version 2.4.9, the AES GCM encryption in
    mod_auth_openidc uses a static IV and AAD. It is important to fix
    because this creates a static nonce and since aes-gcm is a stream
    cipher, this can lead to known cryptographic issues, since the same
    key is being reused. From 2.4.9 onwards this has been patched to use
    dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2021-32792

- CVSS Score: 4.3
- Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.

- **Vulnerability:** CVE-2024-38476

  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- **Vulnerability:** CVE-2024-38477

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- **Vulnerability:** CVE-2023-31122

  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- **Vulnerability:** CVE-2009-0796

  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- **Vulnerability:** CVE-2024-0727

  - CVSS Score: N/A
  - Description: Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSLto crash leading to a potential Denial of Service attackImpact summary: Applications loading files in the PKCS12 format from untrustedsources might terminate abruptly.A file in PKCS12 format can contain certificates and keys and may come from anuntrusted source. The PKCS12 specification allows certain fields to be NULL, butOpenSSL does not correctly check for this case. This can lead to a NULL pointerdereference that results in OpenSSL crashing. If an application processes PKCS12files from an untrusted source using the OpenSSL APIs then that application willbe vulnerable to this issue.OpenSSL APIs that are vulnerable to this are: PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a similar issue in SMIME_write_PKCS7(). However since thisfunction is related to writing data we do not consider it security significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.

- **Vulnerability:** CVE-2014-0118

  - CVSS Score: 4.3

- – Description: The deflate_in_filter function in mod_deflate.c in the mod_deflate module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.

- Vulnerability: CVE-2013-6438

  - – CVSS Score: 5
  - – Description: The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.

- Vulnerability: CVE-2020-1927

  - – CVSS Score: 5.8
  - – Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.

- Vulnerability: CVE-2023-0286

  - – CVSS Score: N/A
  - – Description: There is a type confusion vulnerability relating to X.400 address processinginside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING butthe public structure definition for GENERAL_NAME incorrectly specified the typeof the x400Address field as ASN1_TYPE. This field is subsequently interpreted bythe OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than anASN1_STRING.When CRL checking is enabled (i.e. the application sets theX509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to passarbitrary pointers to a memcmp call, enabling them to read memory contents orenact a denial of service. In most cases, the attack requires the attacker toprovide both the certificate chain and CRL, neither of which need to have avalid signature. If the attacker only controls one of these inputs, the otherinput must already contain an X.400 address as a CRL distribution point, whichis uncommon. As such, this vulnerability is most likely to only affectapplications which have implemented their own functionality for retrieving CRLsover a network.

- Vulnerability: CVE-2023-3817

  - – CVSS Score: N/A

- Description: Issue summary: Checking excessively long DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH key or DH parameters may experience longdelays. Where the key or parameters that are being checked have been obtainedfrom an untrusted source this may lead to a Denial of Service.The function DH_check() performs various checks on DH parameters. After fixingCVE-2023-3446 it was discovered that a large q parameter value can also triggeran overly long computation during some of these checks. A correct q value,if present, cannot be larger than the modulus p parameter, thus it isunnecessary to perform these checks if q is larger than p.An application that calls DH_check() and supplies a key or parameters obtainedfrom an untrusted source could be vulnerable to a Denial of Service attack.The function DH_check() is itself called by a number of other OpenSSL functions.An application calling any of those other functions may similarly be affected.The other functions affected by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable are the OpenSSL dhparam and pkeyparam command line applicationswhen using the "-check" option.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2017-3167

  - CVSS Score: 7.5

  - Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.

- Vulnerability: CVE-2021-32786

  - CVSS Score: 5.8

  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, 'oidc_validate_redirect_url()' does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring 'mod_auth_openidc' to only allow redirection whose destination matches a given regular expression.

- Vulnerability: CVE-2021-32785

  - CVSS Score: 4.3

– Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache (`OIDCCacheEncrypt off`, `OIDCSessionType server-cache`, `OIDCCacheType redis`), `mod_auth_openidc` wrongly performed argument interpolation before passing Redis requests to `hiredis`, which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the `hiredis` API. As a workaround, this vulnerability can be mitigated by setting `OIDCCacheEncrypt` to `on`, as cache keys are cryptographically hashed before use when this option is enabled.

- Vulnerability: CVE-2007-4723

  – CVSS Score: 7.5

  – Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2021-44790

  – CVSS Score: 7.5

  – Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

- Vulnerability: CVE-2016-4975

  – CVSS Score: 4.3

  – Description: Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).

- Vulnerability: CVE-2020-13938

  – CVSS Score: 2.1

  – Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

- Vulnerability: CVE-2023-2650

  – CVSS Score: N/A

- Description: Issue summary: Processing some specially crafted ASN.1 object identifiers ordata containing them may be very slow.Impact summary: Applications that use OBJ_obj2txt() directly, or use any ofthe OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no messagesize limit may experience notable to very long delays when processing thosemessages, which may lead to a Denial of Service.An OBJECT IDENTIFIER is composed of a series of numbers - sub-identifiers -most of which have no size limit. OBJ_obj2txt() may be used to translatean ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSLtype ASN1_OBJECT) to its canonical numeric text form, which are thesub-identifiers of the OBJECT IDENTIFIER in decimal form, separated byperiods.When one of the sub-identifiers in the OBJECT IDENTIFIER is very large(these are sizes that are seen as absurdly large, taking up tens or hundredsof KiBs), the translation to a decimal number in text may take a very longtime. The time complexity is $O(n^2)$ with 'n' being the size of thesub-identifiers in bytes (*).With OpenSSL 3.0, support to fetch cryptographic algorithms using names /identifiers in string form was introduced. This includes using OBJECTIDENTIFIERs in canonical numeric text form as identifiers for fetchingalgorithms.Such OBJECT IDENTIFIERs may be received through the ASN.1 structureAlgorithmIdentifier, which is commonly used in multiple protocols to specifywhat cryptographic algorithm should be used to sign or verify, encrypt ordecrypt, or digest passed data.Applications that call OBJ_obj2txt() directly with untrusted data areaffected, with any version of OpenSSL. If the use is for the mere purposeof display, the severity is considered low.In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME,CMS, CMP/CRMF or TS. It also impacts anything that processes X.509certificates, including simple things like verifying its signature.The impact on TLS is relatively low, because all versions of OpenSSL have a100KiB limit on the peer's certificate chain. Additionally, this onlyimpacts clients, or servers that have explicitly enabled clientauthentication.In OpenSSL 1.1.1 and 1.0.2, this only affects displaying diverse objects,such as X.509 certificates. This is assumed to not happen in such a waythat it would cause a Denial of Service, so these versions are considerednot affected by this issue in such a way that it would be cause for concern,and the severity is therefore considered low.
- Vulnerability: CVE-2023-0215
  - CVSS Score: N/A

- Description: The public API function BIO_new_NDEF is a helper function used for streamingASN.1 data via a BIO. It is primarily used internally to OpenSSL to support theSMIME, CMS and PKCS7 streaming capabilities, but may also be called directly byend user applications.The function receives a BIO from the caller, prepends a new BIO_f_asn1 filterBIO onto the front of it to form a BIO chain, and then returns the new head ofthe BIO chain to the caller. Under certain conditions, for example if a CMSrecipient public key is invalid, the new filter BIO is freed and the functionreturns a NULL result indicating a failure. However, in this case, the BIO chainis not properly cleaned up and the BIO passed by the caller still retainsinternal pointers to the previously freed filter BIO. If the caller then goes onto call BIO_pop() on the BIO then a use-after-free will occur. This will mostlikely result in a crash.This scenario occurs directly in the internal function B64_write_ASN1() whichmay cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() onthe BIO. This internal function is in turn called by the public API functionsPEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream,SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7.Other public API functions that may be impacted by this includei2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream andi2d_PKCS7_bio_stream.The OpenSSL cms and smime command line applications are similarly affected.

- Vulnerability: CVE-2015-3183

  - CVSS Score: 5
  - Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

- Vulnerability: CVE-2020-35452

  - CVSS Score: 6.8
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

- Vulnerability: CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2022-31628

  - CVSS Score: N/A
  - Description: In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the phar uncompressor code would recursively uncompress "quines" gzip files, resulting in an infinite loop.

- Vulnerability: CVE-2022-31629

  - CVSS Score: N/A

- Description: In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the vulnerability enables network and same-site attackers to set a standard insecure cookie in the victim's browser which is treated as a '__Host-' or '__Secure-' cookie by PHP applications.

- Vulnerability: CVE-2020-1934

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

- Vulnerability: CVE-2022-36760

  - CVSS Score: N/A
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-4304

  - CVSS Score: N/A
  - Description: A timing based side channel exists in the OpenSSL RSA Decryption implementationwhich could be sufficient to recover a plaintext across a network in aBleichenbacher style attack. To achieve a successful decryption an attackerwould have to be able to send a very large number of trial messages fordecryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5,RSA-OEAP and RSASVE.For example, in a TLS connection, RSA is commonly used by a client to send anencrypted pre-master secret to the server. An attacker that had observed agenuine connection between a client and a server could use this flaw to sendtrial messages to the server and record the time taken to process them. After asufficiently large number of messages the attacker could recover the pre-mastersecret used for the original connection and thus be able to decrypt theapplication data sent over that connection.

- Vulnerability: CVE-2018-19396

  - CVSS Score: 5
  - Description: ext/standard/var_unserializer.c in PHP 5.x through 7.1.24 allows attackers to cause a denial of service (application crash) via an unserialize call for the com, dotnet, or variant class.

- Vulnerability: CVE-2018-19395

  - CVSS Score: 5
  - Description: ext/standard/var.c in PHP 5.x through 7.1.24 on Windows allows attackers to cause a denial of service (NULL pointer dereference and application crash) because com and com_safearray_proxy return NULL in com_properties_get in ext/com_dotnet/com_handlers.c, as demonstrated by a serialize call on COM("WScript.Shell").

- Vulnerability: CVE-2017-8923

  - CVSS Score: 7.5
  - Description: The zend_string_extend function in Zend/zend_string.h in PHP through 7.1.5 does not prevent changes to string objects that result in a negative length, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact by leveraging a script's use of .= with a long string.

- Vulnerability: CVE-2019-1563

  – CVSS Score: 4.3

  – Description: In situations where an attacker receives automated notification
                 of the success or failure of a decryption attempt an attacker,
                 after sending a very large number of messages to be decrypted, can
                 recover a CMS/PKCS7 transported encryption key or decrypt any RSA
                 encrypted message that was encrypted with the public RSA key, using a
                 Bleichenbacher padding oracle attack. Applications are not affected
                 if they use a certificate together with the private RSA key to the
                 CMS_decrypt or PKCS7_decrypt functions to select the correct recipient
                 info to decrypt. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c).
                 Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL
                 1.0.2t (Affected 1.0.2-1.0.2s).

- Vulnerability: CVE-2014-3523

  – CVSS Score: 5

  – Description: Memory leak in the winnt_accept function in server/mpm/winnt/child.c
                 in the WinNT MPM in the Apache HTTP Server 2.4.x before 2.4.10 on
                 Windows, when the default AcceptFilter is enabled, allows remote
                 attackers to cause a denial of service (memory consumption) via
                 crafted requests.

- Vulnerability: CVE-2013-5704

  – CVSS Score: 5

  – Description: The mod_headers module in the Apache HTTP Server 2.2.22 allows remote
                 attackers to bypass "RequestHeader unset" directives by placing a
                 header in the trailer portion of data sent with chunked transfer
                 coding. NOTE: the vendor states "this is not a security issue in
                 httpd as such."

- Vulnerability: CVE-2019-9639

  – CVSS Score: 5

  – Description: An issue was discovered in the EXIF component in PHP before
                 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is
                 an uninitialized read in exif_process_IFD_in_MAKERNOTE because of
                 mishandling the data_len variable.

- Vulnerability: CVE-2019-9638

  – CVSS Score: 5

  – Description: An issue was discovered in the EXIF component in PHP before
                 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is
                 an uninitialized read in exif_process_IFD_in_MAKERNOTE because of
                 mishandling the maker_note->offset relationship to value_len.

- Vulnerability: CVE-2019-17567

  – CVSS Score: 5

  – Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel
                 configured on an URL that is not necessarily Upgraded by the origin
                 server was tunneling the whole connection regardless, thus allowing
                 for subsequent requests on the same connection to pass through
                 with no HTTP validation, authentication or authorization possibly
                 configured.

- Vulnerability: CVE-2022-31813

  – CVSS Score: 7.5

– Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-*
headers to the origin server based on client side Connection
header hop-by-hop mechanism. This may be used to bypass IP based
authentication on the origin server/application.

- Vulnerability: CVE-2013-2220

  – CVSS Score: 7.5
  – Description: Buffer overflow in the radius_get_vendor_attr function in the Radius
extension before 1.2.7 for PHP allows remote attackers to cause a
denial of service (crash) and possibly execute arbitrary code via a
large Vendor Specific Attributes (VSA) length value.

- Vulnerability: CVE-2019-9637

  – CVSS Score: 5
  – Description: An issue was discovered in PHP before 7.1.27, 7.2.x before 7.2.16,
and 7.3.x before 7.3.3. Due to the way rename() across filesystems
is implemented, it is possible that file being renamed is briefly
available with wrong permissions while the rename is ongoing, thus
enabling unauthorized users to access the data.

- Vulnerability: CVE-2012-4360

  – CVSS Score: 4.3
  – Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module
0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote
attackers to inject arbitrary web script or HTML via unspecified
vectors.

- Vulnerability: CVE-2014-0231

  – CVSS Score: 5
  – Description: The mod_cgid module in the Apache HTTP Server before 2.4.10 does not
have a timeout mechanism, which allows remote attackers to cause a
denial of service (process hang) via a request to a CGI script that
does not read from its stdin file descriptor.

- Vulnerability: CVE-2021-26690

  – CVSS Score: 5
  – Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted
Cookie header handled by mod_session can cause a NULL pointer
dereference and crash, leading to a possible Denial Of Service

- Vulnerability: CVE-2021-26691

  – CVSS Score: 7.5
  – Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted
SessionHeader sent by an origin server could cause a heap overflow

- Vulnerability: CVE-2019-0220

  – CVSS Score: 5
  – Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38.
When the path component of a request URL contains multiple
consecutive slashes ('/'), directives such as LocationMatch and
RewriteRule must account for duplicates in regular expressions while
other aspects of the servers processing will implicitly collapse
them.

- Vulnerability: CVE-2017-7963

  – CVSS Score: 5

– Description: The GNU Multiple Precision Arithmetic Library (GMP) interfaces for PHP through 7.1.4 allow attackers to cause a denial of service (memory consumption and application crash) via operations on long strings. NOTE: the vendor disputes this, stating "There is no security issue here, because GMP safely aborts in case of an OOM condition. The only attack vector here is denial of service. However, if you allow attacker-controlled, unbounded allocations you have a DoS vector regardless of GMP's OOM behavior.

- Vulnerability: CVE-2022-30556

  – CVSS Score: 5
  – Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- Vulnerability: CVE-2021-39275

  – CVSS Score: 7.5
  – Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2014-3581

  – CVSS Score: 5
  – Description: The cache_merge_headers_out function in modules/cache/cache_util.c in the mod_cache module in the Apache HTTP Server before 2.4.11 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty HTTP Content-Type header.

- Vulnerability: CVE-2016-0736

  – CVSS Score: 5
  – Description: In Apache HTTP Server versions 2.4.0 to 2.4.23, mod_session_crypto was encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This made it vulnerable to padding oracle attacks, particularly with CBC.

- Vulnerability: CVE-2022-29404

  – CVSS Score: 5
  – Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2018-1312

  – CVSS Score: 6.8
  – Description: In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

- Vulnerability: CVE-2022-22720

  – CVSS Score: 7.5

- Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2007-3205

  - CVSS Score: 5
  - Description: The parse_str function in (1) PHP, (2) Hardened-PHP, and (3) Suhosin, when called without a second parameter, might allow remote attackers to overwrite arbitrary variables by specifying variable names and values in the string to be parsed. NOTE: it is not clear whether this is a design limitation of the function or a bug in PHP, although it is likely to be regarded as a bug in Hardened-PHP and Suhosin.

- Vulnerability: CVE-2017-15710

  - CVSS Score: 5
  - Description: In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.

- Vulnerability: CVE-2014-0226

  - CVSS Score: 6.8
  - Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

- Vulnerability: CVE-2022-2068

  - CVSS Score: 10
  - Description: In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze).

- Vulnerability: CVE-2009-3766

- CVSS Score: 6.8
- Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when OpenSSL is used, does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

- Vulnerability: CVE-2009-3767

  - CVSS Score: 4.3
  - Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other versions, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2009-3765

  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2022-22721

  - CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2006-20001

  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2019-10092

  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

- Vulnerability: CVE-2021-3712

  - CVSS Score: 5.8

- Description: ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own "d2i" functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the "data" and "length" fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the "data" field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). It can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y).

- Vulnerability: CVE-2023-0464

  - CVSS Score: N/A

  - Description: A security vulnerability has been identified in all supported versionsof OpenSSL related to the verification of X.509 certificate chainsthat include policy constraints. Attackers may be able to exploit thisvulnerability by creating a malicious certificate chain that triggersexponential use of computational resources, leading to a denial-of-service(DoS) attack on affected systems.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0465

  - CVSS Score: N/A

- Description: Applications that use a non-default option when verifying
  certificates may bevulnerable to an attack from a malicious CA
  to circumvent certain checks.Invalid certificate policies in leaf
  certificates are silently ignored byOpenSSL and other certificate
  policy checks are skipped for that certificate.A malicious CA could
  use this to deliberately assert invalid certificate policiesin order
  to circumvent policy checking on the certificate altogether.Policy
  processing is disabled by default but can be enabled by passingthe
  '-policy' argument to the command line utilities or by calling
  the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0466

  - CVSS Score: N/A

  - Description: The function X509_VERIFY_PARAM_add0_policy() is documented
    toimplicitly enable the certificate policy check when doing
    certificateverification. However the implementation of the
    function does notenable the check which allows certificates
    with invalid or incorrectpolicies to pass the certificate
    verification.As suddenly enabling the policy check could break
    existing deployments it wasdecided to keep the existing behavior of
    the X509_VERIFY_PARAM_add0_policy()function.Instead the applications
    that require OpenSSL to perform certificatepolicy check need
    to use X509_VERIFY_PARAM_set1_policies() or explicitlyenable the
    policy check by calling X509_VERIFY_PARAM_set_flags() withthe
    X509_V_FLAG_POLICY_CHECK flag argument.Certificate policy checks
    are disabled by default in OpenSSL and are notcommonly used by
    applications.

- Vulnerability: CVE-2015-9253

  - CVSS Score: 6.8

  - Description: An issue was discovered in PHP 7.3.x before 7.3.0alpha3, 7.2.x before
    7.2.8, and before 7.1.20. The php-fpm master process restarts
    a child process in an endless loop when using program execution
    functions (e.g., passthru, exec, shell_exec, or system) with a
    non-blocking STDIN stream, causing this master process to consume
    100% of the CPU, and consume disk space with a large volume of error
    logs, as demonstrated by an attack by a customer of a shared-hosting
    facility.

- Vulnerability: CVE-2015-0228

  - CVSS Score: 5

  - Description: The lua_websocket_read function in lua_request.c in the mod_lua module
    in the Apache HTTP Server through 2.4.12 allows remote attackers to
    cause a denial of service (child-process crash) by sending a crafted
    WebSocket Ping frame after a Lua script has called the wsupgrade
    function.

- Vulnerability: CVE-2016-5387

  - CVSS Score: 6.8

  - Description: The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18
    and therefore does not protect applications from the presence of
    untrusted client data in the HTTP_PROXY environment variable, which
    might allow remote attackers to redirect an application's outbound
    HTTP traffic to an arbitrary proxy server via a crafted Proxy header
    in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states
    "This mitigation has been assigned the identifier CVE-2016-5387"; in
    other words, this is not a CVE ID for a vulnerability.

- Vulnerability: CVE-2017-15715

  – CVSS Score: 6.8
  – Description: In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.

- Vulnerability: CVE-2021-40438

  – CVSS Score: 6.8
  – Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2011-1176

  – CVSS Score: 4.3
  – Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2022-23943

  – CVSS Score: 7.5
  – Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

- Vulnerability: CVE-2021-23840

  – CVSS Score: 5
  – Description: Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissable length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2021-23841

  – CVSS Score: 4.3

– Description: The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack. The function X509_issuer_and_serial_hash() is never directly called by OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on certificates that may have been obtained from untrusted sources. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

• Vulnerability: CVE-2018-1301

    – CVSS Score: 4.3
    – Description: A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.

• Vulnerability: CVE-2018-1302

    – CVSS Score: 4.3
    – Description: When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.

• Vulnerability: CVE-2020-1968

    – CVSS Score: 4.3
    – Description: The Raccoon attack exploits a flaw in the TLS specification which can lead to an attacker being able to compute the pre-master secret in connections which have used a Diffie-Hellman (DH) based ciphersuite. In such a case this would result in the attacker being able to eavesdrop on all encrypted communications sent over that TLS connection. The attack can only be exploited if an implementation re-uses a DH secret across multiple TLS connections. Note that this issue only impacts DH ciphersuites and not ECDH ciphersuites. This issue affects OpenSSL 1.0.2 which is out of support and no longer receiving public updates. OpenSSL 1.1.1 is not vulnerable to this issue. Fixed in OpenSSL 1.0.2w (Affected 1.0.2-1.0.2v).

• Vulnerability: CVE-2021-34798

    – CVSS Score: 5
    – Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

• Vulnerability: CVE-2023-25690

- CVSS Score: N/A
- Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0
  through 2.4.55 allow a HTTP Request Smuggling attack.Configurations
  are affected when mod_proxy is enabled along with some form of
  RewriteRule or ProxyPassMatch in which a non-specific pattern
  matches some portion of the user-supplied request-target (URL)
  data and is then re-inserted into the proxied request-target using
  variable substitution. For example, something like:RewriteEngine
  onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1";
  [P]ProxyPassReverse /here/ http://example.com:8080/Request
  splitting/smuggling could result in bypass of access controls in the
  proxy server, proxying unintended URLs to existing origin servers,
  and cache poisoning. Users are recommended to update to at least
  version 2.4.56 of Apache HTTP Server.

- **Vulnerability:** CVE-2019-10098

  - CVSS Score: 5.8
  - Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with
    mod_rewrite that were intended to be self-referential might be fooled
    by encoded newlines and redirect instead to an unexpected URL within
    the request URL.

- **Vulnerability:** CVE-2020-11985

  - CVSS Score: 4.3
  - Description: IP address spoofing when proxying using mod_remoteip and mod_rewrite
    For configurations using proxying with mod_remoteip and certain
    mod_rewrite rules, an attacker could spoof their IP address for
    logging and PHP scripts. Note this issue was fixed in Apache HTTP
    Server 2.4.24 but was retrospectively allocated a low severity CVE in
    2020.

- **Vulnerability:** CVE-2021-4160

  - CVSS Score: 4.3
  - Description: There is a carry propagation bug in the MIPS32 and MIPS64 squaring
    procedure. Many EC algorithms are affected, including some of the
    TLS 1.3 default curves. Impact was not analyzed in detail, because
    the pre-requisites for attack are considered unlikely and include
    reusing private keys. Analysis suggests that attacks against RSA and
    DSA as a result of this defect would be very difficult to perform
    and are not believed likely. Attacks against DH are considered
    just feasible (although very difficult) because most of the work
    necessary to deduce information about a private key may be performed
    offline. The amount of resources required for such an attack would
    be significant. However, for an attack on TLS to be meaningful, the
    server would have to share the DH private key among multiple clients,
    which is no longer an option since CVE-2016-0701. This issue affects
    OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the
    releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For
    the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that
    is available to premium support customers only. It will be made
    available in 1.0.2zc when it is released. The issue only affects
    OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0).
    Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL
    1.0.2zc-dev (Affected 1.0.2-1.0.2zb).

- **Vulnerability:** CVE-2013-4352

  - CVSS Score: 4.3

- Description: The cache_invalidate function in modules/cache/cache_storage.c in the mod_cache module in the Apache HTTP Server 2.4.6, when a caching forward proxy is enabled, allows remote HTTP servers to cause a denial of service (NULL pointer dereference and daemon crash) via vectors that trigger a missing hostname value.

- **Vulnerability:** CVE-2022-26377

  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- **Vulnerability:** CVE-2014-0098

  - CVSS Score: 5
  - Description: The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.

- **Vulnerability:** CVE-2019-9641

  - CVSS Score: 7.5
  - Description: An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_TIFF.

- **Vulnerability:** CVE-2016-8743

  - CVSS Score: 5
  - Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

- **Vulnerability:** CVE-2024-40898

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- **Vulnerability:** CVE-2024-38474

  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- **Vulnerability:** CVE-2022-0778

  - CVSS Score: 5

- Description: The BN_mod_sqrt() function, which computes a modular square root,
  contains a bug that can cause it to loop forever for non-prime
  moduli. Internally this function is used when parsing certificates
  that contain elliptic curve public keys in compressed form or
  explicit elliptic curve parameters with a base point encoded in
  compressed form. It is possible to trigger the infinite loop by
  crafting a certificate that has invalid explicit curve parameters.
  Since certificate parsing happens prior to verification of the
  certificate signature, any process that parses an externally supplied
  certificate may thus be subject to a denial of service attack. The
  infinite loop can also be reached when parsing crafted private
  keys as they can contain explicit elliptic curve parameters. Thus
  vulnerable situations include: - TLS clients consuming server
  certificates - TLS servers consuming client certificates - Hosting
  providers taking certificates or private keys from customers
  - Certificate authorities parsing certification requests from
  subscribers - Anything else which parses ASN.1 elliptic curve
  parameters Also any other applications that use the BN_mod_sqrt()
  where the attacker can control the parameter values are vulnerable
  to this DoS issue. In the OpenSSL 1.0.2 version the public key is
  not parsed during initial parsing of the certificate which makes
  it slightly harder to trigger the infinite loop. However any
  operation which requires the public key from the certificate will
  trigger the infinite loop. In particular the attacker can use a
  self-signed certificate to trigger the loop during verification
  of the certificate signature. This issue affects OpenSSL versions
  1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n
  and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected
  3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m).
  Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

- Vulnerability: CVE-2020-1971

  - CVSS Score: 4.3

– Description: The X.509 GeneralName type is a generic type for representing
                 different types of names. One of those name types is known as
                 EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which
                 compares different instances of a GENERAL_NAME to see if they
                 are equal or not. This function behaves incorrectly when both
                 GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference
                 and a crash may occur leading to a possible denial of service
                 attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two
                 purposes: 1) Comparing CRL distribution point names between an
                 available CRL and a CRL distribution point embedded in an X509
                 certificate 2) When verifying that a timestamp response token signer
                 matches the timestamp authority name (exposed via the API functions
                 TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can
                 control both items being compared then that attacker could trigger
                 a crash. For example if the attacker can trick a client or server
                 into checking a malicious certificate against a malicious CRL then
                 this may occur. Note that some applications automatically download
                 CRLs based on a URL embedded in a certificate. This checking happens
                 prior to the signatures on the certificate and CRL being verified.
                 OpenSSL's s_server, s_client and verify tools have support for the
                 "-crl_download" option which implements automatic CRL downloading and
                 this attack has been demonstrated to work against those tools. Note
                 that an unrelated bug means that affected versions of OpenSSL cannot
                 parse or construct correct encodings of EDIPARTYNAME. However it is
                 possible to construct a malformed EDIPARTYNAME that OpenSSL's parser
                 will accept and hence trigger this attack. All OpenSSL 1.1.1 and
                 1.0.2 versions are affected by this issue. Other OpenSSL releases
                 are out of support and have not been checked. Fixed in OpenSSL
                 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected
                 1.0.2-1.0.2w).

- Vulnerability: CVE-2009-1390

  – CVSS Score: 6.8

  – Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2)
                   GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS
                   certificate in the chain is accepted instead of verifying the entire
                   chain, which allows remote attackers to spoof trusted servers via a
                   man-in-the-middle attack.

- Vulnerability: CVE-2012-3526

  – CVSS Score: 5

  – Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the
                   Apache HTTP Server allows remote attackers to cause a denial of
                   service (server or application crash) via multiple X-Forwarded-For
                   headers in a request.

- Vulnerability: CVE-2023-5678

  – CVSS Score: N/A

- Description: Issue summary: Generating excessively long X9.42 DH keys or checkingexcessively long X9.42 DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_generate_key() togenerate an X9.42 DH key may experience long delays. Likewise, applicationsthat use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check()to check an X9.42 DH key or X9.42 DH parameters may experience long delays.Where the key or parameters that are being checked have been obtained froman untrusted source this may lead to a Denial of Service.While DH_check() performs all the necessary checks (as of CVE-2023-3817),DH_check_pub_key() doesn't make any of these checks, and is thereforevulnerable for excessively large P and Q parameters.Likewise, while DH_generate_key() performs a check for an excessively largeP, it doesn't check for an excessively large Q.An application that calls DH_generate_key() or DH_check_pub_key() andsupplies a key or parameters obtained from an untrusted source could bevulnerable to a Denial of Service attack.DH_generate_key() and DH_check_pub_key() are also called by a number ofother OpenSSL functions. An application calling any of those otherfunctions may similarly be affected. The other functions affected by thisare DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate().Also vulnerable are the OpenSSL pkey command line application when using the"-pubcheck" option, as well as the OpenSSL genpkey command line application.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2017-3736

  - CVSS Score: 4

  - Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

- Vulnerability: CVE-2017-3737

  - CVSS Score: 4.3

– Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

- Vulnerability: CVE-2019-1547

    – CVSS Score: 1.9

    – Description: Normally in OpenSSL EC groups always have a co-factor present and this is used in side channel resistant code paths. However, in some cases, it is possible to construct a group using explicit parameters (instead of using a named curve). In those cases it is possible that such a group does not have the cofactor present. This can occur even where all the parameters match a known named curve. If such a curve is used then OpenSSL falls back to non-side channel resistant code paths which may result in full key recovery during an ECDSA signature operation. In order to be vulnerable an attacker would have to have the ability to time the creation of a large number of signatures where explicit parameters with no co-factor present are in use by an application using libcrypto. For the avoidance of doubt libssl is not vulnerable because explicit parameters are never used. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).

- Vulnerability: CVE-2017-3735

    – CVSS Score: 5

    – Description: While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL before 1.0.2m and 1.1.0g.

- Vulnerability: CVE-2009-2299

    – CVSS Score: 5

    – Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2022-1292

    – CVSS Score: 10

– Description: The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n). Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).

- Vulnerability: CVE-2017-3738

  – CVSS Score: 4.3
  – Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

- Vulnerability: CVE-2020-11579

  – CVSS Score: 5
  – Description: An issue was discovered in Chadha PHPKB 9.0 Enterprise Edition. installer/test-connection.php (part of the installation process) allows a remote unauthenticated attacker to disclose local files on hosts running PHP before 7.2.16, or on hosts where the MySQL ALLOW LOCAL DATA INFILE option is enabled.

- Vulnerability: CVE-2012-4001

  – CVSS Score: 5
  – Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2022-37436

  – CVSS Score: N/A
  – Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2018-17199

  – CVSS Score: 5

- Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session
                   checks the session expiry time before decoding the session. This
                   causes session expiry time to be ignored for mod_session_cookie
                   sessions since the expiry time is loaded when the session is decoded.

- Vulnerability: CVE-2018-0737

  - CVSS Score: 4.3
  - Description: The OpenSSL RSA Key generation algorithm has been shown to be
                   vulnerable to a cache timing side channel attack. An attacker with
                   sufficient access to mount cache timing attacks during the RSA key
                   generation process could recover the private key. Fixed in OpenSSL
                   1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev
                   (Affected 1.0.2b-1.0.2o).

- Vulnerability: CVE-2018-0734

  - CVSS Score: 4.3
  - Description: The OpenSSL DSA signature algorithm has been shown to be vulnerable
                   to a timing side channel attack. An attacker could use variations
                   in the signing algorithm to recover the private key. Fixed in
                   OpenSSL 1.1.1a (Affected 1.1.1). Fixed in OpenSSL 1.1.0j (Affected
                   1.1.0-1.1.0i). Fixed in OpenSSL 1.0.2q (Affected 1.0.2-1.0.2p).

- Vulnerability: CVE-2018-0732

  - CVSS Score: 5
  - Description: During key agreement in a TLS handshake using a DH(E) based
                   ciphersuite a malicious server can send a very large prime value
                   to the client. This will cause the client to spend an unreasonably
                   long period of time generating a key for this prime resulting in a
                   hang until the client has finished. This could be exploited in a
                   Denial Of Service attack. Fixed in OpenSSL 1.1.0i-dev (Affected
                   1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2-1.0.2o).

- Vulnerability: CVE-2017-9788

  - CVSS Score: 6.4
  - Description: In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value
                   placeholder in [Proxy-]Authorization headers of type 'Digest' was
                   not initialized or reset before or between successive key=value
                   assignments by mod_auth_digest. Providing an initial key with no
                   '=' assignment could reflect the stale value of uninitialized pool
                   memory used by the prior request, leading to leakage of potentially
                   confidential information, and a segfault in other cases resulting in
                   denial of service.

- Vulnerability: CVE-2018-0739

  - CVSS Score: 4.3
  - Description: Constructed ASN.1 types with a recursive definition (such as can be
                   found in PKCS7) could eventually exceed the stack given malicious
                   input with excessive recursion. This could result in a Denial Of
                   Service attack. There are no such structures used within SSL/TLS
                   that come from untrusted sources so this is considered safe. Fixed
                   in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o
                   (Affected 1.0.2b-1.0.2n).

- Vulnerability: CVE-2014-8109

  - CVSS Score: 4.3

- Description: mod_lua.c in the mod_lua module in the Apache HTTP Server 2.3.x and 2.4.x through 2.4.10 does not support an httpd configuration in which the same Lua authorization provider is used with different arguments within different contexts, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives, as demonstrated by a configuration that specifies authorization for one group to access a certain directory, and authorization for a second group to access a second directory.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2016-2161

  - CVSS Score: 5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.23, malicious input to mod_auth_digest can cause the server to crash, and each instance continues to crash even for subsequently valid requests.

- Vulnerability: CVE-2016-8612

  - CVSS Score: 3.3
  - Description: Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.

- Vulnerability: CVE-2019-1552

  - CVSS Score: 1.9

- Description: OpenSSL has internal defaults for a directory tree where it can find a configuration file as well as certificates used for verification in TLS. This directory is most commonly referred to as OPENSSLDIR, and is configurable with the --prefix / --openssldir configuration options. For OpenSSL versions 1.1.0 and 1.1.1, the mingw configuration targets assume that resulting programs and libraries are installed in a Unix-like environment and the default prefix for program installation as well as for OPENSSLDIR should be '/usr/local'. However, mingw programs are Windows programs, and as such, find themselves looking at sub-directories of 'C:/usr/local', which may be world writable, which enables untrusted users to modify OpenSSL's default configuration, insert CA certificates, modify (or even replace) existing engine modules, etc. For OpenSSL 1.0.2, '/usr/local/ssl' is used as default for OPENSSLDIR on all Unix and Windows targets, including Visual C builds. However, some build instructions for the diverse Windows targets on 1.0.2 encourage you to specify your own --prefix. OpenSSL versions 1.1.1, 1.1.0 and 1.0.2 are affected by this issue. Due to the limited scope of affected deployments this has been assessed as low severity and therefore we are not creating new releases at this time. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2019-1551

  - CVSS Score: 5
  - Description: There is an overflow bug in the x64_64 Montgomery squaring procedure used in exponentiation with 512-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against 2-prime RSA1024, 3-prime RSA1536, and DSA1024 as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH512 are considered just feasible. However, for an attack the target would have to re-use the DH512 private key, which is not recommended anyway. Also applications directly using the low level API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME. Fixed in OpenSSL 1.1.1e (Affected 1.1.1-1.1.1d). Fixed in OpenSSL 1.0.2u (Affected 1.0.2-1.0.2t).

- Vulnerability: CVE-2019-1559

  - CVSS Score: 4.3

- Description: If an application encounters a fatal protocol error and then calls
               SSL_shutdown() twice (once to send a close_notify, and once to
               receive one) then OpenSSL can respond differently to the calling
               application if a 0 byte record is received with invalid padding
               compared to if a 0 byte record is received with an invalid MAC. If
               the application then behaves differently based on that in a way that
               is detectable to the remote peer, then this amounts to a padding
               oracle that could be used to decrypt data. In order for this to be
               exploitable "non-stitched" ciphersuites must be in use. Stitched
               ciphersuites are optimised implementations of certain commonly
               used ciphersuites. Also the application must call SSL_shutdown()
               twice even if a protocol error has occurred (applications should
               not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected
               1.0.2-1.0.2q).

- Vulnerability: CVE-2023-45802

  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a
                time window were the request's memory resources were not reclaimed
                immediately. Instead, de-allocation was deferred to connection
                close. A client could send new requests and resets, keeping the
                connection busy and open and causing the memory footprint to keep
                on growing. On connection close, all resources were reclaimed, but
                the process might run out of memory before that.This was found by
                the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset
                Exploit) with their own test client. During "normal" HTTP/2 use, the
                probability to hit this bug is very low. The kept memory would not
                become noticeable before the connection closes or times out.Users are
                recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2018-1283

  - CVSS Score: 3.5
  - Description: In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to
                forward its session data to CGI applications (SessionEnv on, not
                the default), a remote user may influence their content by using a
                "Session" header. This comes from the "HTTP_SESSION" variable name
                used by mod_session to forward its data to CGIs, since the prefix
                "HTTP_" is also used by the Apache HTTP Server to pass HTTP header
                fields, per CGI specifications.

- Vulnerability: CVE-2018-1303

  - CVSS Score: 5
  - Description: A specially crafted HTTP request header could have crashed the Apache
                HTTP Server prior to version 2.4.30 due to an out of bound read while
                preparing data to be cached in shared memory. It could be used as
                a Denial of Service attack against users of mod_cache_socache. The
                vulnerability is considered as low risk since mod_cache_socache is not
                widely used, mod_cache_disk is not concerned by this vulnerability.

- Vulnerability: CVE-2019-0217

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition
                in mod_auth_digest when running in a threaded server could allow a
                user with valid credentials to authenticate using another username,
                bypassing configured access control restrictions.

- Vulnerability: CVE-2022-28615

– CVSS Score: 6.4

– Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

• Vulnerability: CVE-2022-28614

– CVSS Score: 5

– Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

11.7 IP Address: 193.205.78.171

- Organization: INFN - Milano

- Operating System: N/A

- Critical Vulnerabilities: 4

- High Vulnerabilities: 27

- Medium Vulnerabilities: 105

- Low Vulnerabilities: 6

- Total Vulnerabilities: 142

Services Running on IP Address

- Service: Apache httpd

  - Port: 80
  - Version: 2.4.37
  - Location: /

- Service: Apache httpd

  - Port: 443
  - Version: 2.4.37
  - Location: /

Vulnerabilities Found

- Vulnerability: CVE-2019-0215

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in mod_ssl when using per-location client certificate verification with TLSv1.3 allowed a client to bypass configured access control restrictions.

- Vulnerability: CVE-2013-4365

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2022-28330

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2021-32791

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2021-32792

  – CVSS Score: 4.3
  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.

- Vulnerability: CVE-2023-31122

  – CVSS Score: N/A
  – Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2024-38476

  – CVSS Score: N/A
  – Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-27316

  – CVSS Score: N/A
  – Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

- Vulnerability: CVE-2024-38474

  – CVSS Score: N/A
  – Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2009-0796

  – CVSS Score: 2.6
  – Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2022-2068

  – CVSS Score: 10

- Description: In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze).

- Vulnerability: CVE-2021-36160

  - CVSS Score: 5
  - Description: A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS). This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48 (inclusive).

- Vulnerability: CVE-2020-1927

  - CVSS Score: 5.8
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.

- Vulnerability: CVE-2023-0286

  - CVSS Score: N/A
  - Description: There is a type confusion vulnerability relating to X.400 address processinginside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING butthe public structure definition for GENERAL_NAME incorrectly specified the typeof the x400Address field as ASN1_TYPE. This field is subsequently interpreted bythe OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than anASN1_STRING.When CRL checking is enabled (i.e. the application sets theX509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to passarbitrary pointers to a memcmp call, enabling them to read memory contents orenact a denial of service. In most cases, the attack requires the attacker toprovide both the certificate chain and CRL, neither of which need to have avalid signature. If the attacker only controls one of these inputs, the otherinput must already contain an X.400 address as a CRL distribution point, whichis uncommon. As such, this vulnerability is most likely to only affectapplications which have implemented their own functionality for retrieving CRLsover a network.

- Vulnerability: CVE-2023-3817

  - CVSS Score: N/A

– Description: Issue summary: Checking excessively long DH keys or parameters may
                be very slow.Impact summary: Applications that use the functions
                DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH
                key or DH parameters may experience longdelays. Where the key or
                parameters that are being checked have been obtainedfrom an untrusted
                source this may lead to a Denial of Service.The function DH_check()
                performs various checks on DH parameters. After fixingCVE-2023-3446
                it was discovered that a large q parameter value can also triggeran
                overly long computation during some of these checks. A correct q
                value,if present, cannot be larger than the modulus p parameter, thus
                it isunnecessary to perform these checks if q is larger than p.An
                application that calls DH_check() and supplies a key or parameters
                obtainedfrom an untrusted source could be vulnerable to a Denial of
                Service attack.The function DH_check() is itself called by a number
                of other OpenSSL functions.An application calling any of those other
                functions may similarly be affected.The other functions affected
                by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable
                are the OpenSSL dhparam and pkeyparam command line applicationswhen
                using the "-check" option.The OpenSSL SSL/TLS implementation is not
                affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not
                affected by this issue.

- Vulnerability: CVE-2021-32786

    – CVSS Score: 5.8

    – Description: mod_auth_openidc is an authentication/authorization module for the
                    Apache 2.x HTTP server that functions as an OpenID Connect Relying
                    Party, authenticating users against an OpenID Connect Provider. In
                    versions prior to 2.4.9, 'oidc_validate_redirect_url()' does not parse
                    URLs the same way as most browsers do. As a result, this function
                    can be bypassed and leads to an Open Redirect vulnerability in the
                    logout functionality. This bug has been fixed in version 2.4.9
                    by replacing any backslash of the URL to redirect with slashes
                    to address a particular breaking change between the different
                    specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this
                    vulnerability can be mitigated by configuring 'mod_auth_openidc' to
                    only allow redirection whose destination matches a given regular
                    expression.

- Vulnerability: CVE-2021-32785

    – CVSS Score: 4.3

    – Description: mod_auth_openidc is an authentication/authorization module for the
                    Apache 2.x HTTP server that functions as an OpenID Connect Relying
                    Party, authenticating users against an OpenID Connect Provider. When
                    mod_auth_openidc versions prior to 2.4.9 are configured to use an
                    unencrypted Redis cache ('OIDCCacheEncrypt off', 'OIDCSessionType
                    server-cache', 'OIDCCacheType redis'), 'mod_auth_openidc' wrongly
                    performed argument interpolation before passing Redis requests to
                    'hiredis', which would perform it again and lead to an uncontrolled
                    format string bug. Initial assessment shows that this bug does
                    not appear to allow gaining arbitrary code execution, but can
                    reliably provoke a denial of service by repeatedly crashing the
                    Apache workers. This bug has been corrected in version 2.4.9 by
                    performing argument interpolation only once, using the 'hiredis'
                    API. As a workaround, this vulnerability can be mitigated by setting
                    'OIDCCacheEncrypt' to 'on', as cache keys are cryptographically
                    hashed before use when this option is enabled.

- Vulnerability: CVE-2020-9490

- CVSS Score: 5
- Description: Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.

- **Vulnerability: CVE-2007-4723**

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- **Vulnerability: CVE-2021-44790**

  - CVSS Score: 7.5
  - Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

- **Vulnerability: CVE-2020-13938**

  - CVSS Score: 2.1
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

- **Vulnerability: CVE-2023-2650**

  - CVSS Score: N/A

– Description: Issue summary: Processing some specially crafted ASN.1 object
identifiers ordata containing them may be very slow.Impact summary:
Applications that use OBJ_obj2txt() directly, or use any ofthe
OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with
no messagesize limit may experience notable to very long delays
when processing thosemessages, which may lead to a Denial of
Service.An OBJECT IDENTIFIER is composed of a series of numbers –
sub-identifiers –most of which have no size limit. OBJ_obj2txt() may
be used to translatean ASN.1 OBJECT IDENTIFIER given in DER encoding
form (using the OpenSSLtype ASN1_OBJECT) to its canonical numeric
text form, which are thesub-identifiers of the OBJECT IDENTIFIER in
decimal form, separated byperiods.When one of the sub-identifiers in
the OBJECT IDENTIFIER is very large(these are sizes that are seen as
absurdly large, taking up tens or hundredsof KiBs), the translation
to a decimal number in text may take a very longtime. The time
complexity is $O(n^2)$ with 'n' being the size of thesub-identifiers
in bytes (*).With OpenSSL 3.0, support to fetch cryptographic
algorithms using names /identifiers in string form was introduced.
This includes using OBJECTIDENTIFIERs in canonical numeric text form
as identifiers for fetchingalgorithms.Such OBJECT IDENTIFIERs may
be received through the ASN.1 structureAlgorithmIdentifier, which
is commonly used in multiple protocols to specifywhat cryptographic
algorithm should be used to sign or verify, encrypt ordecrypt, or
digest passed data.Applications that call OBJ_obj2txt() directly
with untrusted data areaffected, with any version of OpenSSL. If the
use is for the mere purposeof display, the severity is considered
low.In OpenSSL 3.0 and newer, this affects the subsystems OCSP,
PKCS7/SMIME,CMS, CMP/CRMF or TS. It also impacts anything that
processes X.509certificates, including simple things like verifying
its signature.The impact on TLS is relatively low, because all
versions of OpenSSL have a100KiB limit on the peer's certificate
chain. Additionally, this onlyimpacts clients, or servers that
have explicitly enabled clientauthentication.In OpenSSL 1.1.1 and
1.0.2, this only affects displaying diverse objects,such as X.509
certificates. This is assumed to not happen in such a waythat it
would cause a Denial of Service, so these versions are considerednot
affected by this issue in such a way that it would be cause for
concern,and the severity is therefore considered low.

- Vulnerability: CVE-2023-0215

  – CVSS Score: N/A

- Description: The public API function BIO_new_NDEF is a helper function used for streamingASN.1 data via a BIO. It is primarily used internally to OpenSSL to support theSMIME, CMS and PKCS7 streaming capabilities, but may also be called directly byend user applications.The function receives a BIO from the caller, prepends a new BIO_f_asn1 filterBIO onto the front of it to form a BIO chain, and then returns the new head ofthe BIO chain to the caller. Under certain conditions, for example if a CMSrecipient public key is invalid, the new filter BIO is freed and the functionreturns a NULL result indicating a failure. However, in this case, the BIO chainis not properly cleaned up and the BIO passed by the caller still retainsinternal pointers to the previously freed filter BIO. If the caller then goes onto call BIO_pop() on the BIO then a use-after-free will occur. This will mostlikely result in a crash.This scenario occurs directly in the internal function B64_write_ASN1() whichmay cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() onthe BIO. This internal function is in turn called by the public API functionsPEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream,SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7.Other public API functions that may be impacted by this includei2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream andi2d_PKCS7_bio_stream.The OpenSSL cms and smime command line applications are similarly affected.

- Vulnerability: CVE-2020-35452

  - CVSS Score: 6.8
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

- Vulnerability: CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2020-1934

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

- Vulnerability: CVE-2022-36760

  - CVSS Score: N/A
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-4304

  - CVSS Score: N/A

- Description: A timing based side channel exists in the OpenSSL RSA Decryption implementationwhich could be sufficient to recover a plaintext across a network in aBleichenbacher style attack. To achieve a successful decryption an attackerwould have to be able to send a very large number of trial messages fordecryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5,RSA-OEAP and RSASVE.For example, in a TLS connection, RSA is commonly used by a client to send anencrypted pre-master secret to the server. An attacker that had observed agenuine connection between a client and a server could use this flaw to sendtrial messages to the server and record the time taken to process them. After asufficiently large number of messages the attacker could recover the pre-mastersecret used for the original connection and thus be able to decrypt theapplication data sent over that connection.

- Vulnerability: CVE-2019-9517

  - CVSS Score: 7.8
  - Description: Some HTTP/2 implementations are vulnerable to unconstrained interal data buffering, potentially leading to a denial of service. The attacker opens the HTTP/2 window so the peer can send without constraint; however, they leave the TCP window closed so the peer cannot actually write (many of) the bytes on the wire. The attacker then sends a stream of requests for a large response object. Depending on how the servers queue the responses, this can consume excess memory, CPU, or both.

- Vulnerability: CVE-2019-0217

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.

- Vulnerability: CVE-2019-0197

  - CVSS Score: 4.9
  - Description: A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue.

- Vulnerability: CVE-2019-0196

  - CVSS Score: 5
  - Description: A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.

- Vulnerability: CVE-2019-0190

  - CVSS Score: 5
  - Description: A bug exists in the way mod_ssl handled client renegotiations. A remote attacker could send a carefully crafted request that would cause mod_ssl to enter a loop leading to a denial of service. This bug can be only triggered with Apache HTTP Server version 2.4.37 when using OpenSSL version 1.1.1 or later, due to an interaction in changes to handling of renegotiation attempts.

- Vulnerability: CVE-2021-33193

  – CVSS Score: 5
  – Description: A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.

- Vulnerability: CVE-2019-0211

  – CVSS Score: 7.2
  – Description: In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.

- Vulnerability: CVE-2019-17567

  – CVSS Score: 5
  – Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

- Vulnerability: CVE-2022-31813

  – CVSS Score: 7.5
  – Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

- Vulnerability: CVE-2012-4360

  – CVSS Score: 4.3
  – Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2023-4807

  – CVSS Score: N/A

- Description: Issue summary: The POLY1305 MAC (message authentication code) implementationcontains a bug that might corrupt the internal state of applications on theWindows 64 platform when running on newer X86_64 processors supporting theAVX512-IFMA instructions.Impact summary: If in an application that uses the OpenSSL library an attackercan influence whether the POLY1305 MAC algorithm is used, the applicationstate might be corrupted with various application dependent consequences.The POLY1305 MAC (message authentication code) implementation in OpenSSL doesnot save the contents of non-volatile XMM registers on Windows 64 platformwhen calculating the MAC of data larger than 64 bytes. Before returning tothe caller all the XMM registers are set to zero rather than restoring theirprevious content. The vulnerable code is used only on newer x86_64 processorssupporting the AVX512-IFMA instructions.The consequences of this kind of internal application state corruption canbe various – from no consequences, if the calling application does notdepend on the contents of non-volatile XMM registers at all, to the worstconsequences, where the attacker could get complete control of the applicationprocess. However given the contents of the registers are just zeroized sothe attacker cannot put arbitrary values inside, the most likely consequence,if any, would be an incorrect result of some application dependentcalculations or a crash leading to a denial of service.The POLY1305 MAC algorithm is most frequently used as part of theCHACHA20-POLY1305 AEAD (authenticated encryption with associated data)algorithm. The most common usage of this AEAD cipher is with TLS protocolversions 1.2 and 1.3 and a malicious client can influence whether this AEADcipher is used by the server. This implies that server applications usingOpenSSL can be potentially impacted. However we are currently not aware ofany concrete application that would be affected by this issue therefore weconsider this a Low severity security issue.As a workaround the AVX512-IFMA instructions support can be disabled atruntime by setting the environment variable OPENSSL_ia32cap: OPENSSL_ia32cap=:~0x200000The FIPS provider is not affected by this issue.

- Vulnerability: CVE-2009-3767

  - CVSS Score: 4.3
  - Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other versions, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2021-26690

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service

- Vulnerability: CVE-2021-26691

  - CVSS Score: 7.5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow

- Vulnerability: CVE-2019-0220

- CVSS Score: 5
- Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.

- Vulnerability: CVE-2024-38477

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- Vulnerability: CVE-2021-39275

  - CVSS Score: 7.5
  - Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2018-17189

  - CVSS Score: 5
  - Description: In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 (mod_http2) connections.

- Vulnerability: CVE-2022-29404

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2006-20001

  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2020-11993

  - CVSS Score: 4.3
  - Description: Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2021-3711

  – CVSS Score: 7.5

  – Description: In order to decrypt SM2 encrypted data an application is expected to call the API function EVP_PKEY_decrypt(). Typically an application will call this function twice. The first time, on entry, the "out" parameter can be NULL and, on exit, the "outlen" parameter is populated with the buffer size required to hold the decrypted plaintext. The application can then allocate a sufficiently sized buffer and call EVP_PKEY_decrypt() again, but this time passing a non-NULL value for the "out" parameter. A bug in the implementation of the SM2 decryption code means that the calculation of the buffer size required to hold the plaintext returned by the first call to EVP_PKEY_decrypt() can be smaller than the actual size required by the second call. This can lead to a buffer overflow when EVP_PKEY_decrypt() is called by the application a second time with a buffer that is too small. A malicious attacker who is able present SM2 content for decryption to an application could cause attacker chosen data to overflow the buffer by up to a maximum of 62 bytes altering the contents of other data held after the buffer, possibly changing application behaviour or causing the application to crash. The location of the buffer is application dependent but is typically heap allocated. Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k).

- Vulnerability: CVE-2024-0727

  – CVSS Score: N/A

  – Description: Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSLto crash leading to a potential Denial of Service attackImpact summary: Applications loading files in the PKCS12 format from untrustedsources might terminate abruptly.A file in PKCS12 format can contain certificates and keys and may come from anuntrusted source. The PKCS12 specification allows certain fields to be NULL, butOpenSSL does not correctly check for this case. This can lead to a NULL pointerdereference that results in OpenSSL crashing. If an application processes PKCS12files from an untrusted source using the OpenSSL APIs then that application willbe vulnerable to this issue.OpenSSL APIs that are vulnerable to this are: PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a similar issue in SMIME_write_PKCS7(). However since thisfunction is related to writing data we do not consider it security significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.

- Vulnerability: CVE-2009-3766

  – CVSS Score: 6.8

  – Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when OpenSSL is used, does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

- Vulnerability: CVE-2021-44224

  – CVSS Score: 6.4

- Description: A crafted URI sent to httpd configured as a forward proxy
  (ProxyRequests on) can cause a crash (NULL pointer dereference) or,
  for configurations mixing forward and reverse proxy declarations, can
  allow for requests to be directed to a declared Unix Domain Socket
  endpoint (Server Side Request Forgery). This issue affects Apache
  HTTP Server 2.4.7 up to 2.4.51 (included).

- Vulnerability: CVE-2009-3765

  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does
    not properly handle a '\{}0' character in a domain name in the
    subject's Common Name (CN) field of an X.509 certificate, which
    allows man-in-the-middle attackers to spoof arbitrary SSL servers via
    a crafted certificate issued by a legitimate Certification Authority,
    a related issue to CVE-2009-2408.

- Vulnerability: CVE-2022-22721

  - CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than
    350MB (defaults to 1M) on 32 bit systems an integer overflow happens
    which later causes out of bounds writes. This issue affects Apache
    HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2022-22720

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound
    connection when errors are encountered discarding the request body,
    exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2019-10092

  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting
    issue was reported affecting the mod_proxy error page. An attacker
    could cause the link on the error page to be malformed and instead
    point to a page of their choice. This would only be exploitable
    where a server was set up with proxying enabled but was misconfigured
    in such a way that the Proxy Error page was displayed.

- Vulnerability: CVE-2021-3712

  - CVSS Score: 5.8

– Description: ASN.1 strings are represented internally within OpenSSL as an
              ASN1_STRING structure which contains a buffer holding the string
              data and a field holding the buffer length. This contrasts with
              normal C strings which are repesented as a buffer for the string
              data which is terminated with a NUL (0) byte. Although not a
              strict requirement, ASN.1 strings that are parsed using OpenSSL's
              own "d2i" functions (and other similar parsing functions) as well
              as any string whose value has been set with the ASN1_STRING_set()
              function will additionally NUL terminate the byte array in the
              ASN1_STRING structure. However, it is possible for applications
              to directly construct valid ASN1_STRING structures which do not NUL
              terminate the byte array by directly setting the "data" and "length"
              fields in the ASN1_STRING array. This can also happen by using
              the ASN1_STRING_set0() function. Numerous OpenSSL functions that
              print ASN.1 data have been found to assume that the ASN1_STRING byte
              array will be NUL terminated, even though this is not guaranteed for
              strings that have been directly constructed. Where an application
              requests an ASN.1 structure to be printed, and where that ASN.1
              structure contains ASN1_STRINGs that have been directly constructed
              by the application without NUL terminating the "data" field, then
              a read buffer overrun can occur. The same thing can also occur
              during name constraints processing of certificates (for example
              if a certificate has been directly constructed by the application
              instead of loading it via the OpenSSL parsing functions, and the
              certificate contains non NUL terminated ASN1_STRING structures).
              It can also occur in the X509_get1_email(), X509_REQ_get1_email()
              and X509_get1_ocsp() functions. If a malicious actor can cause an
              application to directly construct an ASN1_STRING and then process it
              through one of the affected OpenSSL functions then this issue could
              be hit. This might result in a crash (causing a Denial of Service
              attack). It could also result in the disclosure of private memory
              contents (such as private keys, or sensitive plaintext). Fixed in
              OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za
              (Affected 1.0.2-1.0.2y).

• Vulnerability: CVE-2023-0464

  – CVSS Score: N/A

  – Description: A security vulnerability has been identified in all supported
              versionsof OpenSSL related to the verification of X.509 certificate
              chainsthat include policy constraints. Attackers may be able to
              exploit thisvulnerability by creating a malicious certificate chain
              that triggersexponential use of computational resources, leading
              to a denial-of-service(DoS) attack on affected systems.Policy
              processing is disabled by default but can be enabled by passingthe
              '-policy' argument to the command line utilities or by calling
              the'X509_VERIFY_PARAM_set1_policies()' function.

• Vulnerability: CVE-2023-0465

  – CVSS Score: N/A

- Description: Applications that use a non-default option when verifying
  certificates may bevulnerable to an attack from a malicious CA
  to circumvent certain checks.Invalid certificate policies in leaf
  certificates are silently ignored byOpenSSL and other certificate
  policy checks are skipped for that certificate.A malicious CA could
  use this to deliberately assert invalid certificate policiesin order
  to circumvent policy checking on the certificate altogether.Policy
  processing is disabled by default but can be enabled by passingthe
  '-policy' argument to the command line utilities or by calling
  the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0466

  - CVSS Score: N/A
  - Description: The function X509_VERIFY_PARAM_add0_policy() is documented
    toimplicitly enable the certificate policy check when doing
    certificateverification. However the implementation of the
    function does notenable the check which allows certificates
    with invalid or incorrectpolicies to pass the certificate
    verification.As suddenly enabling the policy check could break
    existing deployments it wasdecided to keep the existing behavior of
    the X509_VERIFY_PARAM_add0_policy()function.Instead the applications
    that require OpenSSL to perform certificatepolicy check need
    to use X509_VERIFY_PARAM_set1_policies() or explicitlyenable the
    policy check by calling X509_VERIFY_PARAM_set_flags() withthe
    X509_V_FLAG_POLICY_CHECK flag argument.Certificate policy checks
    are disabled by default in OpenSSL and are notcommonly used by
    applications.

- Vulnerability: CVE-2019-10098

  - CVSS Score: 5.8
  - Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with
    mod_rewrite that were intended to be self-referential might be fooled
    by encoded newlines and redirect instead to an unexpected URL within
    the request URL.

- Vulnerability: CVE-2019-10097

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4.32-2.4.39, when mod_remoteip was configured
    to use a trusted intermediary proxy server using the "PROXY"
    protocol, a specially crafted PROXY header could trigger a stack
    buffer overflow or NULL pointer deference. This vulnerability
    could only be triggered by a trusted proxy and not by untrusted HTTP
    clients.

- Vulnerability: CVE-2021-40438

  - CVSS Score: 6.8
  - Description: A crafted request uri-path can cause mod_proxy to forward the request
    to an origin server choosen by the remote user. This issue affects
    Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk
    Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP
    Server does not properly handle certain configuration sections that
    specify NiceValue but not AssignUserID, which might allow remote
    attackers to gain privileges by leveraging the root uid and root gid
    of an mpm-itk process.

- Vulnerability: CVE-2022-23943

  – CVSS Score: 7.5
  – Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

- Vulnerability: CVE-2018-17199

  – CVSS Score: 5
  – Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

- Vulnerability: CVE-2021-34798

  – CVSS Score: 5
  – Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2023-25690

  – CVSS Score: N/A
  – Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2020-11984

  – CVSS Score: 7.5
  – Description: Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE

- Vulnerability: CVE-2021-4160

  – CVSS Score: 4.3

- Description: There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that is available to premium support customers only. It will be made available in 1.0.2zc when it is released. The issue only affects OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0). Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL 1.0.2zc-dev (Affected 1.0.2-1.0.2zb).

- Vulnerability: CVE-2022-26377

  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2019-10081

  - CVSS Score: 5
  - Description: HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example configured with "H2PushResource", could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client.

- Vulnerability: CVE-2019-10082

  - CVSS Score: 6.4
  - Description: In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.

- Vulnerability: CVE-2024-40898

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2022-0778

  - CVSS Score: 5

- Description: The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - TLS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

- Vulnerability: CVE-2022-2097

  - CVSS Score: 5

  - Description: AES OCB mode for 32-bit x86 platforms using the AES-NI assembly optimised implementation will not encrypt the entirety of the data under some circumstances. This could reveal sixteen bytes of data that was preexisting in the memory that wasn't written. In the special case of "in place" encryption, sixteen bytes of the plaintext would be revealed. Since OpenSSL does not support OCB based cipher suites for TLS and DTLS, they are both unaffected. Fixed in OpenSSL 3.0.5 (Affected 3.0.0-3.0.4). Fixed in OpenSSL 1.1.1q (Affected 1.1.1-1.1.1p).

- Vulnerability: CVE-2023-27522

  - CVSS Score: N/A

  - Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.Special characters in the origin response header can truncate/split the response forwarded to the client.

- Vulnerability: CVE-2009-1390

  - CVSS Score: 6.8

  - Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2) GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS certificate in the chain is accepted instead of verifying the entire chain, which allows remote attackers to spoof trusted servers via a man-in-the-middle attack.

- Vulnerability: CVE-2012-3526

  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2023-5678

  - CVSS Score: N/A
  - Description: Issue summary: Generating excessively long X9.42 DH keys or checkingexcessively long X9.42 DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_generate_key() togenerate an X9.42 DH key may experience long delays. Likewise, applicationsthat use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check()to check an X9.42 DH key or X9.42 DH parameters may experience long delays.Where the key or parameters that are being checked have been obtained froman untrusted source this may lead to a Denial of Service.While DH_check() performs all the necessary checks (as of CVE-2023-3817),DH_check_pub_key() doesn't make any of these checks, and is thereforevulnerable for excessively large P and Q parameters.Likewise, while DH_generate_key() performs a check for an excessively largeP, it doesn't check for an excessively large Q.An application that calls DH_generate_key() or DH_check_pub_key() andsupplies a key or parameters obtained from an untrusted source could bevulnerable to a Denial of Service attack.DH_generate_key() and DH_check_pub_key() are also called by a number ofother OpenSSL functions. An application calling any of those otherfunctions may similarly be affected. The other functions affected by thisare DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate().Also vulnerable are the OpenSSL pkey command line application when using the"-pubcheck" option, as well as the OpenSSL genpkey command line application.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2022-1292

  - CVSS Score: 10
  - Description: The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n). Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).

- Vulnerability: CVE-2012-4001

- CVSS Score: 5
- Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2022-37436

  - CVSS Score: N/A
  - Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2022-4450

  - CVSS Score: N/A
  - Description: The function PEM_read_bio_ex() reads a PEM file from a BIO and parses anddecodes the "name" (e.g. "CERTIFICATE"), any header data and the payload data.If the function succeeds then the "name_out", "header" and "data" arguments arepopulated with pointers to buffers containing the relevant decoded data. Thecaller is responsible for freeing those buffers. It is possible to construct aPEM file that results in 0 bytes of payload data. In this case PEM_read_bio_ex()will return a failure code but will populate the header argument with a pointerto a buffer that has already been freed. If the caller also frees this bufferthen a double free will occur. This will most likely lead to a crash. Thiscould be exploited by an attacker who has the ability to supply malicious PEMfiles for parsing to achieve a denial of service attack.The functions PEM_read_bio() and PEM_read() are simple wrappers aroundPEM_read_bio_ex() and therefore these functions are also directly affected.These functions are also called indirectly by a number of other OpenSSLfunctions including PEM_X509_INFO_read_bio_ex() andSSL_CTX_use_serverinfo_file() which are also vulnerable. Some OpenSSL internaluses of these functions are not vulnerable because the caller does not free theheader argument if PEM_read_bio_ex() returns a failure code. These locationsinclude the PEM_read_bio_TYPE() functions as well as the decoders introduced inOpenSSL 3.0.The OpenSSL asn1parse command line application is also impacted by this issue.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1

- Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5
  for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM
  Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows
  use an improper encryption algorithm and a weak key for maintaining
  the stored data of the node secret for the SecurID Authentication
  API, which allows local users to obtain sensitive information via
  cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication
    Agent 7.1 before 7.1.1 for Web for Internet Information Services,
    and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to
    inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2023-45802

  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a
    time window were the request's memory resources were not reclaimed
    immediately. Instead, de-allocation was deferred to connection
    close. A client could send new requests and resets, keeping the
    connection busy and open and causing the memory footprint to keep
    on growing. On connection close, all resources were reclaimed, but
    the process might run out of memory before that.This was found by
    the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset
    Exploit) with their own test client. During "normal" HTTP/2 use, the
    probability to hit this bug is very low. The kept memory would not
    become noticeable before the connection closes or times out.Users are
    recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-28615

  - CVSS Score: 6.4
  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose
    information due to a read beyond bounds in ap_strcmp_match() when
    provided with an extremely large input buffer. While no code
    distributed with the server can be coerced into such a call,
    third-party modules or lua scripts that use ap_strcmp_match() may
    hypothetically be affected.

- Vulnerability: CVE-2022-28614

  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier
    may read unintended memory if an attacker can cause the server to
    reflect very large input using ap_rwrite() or ap_rputs(), such as
    with mod_luas r:puts() function. Modules compiled and distributed
    separately from Apache HTTP Server that use the 'ap_rputs' function
    and may pass it a very large (INT_MAX or larger) string must be
    compiled against current headers to resolve the issue.

- Vulnerability: CVE-2019-0215

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in
    mod_ssl when using per-location client certificate verification
    with TLSv1.3 allowed a client to bypass configured access control
    restrictions.

- Vulnerability: CVE-2024-4577

- CVSS Score: N/A
- Description: In PHP versions8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in command line given toWin32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc.

- **Vulnerability: CVE-2013-4365**

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- **Vulnerability: CVE-2022-28330**

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- **Vulnerability: CVE-2021-32791**

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

- **Vulnerability: CVE-2021-32792**

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.

- **Vulnerability: CVE-2023-31122**

  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- **Vulnerability: CVE-2024-38476**

  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- **Vulnerability: CVE-2024-27316**

- CVSS Score: N/A

- Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

- Vulnerability: CVE-2024-38474

  - CVSS Score: N/A

  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2023-3247

  - CVSS Score: N/A

  - Description: In PHP versions 8.0.* before 8.0.29, 8.1.* before 8.1.20, 8.2.* before 8.2.7 when using SOAP HTTP Digest Authentication, random value generator was not checked for failure, and was using narrower range of values than it should have. In case of random generator failure, it could lead to a disclosure of 31 bits of uninitialized memory from the client to the server, and it also made easier to a malicious server to guess the client's nonce.

- Vulnerability: CVE-2009-0796

  - CVSS Score: 2.6

  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2022-2068

  - CVSS Score: 10

  - Description: In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze).

- Vulnerability: CVE-2021-36160

  - CVSS Score: 5

  - Description: A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS). This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48 (inclusive).

- Vulnerability: CVE-2020-1927

  - CVSS Score: 5.8
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.

- Vulnerability: CVE-2023-0286

  - CVSS Score: N/A
  - Description: There is a type confusion vulnerability relating to X.400 address processinginside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING butthe public structure definition for GENERAL_NAME incorrectly specified the typeof the x400Address field as ASN1_TYPE. This field is subsequently interpreted bythe OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than anASN1_STRING.When CRL checking is enabled (i.e. the application sets theX509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to passarbitrary pointers to a memcmp call, enabling them to read memory contents orenact a denial of service. In most cases, the attack requires the attacker toprovide both the certificate chain and CRL, neither of which need to have avalid signature. If the attacker only controls one of these inputs, the otherinput must already contain an X.400 address as a CRL distribution point, whichis uncommon. As such, this vulnerability is most likely to only affectapplications which have implemented their own functionality for retrieving CRLsover a network.

- Vulnerability: CVE-2023-3817

  - CVSS Score: N/A
  - Description: Issue summary: Checking excessively long DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH key or DH parameters may experience longdelays. Where the key or parameters that are being checked have been obtainedfrom an untrusted source this may lead to a Denial of Service.The function DH_check() performs various checks on DH parameters. After fixingCVE-2023-3446 it was discovered that a large q parameter value can also triggeran overly long computation during some of these checks. A correct q value,if present, cannot be larger than the modulus p parameter, thus it isunnecessary to perform these checks if q is larger than p.An application that calls DH_check() and supplies a key or parameters obtainedfrom an untrusted source could be vulnerable to a Denial of Service attack.The function DH_check() is itself called by a number of other OpenSSL functions.An application calling any of those other functions may similarly be affected.The other functions affected by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable are the OpenSSL dhparam and pkeyparam command line applicationswhen using the "-check" option.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2021-32786

  - CVSS Score: 5.8

453

– Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, `oidc_validate_redirect_url()` does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring `mod_auth_openidc` to only allow redirection whose destination matches a given regular expression.

- Vulnerability: CVE-2021-32785

  – CVSS Score: 4.3

  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache (`OIDCCacheEncrypt off`, `OIDCSessionType server-cache`, `OIDCCacheType redis`), `mod_auth_openidc` wrongly performed argument interpolation before passing Redis requests to `hiredis`, which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the `hiredis` API. As a workaround, this vulnerability can be mitigated by setting `OIDCCacheEncrypt` to `on`, as cache keys are cryptographically hashed before use when this option is enabled.

- Vulnerability: CVE-2020-9490

  – CVSS Score: 5

  – Description: Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2007-4723

  – CVSS Score: 7.5

  – Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2021-44790

  – CVSS Score: 7.5

  – Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

- Vulnerability: CVE-2020-13938
  - CVSS Score: 2.1
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows
- Vulnerability: CVE-2023-2650
  - CVSS Score: N/A
  - Description: Issue summary: Processing some specially crafted ASN.1 object identifiers ordata containing them may be very slow.Impact summary: Applications that use OBJ_obj2txt() directly, or use any ofthe OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no messagesize limit may experience notable to very long delays when processing thosemessages, which may lead to a Denial of Service.An OBJECT IDENTIFIER is composed of a series of numbers – sub-identifiers -most of which have no size limit. OBJ_obj2txt() may be used to translatean ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSLtype ASN1_OBJECT) to its canonical numeric text form, which are thesub-identifiers of the OBJECT IDENTIFIER in decimal form, separated byperiods.When one of the sub-identifiers in the OBJECT IDENTIFIER is very large(these are sizes that are seen as absurdly large, taking up tens or hundredsof KiBs), the translation to a decimal number in text may take a very longtime. The time complexity is O(n$\hat{2}$) with 'n' being the size of thesub-identifiers in bytes (*).With OpenSSL 3.0, support to fetch cryptographic algorithms using names /identifiers in string form was introduced. This includes using OBJECTIDENTIFIERs in canonical numeric text form as identifiers for fetchingalgorithms.Such OBJECT IDENTIFIERs may be received through the ASN.1 structureAlgorithmIdentifier, which is commonly used in multiple protocols to specifywhat cryptographic algorithm should be used to sign or verify, encrypt ordecrypt, or digest passed data.Applications that call OBJ_obj2txt() directly with untrusted data areaffected, with any version of OpenSSL. If the use is for the mere purposeof display, the severity is considered low.In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME,CMS, CMP/CRMF or TS. It also impacts anything that processes X.509certificates, including simple things like verifying its signature.The impact on TLS is relatively low, because all versions of OpenSSL have a100KiB limit on the peer's certificate chain. Additionally, this onlyimpacts clients, or servers that have explicitly enabled clientauthentication.In OpenSSL 1.1.1 and 1.0.2, this only affects displaying diverse objects,such as X.509 certificates. This is assumed to not happen in such a waythat it would cause a Denial of Service, so these versions are considerednot affected by this issue in such a way that it would be cause for concern,and the severity is therefore considered low.
- Vulnerability: CVE-2023-0215
  - CVSS Score: N/A

- Description: The public API function BIO_new_NDEF is a helper function used for streamingASN.1 data via a BIO. It is primarily used internally to OpenSSL to support theSMIME, CMS and PKCS7 streaming capabilities, but may also be called directly byend user applications.The function receives a BIO from the caller, prepends a new BIO_f_asn1 filterBIO onto the front of it to form a BIO chain, and then returns the new head ofthe BIO chain to the caller. Under certain conditions, for example if a CMSrecipient public key is invalid, the new filter BIO is freed and the functionreturns a NULL result indicating a failure. However, in this case, the BIO chainis not properly cleaned up and the BIO passed by the caller still retainsinternal pointers to the previously freed filter BIO. If the caller then goes onto call BIO_pop() on the BIO then a use-after-free will occur. This will mostlikely result in a crash.This scenario occurs directly in the internal function B64_write_ASN1() whichmay cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() onthe BIO. This internal function is in turn called by the public API functionsPEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream,SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7.Other public API functions that may be impacted by this includei2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream andi2d_PKCS7_bio_stream.The OpenSSL cms and smime command line applications are similarly affected.

- Vulnerability: CVE-2024-2408

  - CVSS Score: N/A
  - Description: The openssl_private_decrypt function in PHP, when using PKCS1 padding (OPENSSL_PKCS1_PADDING, which is the default), is vulnerable to the Marvin Attack unless it is used with an OpenSSL version that includes the changes from this pull request: https://github.com/openssl/openssl/pull/13817 (rsa_pkcs1_implicit_rejection). These changes are part of OpenSSL 3.2 and have also been backported to stable versions of various Linux distributions, as well as to the PHP builds provided for Windows since the previous release. All distributors and builders should ensure that this version is used to prevent PHP from being vulnerable.PHP Windows builds for the versions8.1.29,8.2.20 and8.3.8 and above include OpenSSL patches that fix the vulnerability.

- Vulnerability: CVE-2020-35452

  - CVSS Score: 6.8
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

- Vulnerability: CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2020-1934

  - CVSS Score: 5

- Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

- **Vulnerability: CVE-2022-36760**

  - CVSS Score: N/A
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- **Vulnerability: CVE-2022-4304**

  - CVSS Score: N/A
  - Description: A timing based side channel exists in the OpenSSL RSA Decryption implementationwhich could be sufficient to recover a plaintext across a network in aBleichenbacher style attack. To achieve a successful decryption an attackerwould have to be able to send a very large number of trial messages fordecryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5,RSA-OEAP and RSASVE.For example, in a TLS connection, RSA is commonly used by a client to send anencrypted pre-master secret to the server. An attacker that had observed agenuine connection between a client and a server could use this flaw to sendtrial messages to the server and record the time taken to process them. After asufficiently large number of messages the attacker could recover the pre-mastersecret used for the original connection and thus be able to decrypt theapplication data sent over that connection.

- **Vulnerability: CVE-2019-9517**

  - CVSS Score: 7.8
  - Description: Some HTTP/2 implementations are vulnerable to unconstrained interal data buffering, potentially leading to a denial of service. The attacker opens the HTTP/2 window so the peer can send without constraint; however, they leave the TCP window closed so the peer cannot actually write (many of) the bytes on the wire. The attacker then sends a stream of requests for a large response object. Depending on how the servers queue the responses, this can consume excess memory, CPU, or both.

- **Vulnerability: CVE-2019-0217**

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.

- **Vulnerability: CVE-2019-0197**

  - CVSS Score: 4.9
  - Description: A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue.

- **Vulnerability: CVE-2019-0196**

- CVSS Score: 5
- Description: A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.

- Vulnerability: CVE-2019-0190

  - CVSS Score: 5
  - Description: A bug exists in the way mod_ssl handled client renegotiations. A remote attacker could send a carefully crafted request that would cause mod_ssl to enter a loop leading to a denial of service. This bug can be only triggered with Apache HTTP Server version 2.4.37 when using OpenSSL version 1.1.1 or later, due to an interaction in changes to handling of renegotiation attempts.

- Vulnerability: CVE-2021-33193

  - CVSS Score: 5
  - Description: A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.

- Vulnerability: CVE-2019-0211

  - CVSS Score: 7.2
  - Description: In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.

- Vulnerability: CVE-2019-17567

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

- Vulnerability: CVE-2022-31813

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

- Vulnerability: CVE-2013-2220

  - CVSS Score: 7.5
  - Description: Buffer overflow in the radius_get_vendor_attr function in the Radius extension before 1.2.7 for PHP allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a large Vendor Specific Attributes (VSA) length value.

- Vulnerability: CVE-2012-4360

  - CVSS Score: 4.3

- Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- **Vulnerability: CVE-2023-4807**

  - CVSS Score: N/A
  - Description: Issue summary: The POLY1305 MAC (message authentication code) implementationcontains a bug that might corrupt the internal state of applications on theWindows 64 platform when running on newer X86_64 processors supporting theAVX512-IFMA instructions.Impact summary: If in an application that uses the OpenSSL library an attackercan influence whether the POLY1305 MAC algorithm is used, the applicationstate might be corrupted with various application dependent consequences.The POLY1305 MAC (message authentication code) implementation in OpenSSL doesnot save the contents of non-volatile XMM registers on Windows 64 platformwhen calculating the MAC of data larger than 64 bytes. Before returning tothe caller all the XMM registers are set to zero rather than restoring theirprevious content. The vulnerable code is used only on newer x86_64 processorssupporting the AVX512-IFMA instructions.The consequences of this kind of internal application state corruption canbe various - from no consequences, if the calling application does notdepend on the contents of non-volatile XMM registers at all, to the worstconsequences, where the attacker could get complete control of the applicationprocess. However given the contents of the registers are just zeroized sothe attacker cannot put arbitrary values inside, the most likely consequence,if any, would be an incorrect result of some application dependentcalculations or a crash leading to a denial of service.The POLY1305 MAC algorithm is most frequently used as part of theCHACHA20-POLY1305 AEAD (authenticated encryption with associated data)algorithm. The most common usage of this AEAD cipher is with TLS protocolversions 1.2 and 1.3 and a malicious client can influence whether this AEADcipher is used by the server. This implies that server applications usingOpenSSL can be potentially impacted. However we are currently not aware ofany concrete application that would be affected by this issue therefore weconsider this a Low severity security issue.As a workaround the AVX512-IFMA instructions support can be disabled atruntime by setting the environment variable OPENSSL_ia32cap: OPENSSL_ia32cap=:~0x200000The FIPS provider is not affected by this issue.

- **Vulnerability: CVE-2009-3767**

  - CVSS Score: 4.3
  - Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other versions, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- **Vulnerability: CVE-2021-26690**

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service

- Vulnerability: CVE-2021-26691

  - CVSS Score: 7.5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow

- Vulnerability: CVE-2019-0220

  - CVSS Score: 5
  - Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.

- Vulnerability: CVE-2024-38477

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- Vulnerability: CVE-2021-39275

  - CVSS Score: 7.5
  - Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2018-17189

  - CVSS Score: 5
  - Description: In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 (mod_http2) connections.

- Vulnerability: CVE-2022-29404

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2006-20001

  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2007-3205

- CVSS Score: 5
- Description: The parse_str function in (1) PHP, (2) Hardened-PHP, and (3) Suhosin, when called without a second parameter, might allow remote attackers to overwrite arbitrary variables by specifying variable names and values in the string to be parsed. NOTE: it is not clear whether this is a design limitation of the function or a bug in PHP, although it is likely to be regarded as a bug in Hardened-PHP and Suhosin.

- Vulnerability: CVE-2020-11993

  - CVSS Score: 4.3
  - Description: Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2021-3711

  - CVSS Score: 7.5
  - Description: In order to decrypt SM2 encrypted data an application is expected to call the API function EVP_PKEY_decrypt(). Typically an application will call this function twice. The first time, on entry, the "out" parameter can be NULL and, on exit, the "outlen" parameter is populated with the buffer size required to hold the decrypted plaintext. The application can then allocate a sufficiently sized buffer and call EVP_PKEY_decrypt() again, but this time passing a non-NULL value for the "out" parameter. A bug in the implementation of the SM2 decryption code means that the calculation of the buffer size required to hold the plaintext returned by the first call to EVP_PKEY_decrypt() can be smaller than the actual size required by the second call. This can lead to a buffer overflow when EVP_PKEY_decrypt() is called by the application a second time with a buffer that is too small. A malicious attacker who is able present SM2 content for decryption to an application could cause attacker chosen data to overflow the buffer by up to a maximum of 62 bytes altering the contents of other data held after the buffer, possibly changing application behaviour or causing the application to crash. The location of the buffer is application dependent but is typically heap allocated. Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k).

- Vulnerability: CVE-2024-0727

  - CVSS Score: N/A

– Description: Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSLto crash leading to a potential Denial of Service attackImpact summary: Applications loading files in the PKCS12 format from untrustedsources might terminate abruptly.A file in PKCS12 format can contain certificates and keys and may come from anuntrusted source. The PKCS12 specification allows certain fields to be NULL, butOpenSSL does not correctly check for this case. This can lead to a NULL pointerdereference that results in OpenSSL crashing. If an application processes PKCS12files from an untrusted source using the OpenSSL APIs then that application willbe vulnerable to this issue.OpenSSL APIs that are vulnerable to this are: PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a similar issue in SMIME_write_PKCS7(). However since thisfunction is related to writing data we do not consider it security significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.

- Vulnerability: CVE-2009-3766

  – CVSS Score: 6.8
  – Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when OpenSSL is used, does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

- Vulnerability: CVE-2021-44224

  – CVSS Score: 6.4
  – Description: A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).

- Vulnerability: CVE-2009-3765

  – CVSS Score: 6.8
  – Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2022-22721

  – CVSS Score: 5.8
  – Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2022-22720

  – CVSS Score: 7.5
  – Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2019-10092

- CVSS Score: 4.3
- Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

- Vulnerability: CVE-2021-3712

  - CVSS Score: 5.8
  - Description: ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own "d2i" functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the "data" and "length" fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the "data" field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). It can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y).

- Vulnerability: CVE-2023-0464

  - CVSS Score: N/A
  - Description: A security vulnerability has been identified in all supported versionsof OpenSSL related to the verification of X.509 certificate chainsthat include policy constraints. Attackers may be able to exploit thisvulnerability by creating a malicious certificate chain that triggersexponential use of computational resources, leading to a denial-of-service(DoS) attack on affected systems.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0465

- CVSS Score: N/A
- Description: Applications that use a non-default option when verifying certificates may bevulnerable to an attack from a malicious CA to circumvent certain checks.Invalid certificate policies in leaf certificates are silently ignored byOpenSSL and other certificate policy checks are skipped for that certificate.A malicious CA could use this to deliberately assert invalid certificate policiesin order to circumvent policy checking on the certificate altogether.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0466

  - CVSS Score: N/A
  - Description: The function X509_VERIFY_PARAM_add0_policy() is documented toimplicitly enable the certificate policy check when doing certificateverification. However the implementation of the function does notenable the check which allows certificates with invalid or incorrectpolicies to pass the certificate verification.As suddenly enabling the policy check could break existing deployments it wasdecided to keep the existing behavior of the X509_VERIFY_PARAM_add0_policy()function.Instead the applications that require OpenSSL to perform certificatepolicy check need to use X509_VERIFY_PARAM_set1_policies() or explicitlyenable the policy check by calling X509_VERIFY_PARAM_set_flags() withthe X509_V_FLAG_POLICY_CHECK flag argument.Certificate policy checks are disabled by default in OpenSSL and are notcommonly used by applications.

- Vulnerability: CVE-2019-10098

  - CVSS Score: 5.8
  - Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.

- Vulnerability: CVE-2019-10097

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4.32-2.4.39, when mod_remoteip was configured to use a trusted intermediary proxy server using the "PROXY" protocol, a specially crafted PROXY header could trigger a stack buffer overflow or NULL pointer deference. This vulnerability could only be triggered by a trusted proxy and not by untrusted HTTP clients.

- Vulnerability: CVE-2021-40438

  - CVSS Score: 6.8
  - Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2011-1176

  - CVSS Score: 4.3

- Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk
  Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP
  Server does not properly handle certain configuration sections that
  specify NiceValue but not AssignUserID, which might allow remote
  attackers to gain privileges by leveraging the root uid and root gid
  of an mpm-itk process.

- Vulnerability: CVE-2022-23943

  - CVSS Score: 7.5
  - Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server
    allows an attacker to overwrite heap memory with possibly attacker
    provided data. This issue affects Apache HTTP Server 2.4 version
    2.4.52 and prior versions.

- Vulnerability: CVE-2018-17199

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session
    checks the session expiry time before decoding the session. This
    causes session expiry time to be ignored for mod_session_cookie
    sessions since the expiry time is loaded when the session is decoded.

- Vulnerability: CVE-2021-34798

  - CVSS Score: 5
  - Description: Malformed requests may cause the server to dereference a NULL
    pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2023-25690

  - CVSS Score: N/A
  - Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0
    through 2.4.55 allow a HTTP Request Smuggling attack.Configurations
    are affected when mod_proxy is enabled along with some form of
    RewriteRule or ProxyPassMatch in which a non-specific pattern
    matches some portion of the user-supplied request-target (URL)
    data and is then re-inserted into the proxied request-target using
    variable substitution. For example, something like:RewriteEngine
    onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1";
    [P]ProxyPassReverse /here/ http://example.com:8080/Request
    splitting/smuggling could result in bypass of access controls in the
    proxy server, proxying unintended URLs to existing origin servers,
    and cache poisoning. Users are recommended to update to at least
    version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2020-11984

  - CVSS Score: 7.5
  - Description: Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure
    and possible RCE

- Vulnerability: CVE-2021-4160

  - CVSS Score: 4.3

- Description: There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that is available to premium support customers only. It will be made available in 1.0.2zc when it is released. The issue only affects OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0). Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL 1.0.2zc-dev (Affected 1.0.2-1.0.2zb).

- Vulnerability: CVE-2022-26377

  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2019-10081

  - CVSS Score: 5
  - Description: HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example configured with "H2PushResource", could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client.

- Vulnerability: CVE-2019-10082

  - CVSS Score: 6.4
  - Description: In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.

- Vulnerability: CVE-2024-40898

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2024-5585

  - CVSS Score: N/A

- Description: In PHP versions8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, the fix forCVE-2024-1874 does not work if the command name includes trailing spaces. Original issue:when using proc_open() command with array syntax, due to insufficient escaping, if the arguments of the executed command are controlled by a malicious user, the user can supply arguments that would execute arbitrary commands in Windows shell.

- Vulnerability: CVE-2023-27522

  - CVSS Score: N/A

  - Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.Special characters in the origin response header can truncate/split the response forwarded to the client.

- Vulnerability: CVE-2022-0778

  - CVSS Score: 5

  - Description: The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - TLS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

- Vulnerability: CVE-2023-3823

  - CVSS Score: N/A

- Description: In PHP versions 8.0.* before 8.0.30, 8.1.* before 8.1.22, and 8.2.* before 8.2.8 various XML functions rely on libxml global state to track configuration variables, like whether external entities are loaded. This state is assumed to be unchanged unless the user explicitly changes it by calling appropriate function. However, since the state is process-global, other modules - such asImageMagick - may also use this library within the same process, and change that global state for their internal purposes, and leave it in a state where external entities loading is enabled. This can lead to the situation where external XML is parsed with external entities loaded, which can lead to disclosure of any local files accessible to PHP. This vulnerable state may persist in the same process across many requests, until the process is shut down.

- Vulnerability: CVE-2022-2097
  - CVSS Score: 5
  - Description: AES OCB mode for 32-bit x86 platforms using the AES-NI assembly optimised implementation will not encrypt the entirety of the data under some circumstances. This could reveal sixteen bytes of data that was preexisting in the memory that wasn't written. In the special case of "in place" encryption, sixteen bytes of the plaintext would be revealed. Since OpenSSL does not support OCB based cipher suites for TLS and DTLS, they are both unaffected. Fixed in OpenSSL 3.0.5 (Affected 3.0.0-3.0.4). Fixed in OpenSSL 1.1.1q (Affected 1.1.1-1.1.1p).

- Vulnerability: CVE-2023-3824
  - CVSS Score: N/A
  - Description: In PHP version 8.0.* before 8.0.30, 8.1.* before 8.1.22, and 8.2.* before 8.2.8, when loading phar file, while reading PHAR directory entries, insufficient length checking may lead to a stack buffer overflow, leading potentially to memory corruption or RCE.

- Vulnerability: CVE-2009-1390
  - CVSS Score: 6.8
  - Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2) GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS certificate in the chain is accepted instead of verifying the entire chain, which allows remote attackers to spoof trusted servers via a man-in-the-middle attack.

- Vulnerability: CVE-2012-3526
  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2024-5458
  - CVSS Score: N/A
  - Description: In PHP versions8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, due to a code logic error, filtering functions such as filter_var when validating URLs(FILTER_VALIDATE_URL) for certain types of URLs the function will result in invalid user information (username + password part of URLs) being treated as valid user information. This may lead to the downstream code accepting invalid URLs as valid and parsing them incorrectly.

- Vulnerability: CVE-2023-5678

  – CVSS Score: N/A

  – Description: Issue summary: Generating excessively long X9.42 DH keys or checkingexcessively long X9.42 DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_generate_key() togenerate an X9.42 DH key may experience long delays. Likewise, applicationsthat use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check()to check an X9.42 DH key or X9.42 DH parameters may experience long delays.Where the key or parameters that are being checked have been obtained froman untrusted source this may lead to a Denial of Service.While DH_check() performs all the necessary checks (as of CVE-2023-3817),DH_check_pub_key() doesn't make any of these checks, and is thereforevulnerable for excessively large P and Q parameters.Likewise, while DH_generate_key() performs a check for an excessively largeP, it doesn't check for an excessively large Q.An application that calls DH_generate_key() or DH_check_pub_key() andsupplies a key or parameters obtained from an untrusted source could bevulnerable to a Denial of Service attack.DH_generate_key() and DH_check_pub_key() are also called by a number ofother OpenSSL functions. An application calling any of those otherfunctions may similarly be affected. The other functions affected by thisare DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate().Also vulnerable are the OpenSSL pkey command line application when using the"-pubcheck" option, as well as the OpenSSL genpkey command line application.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2009-2299

  – CVSS Score: 5

  – Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2022-1292

  – CVSS Score: 10

  – Description: The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n). Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).

- Vulnerability: CVE-2012-4001

  – CVSS Score: 5

  – Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2022-37436

- CVSS Score: N/A
- Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2022-4450

  - CVSS Score: N/A
  - Description: The function PEM_read_bio_ex() reads a PEM file from a BIO and parses anddecodes the "name" (e.g. "CERTIFICATE"), any header data and the payload data.If the function succeeds then the "name_out", "header" and "data" arguments arepopulated with pointers to buffers containing the relevant decoded data. Thecaller is responsible for freeing those buffers. It is possible to construct aPEM file that results in 0 bytes of payload data. In this case PEM_read_bio_ex()will return a failure code but will populate the header argument with a pointerto a buffer that has already been freed. If the caller also frees this bufferthen a double free will occur. This will most likely lead to a crash. Thiscould be exploited by an attacker who has the ability to supply malicious PEMfiles for parsing to achieve a denial of service attack.The functions PEM_read_bio() and PEM_read() are simple wrappers aroundPEM_read_bio_ex() and therefore these functions are also directly affected.These functions are also called indirectly by a number of other OpenSSLfunctions including PEM_X509_INFO_read_bio_ex() andSSL_CTX_use_serverinfo_file() which are also vulnerable. Some OpenSSL internaluses of these functions are not vulnerable because the caller does not free theheader argument if PEM_read_bio_ex() returns a failure code. These locationsinclude the PEM_read_bio_TYPE() functions as well as the decoders introduced inOpenSSL 3.0.The OpenSSL asn1parse command line application is also impacted by this issue.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

- CVSS Score: 4.3
- Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2023-45802

  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-28615

  - CVSS Score: 6.4
  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- Vulnerability: CVE-2022-28614

  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

11.8 IP Address: 159.149.53.172

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 4

- High Vulnerabilities: 26

- Medium Vulnerabilities: 112

- Low Vulnerabilities: 6

- Total Vulnerabilities: 148

Services Running on IP Address

- Service: Apache httpd

  – Port: 80
  – Version: 2.4.37
  – Location: /

- Service: Apache httpd

  – Port: 443
  – Version: 2.4.37
  – Location: https://cas.unimi.it/login?service=https%3A%2F%2Funimia.unimi.it%2Fportal%2Fse

Vulnerabilities Found

- Vulnerability: CVE-2019-0215

  – CVSS Score: 6
  – Description: In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in
                 mod_ssl when using per-location client certificate verification
                 with TLSv1.3 allowed a client to bypass configured access control
                 restrictions.

- Vulnerability: CVE-2013-4365

  – CVSS Score: 7.5
  – Description: Heap-based buffer overflow in the fcgid_header_bucket_read function
                 in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache
                 HTTP Server allows remote attackers to have an unspecified impact via
                 unknown vectors.

- Vulnerability: CVE-2022-28330

  – CVSS Score: 5
  – Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond
                 bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2021-32791

  – CVSS Score: 4.3

- Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2021-32792

  - CVSS Score: 4.3

  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.

- Vulnerability: CVE-2023-31122

  - CVSS Score: N/A

  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2024-38476

  - CVSS Score: N/A

  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-27316

  - CVSS Score: N/A

  - Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

- Vulnerability: CVE-2024-38474

  - CVSS Score: N/A

  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2009-0796

  - CVSS Score: 2.6

  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2022-2068

– CVSS Score: 10

– Description: In addition to the c_rehash shell command injection identified in
                 CVE-2022-1292, further circumstances where the c_rehash script
                 does not properly sanitise shell metacharacters to prevent command
                 injection were found by code review. When the CVE-2022-1292 was
                 fixed it was not discovered that there are other places in the
                 script where the file names of certificates being hashed were
                 possibly passed to a command executed through the shell. This
                 script is distributed by some operating systems in a manner where
                 it is automatically executed. On such operating systems, an
                 attacker could execute arbitrary commands with the privileges of
                 the script. Use of the c_rehash script is considered obsolete and
                 should be replaced by the OpenSSL rehash command line tool. Fixed in
                 OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL
                 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected
                 1.0.2-1.0.2ze).

• Vulnerability: CVE-2021-3449

– CVSS Score: 4.3

– Description: An OpenSSL TLS server may crash if sent a maliciously crafted
                 renegotiation ClientHello message from a client. If a TLSv1.2
                 renegotiation ClientHello omits the signature_algorithms extension
                 (where it was present in the initial ClientHello), but includes a
                 signature_algorithms_cert extension then a NULL pointer dereference
                 will result, leading to a crash and a denial of service attack. A
                 server is only vulnerable if it has TLSv1.2 and renegotiation enabled
                 (which is the default configuration). OpenSSL TLS clients are not
                 impacted by this issue. All OpenSSL 1.1.1 versions are affected
                 by this issue. Users of these versions should upgrade to OpenSSL
                 1.1.1k. OpenSSL 1.0.2 is not impacted by this issue. Fixed in
                 OpenSSL 1.1.1k (Affected 1.1.1-1.1.1j).

• Vulnerability: CVE-2021-36160

– CVSS Score: 5

– Description: A carefully crafted request uri-path can cause mod_proxy_uwsgi to read
                 above the allocated memory and crash (DoS). This issue affects Apache
                 HTTP Server versions 2.4.30 to 2.4.48 (inclusive).

• Vulnerability: CVE-2020-1927

– CVSS Score: 5.8

– Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with
                 mod_rewrite that were intended to be self-referential might be fooled
                 by encoded newlines and redirect instead to an an unexpected URL
                 within the request URL.

• Vulnerability: CVE-2023-0286

– CVSS Score: N/A

– Description: There is a type confusion vulnerability relating to X.400 address processinginside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING butthe public structure definition for GENERAL_NAME incorrectly specified the typeof the x400Address field as ASN1_TYPE. This field is subsequently interpreted bythe OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than anASN1_STRING.When CRL checking is enabled (i.e. the application sets theX509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to passarbitrary pointers to a memcmp call, enabling them to read memory contents orenact a denial of service. In most cases, the attack requires the attacker toprovide both the certificate chain and CRL, neither of which need to have avalid signature. If the attacker only controls one of these inputs, the otherinput must already contain an X.400 address as a CRL distribution point, whichis uncommon. As such, this vulnerability is most likely to only affectapplications which have implemented their own functionality for retrieving CRLsover a network.

- Vulnerability: CVE-2023-3817

  – CVSS Score: N/A

  – Description: Issue summary: Checking excessively long DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH key or DH parameters may experience longdelays. Where the key or parameters that are being checked have been obtainedfrom an untrusted source this may lead to a Denial of Service.The function DH_check() performs various checks on DH parameters. After fixingCVE-2023-3446 it was discovered that a large q parameter value can also triggeran overly long computation during some of these checks. A correct q value,if present, cannot be larger than the modulus p parameter, thus it isunnecessary to perform these checks if q is larger than p.An application that calls DH_check() and supplies a key or parameters obtainedfrom an untrusted source could be vulnerable to a Denial of Service attack.The function DH_check() is itself called by a number of other OpenSSL functions.An application calling any of those other functions may similarly be affected.The other functions affected by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable are the OpenSSL dhparam and pkeyparam command line applicationswhen using the "-check" option.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2021-32786

  – CVSS Score: 5.8

  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, `oidc_validate_redirect_url()` does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring `mod_auth_openidc` to only allow redirection whose destination matches a given regular expression.

- Vulnerability: CVE-2021-32785

  – CVSS Score: 4.3
  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache ('OIDCCacheEncrypt off', 'OIDCSessionType server-cache', 'OIDCCacheType redis'), 'mod_auth_openidc' wrongly performed argument interpolation before passing Redis requests to 'hiredis', which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the 'hiredis' API. As a workaround, this vulnerability can be mitigated by setting 'OIDCCacheEncrypt' to 'on', as cache keys are cryptographically hashed before use when this option is enabled.

- Vulnerability: CVE-2020-9490

  – CVSS Score: 5
  – Description: Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2007-4723

  – CVSS Score: 7.5
  – Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2021-44790

  – CVSS Score: 7.5
  – Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

- Vulnerability: CVE-2020-13938

  – CVSS Score: 2.1
  – Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

- Vulnerability: CVE-2023-2650

  – CVSS Score: N/A

476

– Description: Issue summary: Processing some specially crafted ASN.1 object identifiers ordata containing them may be very slow.Impact summary: Applications that use OBJ_obj2txt() directly, or use any ofthe OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no messagesize limit may experience notable to very long delays when processing thosemessages, which may lead to a Denial of Service.An OBJECT IDENTIFIER is composed of a series of numbers – sub-identifiers –most of which have no size limit. OBJ_obj2txt() may be used to translatean ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSLtype ASN1_OBJECT) to its canonical numeric text form, which are thesub-identifiers of the OBJECT IDENTIFIER in decimal form, separated byperiods.When one of the sub-identifiers in the OBJECT IDENTIFIER is very large(these are sizes that are seen as absurdly large, taking up tens or hundredsof KiBs), the translation to a decimal number in text may take a very longtime. The time complexity is $O(n^2)$ with 'n' being the size of thesub-identifiers in bytes (*).With OpenSSL 3.0, support to fetch cryptographic algorithms using names /identifiers in string form was introduced. This includes using OBJECTIDENTIFIERs in canonical numeric text form as identifiers for fetchingalgorithms.Such OBJECT IDENTIFIERs may be received through the ASN.1 structureAlgorithmIdentifier, which is commonly used in multiple protocols to specifywhat cryptographic algorithm should be used to sign or verify, encrypt ordecrypt, or digest passed data.Applications that call OBJ_obj2txt() directly with untrusted data areaffected, with any version of OpenSSL. If the use is for the mere purposeof display, the severity is considered low.In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME,CMS, CMP/CRMF or TS. It also impacts anything that processes X.509certificates, including simple things like verifying its signature.The impact on TLS is relatively low, because all versions of OpenSSL have a100KiB limit on the peer's certificate chain. Additionally, this onlyimpacts clients, or servers that have explicitly enabled clientauthentication.In OpenSSL 1.1.1 and 1.0.2, this only affects displaying diverse objects,such as X.509 certificates. This is assumed to not happen in such a waythat it would cause a Denial of Service, so these versions are considerednot affected by this issue in such a way that it would be cause for concern,and the severity is therefore considered low.

- Vulnerability: CVE-2023-0215

  – CVSS Score: N/A

– Description: The public API function BIO_new_NDEF is a helper function used for streamingASN.1 data via a BIO. It is primarily used internally to OpenSSL to support theSMIME, CMS and PKCS7 streaming capabilities, but may also be called directly byend user applications.The function receives a BIO from the caller, prepends a new BIO_f_asn1 filterBIO onto the front of it to form a BIO chain, and then returns the new head ofthe BIO chain to the caller. Under certain conditions, for example if a CMSrecipient public key is invalid, the new filter BIO is freed and the functionreturns a NULL result indicating a failure. However, in this case, the BIO chainis not properly cleaned up and the BIO passed by the caller still retainsinternal pointers to the previously freed filter BIO. If the caller then goes onto call BIO_pop() on the BIO then a use-after-free will occur. This will mostlikely result in a crash.This scenario occurs directly in the internal function B64_write_ASN1() whichmay cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() onthe BIO. This internal function is in turn called by the public API functionsPEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream,SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7.Other public API functions that may be impacted by this includei2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream andi2d_PKCS7_bio_stream.The OpenSSL cms and smime command line applications are similarly affected.

• Vulnerability: CVE-2020-35452

    – CVSS Score: 6.8

    – Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

• Vulnerability: CVE-2022-22719

    – CVSS Score: 5

    – Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

• Vulnerability: CVE-2020-1934

    – CVSS Score: 5

    – Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

• Vulnerability: CVE-2022-36760

    – CVSS Score: N/A

    – Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

• Vulnerability: CVE-2022-4304

    – CVSS Score: N/A

- Description: A timing based side channel exists in the OpenSSL RSA Decryption
  implementationwhich could be sufficient to recover a plaintext
  across a network in aBleichenbacher style attack. To achieve a
  successful decryption an attackerwould have to be able to send a
  very large number of trial messages fordecryption. The vulnerability
  affects all RSA padding modes: PKCS#1 v1.5,RSA-OEAP and RSASVE.For
  example, in a TLS connection, RSA is commonly used by a client to
  send anencrypted pre-master secret to the server. An attacker that
  had observed agenuine connection between a client and a server could
  use this flaw to sendtrial messages to the server and record the time
  taken to process them. After asufficiently large number of messages
  the attacker could recover the pre-mastersecret used for the original
  connection and thus be able to decrypt theapplication data sent over
  that connection.

- Vulnerability: CVE-2019-9517

  - CVSS Score: 7.8
  - Description: Some HTTP/2 implementations are vulnerable to unconstrained interal
    data buffering, potentially leading to a denial of service. The
    attacker opens the HTTP/2 window so the peer can send without
    constraint; however, they leave the TCP window closed so the
    peer cannot actually write (many of) the bytes on the wire. The
    attacker then sends a stream of requests for a large response object.
    Depending on how the servers queue the responses, this can consume
    excess memory, CPU, or both.

- Vulnerability: CVE-2019-0217

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition
    in mod_auth_digest when running in a threaded server could allow a
    user with valid credentials to authenticate using another username,
    bypassing configured access control restrictions.

- Vulnerability: CVE-2019-0197

  - CVSS Score: 4.9
  - Description: A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38.
    When HTTP/2 was enabled for a http: host or H2Upgrade was enabled
    for h2 on a https: host, an Upgrade request from http/1.1 to
    http/2 that was not the first request on a connection could lead
    to a misconfiguration and crash. Server that never enabled the
    h2 protocol or that only enabled it for https: and did not set
    "H2Upgrade on" are unaffected by this issue.

- Vulnerability: CVE-2019-0196

  - CVSS Score: 5
  - Description: A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38.
    Using fuzzed network input, the http/2 request handling could be
    made to access freed memory in string comparison when determining the
    method of a request and thus process the request incorrectly.

- Vulnerability: CVE-2019-0190

  - CVSS Score: 5
  - Description: A bug exists in the way mod_ssl handled client renegotiations. A
    remote attacker could send a carefully crafted request that would
    cause mod_ssl to enter a loop leading to a denial of service. This
    bug can be only triggered with Apache HTTP Server version 2.4.37
    when using OpenSSL version 1.1.1 or later, due to an interaction in
    changes to handling of renegotiation attempts.

- Vulnerability: CVE-2021-33193

  - CVSS Score: 5
  - Description: A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.

- Vulnerability: CVE-2019-0211

  - CVSS Score: 7.2
  - Description: In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.

- Vulnerability: CVE-2019-17567

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

- Vulnerability: CVE-2022-31813

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

- Vulnerability: CVE-2012-4360

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2023-4807

  - CVSS Score: N/A

– Description: Issue summary: The POLY1305 MAC (message authentication code)
                 implementationcontains a bug that might corrupt the internal state
                 of applications on theWindows 64 platform when running on newer
                 X86_64 processors supporting theAVX512-IFMA instructions.Impact
                 summary: If in an application that uses the OpenSSL library an
                 attackercan influence whether the POLY1305 MAC algorithm is used,
                 the applicationstate might be corrupted with various application
                 dependent consequences.The POLY1305 MAC (message authentication
                 code) implementation in OpenSSL doesnot save the contents of
                 non-volatile XMM registers on Windows 64 platformwhen calculating
                 the MAC of data larger than 64 bytes. Before returning tothe
                 caller all the XMM registers are set to zero rather than restoring
                 theirprevious content. The vulnerable code is used only on newer
                 x86_64 processorssupporting the AVX512-IFMA instructions.The
                 consequences of this kind of internal application state corruption
                 canbe various – from no consequences, if the calling application
                 does notdepend on the contents of non-volatile XMM registers at
                 all, to the worstconsequences, where the attacker could get complete
                 control of the applicationprocess. However given the contents of
                 the registers are just zeroized sothe attacker cannot put arbitrary
                 values inside, the most likely consequence,if any, would be an
                 incorrect result of some application dependentcalculations or a crash
                 leading to a denial of service.The POLY1305 MAC algorithm is most
                 frequently used as part of theCHACHA20-POLY1305 AEAD (authenticated
                 encryption with associated data)algorithm. The most common usage
                 of this AEAD cipher is with TLS protocolversions 1.2 and 1.3 and
                 a malicious client can influence whether this AEADcipher is used
                 by the server. This implies that server applications usingOpenSSL
                 can be potentially impacted. However we are currently not aware
                 ofany concrete application that would be affected by this issue
                 therefore weconsider this a Low severity security issue.As a
                 workaround the AVX512-IFMA instructions support can be disabled
                 atruntime by setting the environment variable OPENSSL_ia32cap:
                 OPENSSL_ia32cap=:~0x200000The FIPS provider is not affected by this
                 issue.

• Vulnerability: CVE-2009-3767

   – CVSS Score: 4.3

   – Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other
                   versions, when OpenSSL is used, does not properly handle a '\{}0'
                   character in a domain name in the subject's Common Name (CN) field
                   of an X.509 certificate, which allows man-in-the-middle attackers
                   to spoof arbitrary SSL servers via a crafted certificate issued by a
                   legitimate Certification Authority, a related issue to CVE-2009-2408.

• Vulnerability: CVE-2021-26690

   – CVSS Score: 5

   – Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted
                   Cookie header handled by mod_session can cause a NULL pointer
                   dereference and crash, leading to a possible Denial Of Service

• Vulnerability: CVE-2021-26691

   – CVSS Score: 7.5

   – Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted
                   SessionHeader sent by an origin server could cause a heap overflow

• Vulnerability: CVE-2019-0220

– CVSS Score: 5

– Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38.
When the path component of a request URL contains multiple
consecutive slashes ('/'), directives such as LocationMatch and
RewriteRule must account for duplicates in regular expressions while
other aspects of the servers processing will implicitly collapse
them.

- Vulnerability: CVE-2024-38477

  – CVSS Score: N/A

  – Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59
  and earlier allows an attacker to crash the server via a malicious
  request.Users are recommended to upgrade to version 2.4.60, which
  fixes this issue.

- Vulnerability: CVE-2022-30556

  – CVSS Score: 5

  – Description: Apache HTTP Server 2.4.53 and earlier may return lengths to
  applications calling r:wsread() that point past the end of the
  storage allocated for the buffer.

- Vulnerability: CVE-2021-39275

  – CVSS Score: 7.5

  – Description: ap_escape_quotes() may write beyond the end of a buffer when given
  malicious input. No included modules pass untrusted data to these
  functions, but third-party / external modules may. This issue
  affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2018-17189

  – CVSS Score: 5

  – Description: In Apache HTTP server versions 2.4.37 and prior, by sending request
  bodies in a slow loris way to plain resources, the h2 stream for
  that request unnecessarily occupied a server thread cleaning up that
  incoming data. This affects only HTTP/2 (mod_http2) connections.

- Vulnerability: CVE-2022-29404

  – CVSS Score: 5

  – Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a
  lua script that calls r:parsebody(0) may cause a denial of service
  due to no default limit on possible input size.

- Vulnerability: CVE-2006-20001

  – CVSS Score: N/A

  – Description: A carefully crafted If: request header can cause a memory read, or
  write of a single zero byte, in a pool (heap) memory location beyond
  the header value sent. This could cause the process to crash.This
  issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2020-11993

  – CVSS Score: 4.3

  – Description: Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug
  was enabled for the HTTP/2 module and on certain traffic edge
  patterns, logging statements were made on the wrong connection,
  causing concurrent use of memory pools. Configuring the LogLevel of
  mod_http2 above "info" will mitigate this vulnerability for unpatched
  servers.

- Vulnerability: CVE-2021-3711

  – CVSS Score: 7.5
  – Description: In order to decrypt SM2 encrypted data an application is expected to call the API function EVP_PKEY_decrypt(). Typically an application will call this function twice. The first time, on entry, the "out" parameter can be NULL and, on exit, the "outlen" parameter is populated with the buffer size required to hold the decrypted plaintext. The application can then allocate a sufficiently sized buffer and call EVP_PKEY_decrypt() again, but this time passing a non-NULL value for the "out" parameter. A bug in the implementation of the SM2 decryption code means that the calculation of the buffer size required to hold the plaintext returned by the first call to EVP_PKEY_decrypt() can be smaller than the actual size required by the second call. This can lead to a buffer overflow when EVP_PKEY_decrypt() is called by the application a second time with a buffer that is too small. A malicious attacker who is able present SM2 content for decryption to an application could cause attacker chosen data to overflow the buffer by up to a maximum of 62 bytes altering the contents of other data held after the buffer, possibly changing application behaviour or causing the application to crash. The location of the buffer is application dependent but is typically heap allocated. Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k).

- Vulnerability: CVE-2024-0727

  – CVSS Score: N/A
  – Description: Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSLto crash leading to a potential Denial of Service attackImpact summary: Applications loading files in the PKCS12 format from untrustedsources might terminate abruptly.A file in PKCS12 format can contain certificates and keys and may come from anuntrusted source. The PKCS12 specification allows certain fields to be NULL, butOpenSSL does not correctly check for this case. This can lead to a NULL pointerdereference that results in OpenSSL crashing. If an application processes PKCS12files from an untrusted source using the OpenSSL APIs then that application willbe vulnerable to this issue.OpenSSL APIs that are vulnerable to this are: PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a similar issue in SMIME_write_PKCS7(). However since thisfunction is related to writing data we do not consider it security significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.

- Vulnerability: CVE-2009-3766

  – CVSS Score: 6.8
  – Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when OpenSSL is used, does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

- Vulnerability: CVE-2021-44224

  – CVSS Score: 6.4

- Description: A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).

- **Vulnerability:** CVE-2009-3765

  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- **Vulnerability:** CVE-2022-22721

  - CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- **Vulnerability:** CVE-2022-22720

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- **Vulnerability:** CVE-2019-10092

  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

- **Vulnerability:** CVE-2021-3712

  - CVSS Score: 5.8

- Description: ASN.1 strings are represented internally within OpenSSL as an
  ASN1_STRING structure which contains a buffer holding the string
  data and a field holding the buffer length. This contrasts with
  normal C strings which are repesented as a buffer for the string
  data which is terminated with a NUL (0) byte. Although not a
  strict requirement, ASN.1 strings that are parsed using OpenSSL's
  own "d2i" functions (and other similar parsing functions) as well
  as any string whose value has been set with the ASN1_STRING_set()
  function will additionally NUL terminate the byte array in the
  ASN1_STRING structure. However, it is possible for applications
  to directly construct valid ASN1_STRING structures which do not NUL
  terminate the byte array by directly setting the "data" and "length"
  fields in the ASN1_STRING array. This can also happen by using
  the ASN1_STRING_set0() function. Numerous OpenSSL functions that
  print ASN.1 data have been found to assume that the ASN1_STRING byte
  array will be NUL terminated, even though this is not guaranteed for
  strings that have been directly constructed. Where an application
  requests an ASN.1 structure to be printed, and where that ASN.1
  structure contains ASN1_STRINGs that have been directly constructed
  by the application without NUL terminating the "data" field, then
  a read buffer overrun can occur. The same thing can also occur
  during name constraints processing of certificates (for example
  if a certificate has been directly constructed by the application
  instead of loading it via the OpenSSL parsing functions, and the
  certificate contains non NUL terminated ASN1_STRING structures).
  It can also occur in the X509_get1_email(), X509_REQ_get1_email()
  and X509_get1_ocsp() functions. If a malicious actor can cause an
  application to directly construct an ASN1_STRING and then process it
  through one of the affected OpenSSL functions then this issue could
  be hit. This might result in a crash (causing a Denial of Service
  attack). It could also result in the disclosure of private memory
  contents (such as private keys, or sensitive plaintext). Fixed in
  OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za
  (Affected 1.0.2-1.0.2y).

- Vulnerability: CVE-2023-0464

  - CVSS Score: N/A

  - Description: A security vulnerability has been identified in all supported
    versionsof OpenSSL related to the verification of X.509 certificate
    chainsthat include policy constraints. Attackers may be able to
    exploit thisvulnerability by creating a malicious certificate chain
    that triggersexponential use of computational resources, leading
    to a denial-of-service(DoS) attack on affected systems.Policy
    processing is disabled by default but can be enabled by passingthe
    '-policy' argument to the command line utilities or by calling
    the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0465

  - CVSS Score: N/A

- Description: Applications that use a non-default option when verifying certificates may bevulnerable to an attack from a malicious CA to circumvent certain checks.Invalid certificate policies in leaf certificates are silently ignored byOpenSSL and other certificate policy checks are skipped for that certificate.A malicious CA could use this to deliberately assert invalid certificate policiesin order to circumvent policy checking on the certificate altogether.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0466

  - CVSS Score: N/A
  - Description: The function X509_VERIFY_PARAM_add0_policy() is documented toimplicitly enable the certificate policy check when doing certificateverification. However the implementation of the function does notenable the check which allows certificates with invalid or incorrectpolicies to pass the certificate verification.As suddenly enabling the policy check could break existing deployments it wasdecided to keep the existing behavior of the X509_VERIFY_PARAM_add0_policy()function.Instead the applications that require OpenSSL to perform certificatepolicy check need to use X509_VERIFY_PARAM_set1_policies() or explicitlyenable the policy check by calling X509_VERIFY_PARAM_set_flags() withthe X509_V_FLAG_POLICY_CHECK flag argument.Certificate policy checks are disabled by default in OpenSSL and are notcommonly used by applications.

- Vulnerability: CVE-2019-10098

  - CVSS Score: 5.8
  - Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.

- Vulnerability: CVE-2019-10097

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4.32-2.4.39, when mod_remoteip was configured to use a trusted intermediary proxy server using the "PROXY" protocol, a specially crafted PROXY header could trigger a stack buffer overflow or NULL pointer deference. This vulnerability could only be triggered by a trusted proxy and not by untrusted HTTP clients.

- Vulnerability: CVE-2021-40438

  - CVSS Score: 6.8
  - Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2022-23943

  – CVSS Score: 7.5
  – Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

- Vulnerability: CVE-2018-17199

  – CVSS Score: 5
  – Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

- Vulnerability: CVE-2021-23841

  – CVSS Score: 4.3
  – Description: The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack. The function X509_issuer_and_serial_hash() is never directly called by OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on certificates that may have been obtained from untrusted sources. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2021-34798

  – CVSS Score: 5
  – Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2023-25690

  – CVSS Score: N/A
  – Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2020-11984

- CVSS Score: 7.5
- Description: Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE

- Vulnerability: CVE-2021-4160

  - CVSS Score: 4.3
  - Description: There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that is available to premium support customers only. It will be made available in 1.0.2zc when it is released. The issue only affects OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0). Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL 1.0.2zc-dev (Affected 1.0.2-1.0.2zb).

- Vulnerability: CVE-2022-26377

  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2019-10081

  - CVSS Score: 5
  - Description: HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example configured with "H2PushResource", could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client.

- Vulnerability: CVE-2019-10082

  - CVSS Score: 6.4
  - Description: In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.

- Vulnerability: CVE-2024-40898

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2023-27522

  − CVSS Score: N/A

  − Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via
                  mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30
                  through 2.4.55.Special characters in the origin response header can
                  truncate/split the response forwarded to the client.

- Vulnerability: CVE-2022-0778

  − CVSS Score: 5

  − Description: The BN_mod_sqrt() function, which computes a modular square root,
                  contains a bug that can cause it to loop forever for non-prime
                  moduli. Internally this function is used when parsing certificates
                  that contain elliptic curve public keys in compressed form or
                  explicit elliptic curve parameters with a base point encoded in
                  compressed form. It is possible to trigger the infinite loop by
                  crafting a certificate that has invalid explicit curve parameters.
                  Since certificate parsing happens prior to verification of the
                  certificate signature, any process that parses an externally supplied
                  certificate may thus be subject to a denial of service attack. The
                  infinite loop can also be reached when parsing crafted private
                  keys as they can contain explicit elliptic curve parameters. Thus
                  vulnerable situations include: − TLS clients consuming server
                  certificates − TLS servers consuming client certificates − Hosting
                  providers taking certificates or private keys from customers
                  − Certificate authorities parsing certification requests from
                  subscribers − Anything else which parses ASN.1 elliptic curve
                  parameters Also any other applications that use the BN_mod_sqrt()
                  where the attacker can control the parameter values are vulnerable
                  to this DoS issue. In the OpenSSL 1.0.2 version the public key is
                  not parsed during initial parsing of the certificate which makes
                  it slightly harder to trigger the infinite loop. However any
                  operation which requires the public key from the certificate will
                  trigger the infinite loop. In particular the attacker can use a
                  self-signed certificate to trigger the loop during verification
                  of the certificate signature. This issue affects OpenSSL versions
                  1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n
                  and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected
                  3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m).
                  Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

- Vulnerability: CVE-2022-2097

  − CVSS Score: 5

  − Description: AES OCB mode for 32-bit x86 platforms using the AES-NI assembly
                  optimised implementation will not encrypt the entirety of the data
                  under some circumstances. This could reveal sixteen bytes of data
                  that was preexisting in the memory that wasn't written. In the
                  special case of "in place" encryption, sixteen bytes of the plaintext
                  would be revealed. Since OpenSSL does not support OCB based cipher
                  suites for TLS and DTLS, they are both unaffected. Fixed in OpenSSL
                  3.0.5 (Affected 3.0.0-3.0.4). Fixed in OpenSSL 1.1.1q (Affected
                  1.1.1-1.1.1p).

- Vulnerability: CVE-2020-1971

  − CVSS Score: 4.3

– Description: The X.509 GeneralName type is a generic type for representing
              different types of names. One of those name types is known as
              EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which
              compares different instances of a GENERAL_NAME to see if they
              are equal or not. This function behaves incorrectly when both
              GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference
              and a crash may occur leading to a possible denial of service
              attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two
              purposes: 1) Comparing CRL distribution point names between an
              available CRL and a CRL distribution point embedded in an X509
              certificate 2) When verifying that a timestamp response token signer
              matches the timestamp authority name (exposed via the API functions
              TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can
              control both items being compared then that attacker could trigger
              a crash. For example if the attacker can trick a client or server
              into checking a malicious certificate against a malicious CRL then
              this may occur. Note that some applications automatically download
              CRLs based on a URL embedded in a certificate. This checking happens
              prior to the signatures on the certificate and CRL being verified.
              OpenSSL's s_server, s_client and verify tools have support for the
              "-crl_download" option which implements automatic CRL downloading and
              this attack has been demonstrated to work against those tools. Note
              that an unrelated bug means that affected versions of OpenSSL cannot
              parse or construct correct encodings of EDIPARTYNAME. However it is
              possible to construct a malformed EDIPARTYNAME that OpenSSL's parser
              will accept and hence trigger this attack. All OpenSSL 1.1.1 and
              1.0.2 versions are affected by this issue. Other OpenSSL releases
              are out of support and have not been checked. Fixed in OpenSSL
              1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected
              1.0.2-1.0.2w).

- Vulnerability: CVE-2009-1390

  – CVSS Score: 6.8

  – Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2)
              GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS
              certificate in the chain is accepted instead of verifying the entire
              chain, which allows remote attackers to spoof trusted servers via a
              man-in-the-middle attack.

- Vulnerability: CVE-2012-3526

  – CVSS Score: 5

  – Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the
              Apache HTTP Server allows remote attackers to cause a denial of
              service (server or application crash) via multiple X-Forwarded-For
              headers in a request.

- Vulnerability: CVE-2023-5678

  – CVSS Score: N/A

- Description: Issue summary: Generating excessively long X9.42 DH keys or checkingexcessively long X9.42 DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_generate_key() togenerate an X9.42 DH key may experience long delays. Likewise, applicationsthat use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check()to check an X9.42 DH key or X9.42 DH parameters may experience long delays.Where the key or parameters that are being checked have been obtained froman untrusted source this may lead to a Denial of Service.While DH_check() performs all the necessary checks (as of CVE-2023-3817),DH_check_pub_key() doesn't make any of these checks, and is thereforevulnerable for excessively large P and Q parameters.Likewise, while DH_generate_key() performs a check for an excessively largeP, it doesn't check for an excessively large Q.An application that calls DH_generate_key() or DH_check_pub_key() andsupplies a key or parameters obtained from an untrusted source could bevulnerable to a Denial of Service attack.DH_generate_key() and DH_check_pub_key() are also called by a number ofother OpenSSL functions. An application calling any of those otherfunctions may similarly be affected. The other functions affected by thisare DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate().Also vulnerable are the OpenSSL pkey command line application when using the"-pubcheck" option, as well as the OpenSSL genpkey command line application.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2022-1292

  - CVSS Score: 10
  - Description: The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n). Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).

- Vulnerability: CVE-2012-4001

  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2022-37436

  - CVSS Score: N/A

– Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause
               the response headers to be truncated early, resulting in some headers
               being incorporated into the response body. If the later headers have
               any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2021-23840

   – CVSS Score: 5
   – Description: Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate
               may overflow the output length argument in some cases where the input
               length is close to the maximum permissable length for an integer on
               the platform. In such cases the return value from the function call
               will be 1 (indicating success), but the output length value will be
               negative. This could cause applications to behave incorrectly or
               crash. OpenSSL versions 1.1.1i and below are affected by this issue.
               Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL
               versions 1.0.2x and below are affected by this issue. However
               OpenSSL 1.0.2 is out of support and no longer receiving public
               updates. Premium support customers of OpenSSL 1.0.2 should upgrade
               to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL
               1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected
               1.0.2-1.0.2x).

- Vulnerability: CVE-2022-4450

   – CVSS Score: N/A
   – Description: The function PEM_read_bio_ex() reads a PEM file from a BIO and parses
               anddecodes the "name" (e.g. "CERTIFICATE"), any header data and the
               payload data.If the function succeeds then the "name_out", "header"
               and "data" arguments arepopulated with pointers to buffers containing
               the relevant decoded data. Thecaller is responsible for freeing
               those buffers. It is possible to construct aPEM file that results
               in 0 bytes of payload data. In this case PEM_read_bio_ex()will
               return a failure code but will populate the header argument with
               a pointerto a buffer that has already been freed. If the caller
               also frees this bufferthen a double free will occur. This will
               most likely lead to a crash. Thiscould be exploited by an attacker
               who has the ability to supply malicious PEMfiles for parsing to
               achieve a denial of service attack.The functions PEM_read_bio() and
               PEM_read() are simple wrappers aroundPEM_read_bio_ex() and therefore
               these functions are also directly affected.These functions are also
               called indirectly by a number of other OpenSSLfunctions including
               PEM_X509_INFO_read_bio_ex() andSSL_CTX_use_serverinfo_file() which are
               also vulnerable. Some OpenSSL internaluses of these functions are
               not vulnerable because the caller does not free theheader argument
               if PEM_read_bio_ex() returns a failure code. These locationsinclude
               the PEM_read_bio_TYPE() functions as well as the decoders introduced
               inOpenSSL 3.0.The OpenSSL asn1parse command line application is also
               impacted by this issue.

- Vulnerability: CVE-2013-2765

   – CVSS Score: 5
   – Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server
               allows remote attackers to cause a denial of service (NULL pointer
               dereference, process crash, and disk consumption) via a POST request
               with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2011-2688

   – CVSS Score: 7.5

- Description: SQL injection vulnerability in mysql/mysql-auth.pl in the
  mod_authnz_external module 3.2.5 and earlier for the Apache HTTP
  Server allows remote attackers to execute arbitrary SQL commands
  via the user field.

- **Vulnerability: CVE-2013-0941**

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5
    for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM
    Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows
    use an improper encryption algorithm and a weak key for maintaining
    the stored data of the node secret for the SecurID Authentication
    API, which allows local users to obtain sensitive information via
    cryptographic attacks on this data.

- **Vulnerability: CVE-2013-0942**

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication
    Agent 7.1 before 7.1.1 for Web for Internet Information Services,
    and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to
    inject arbitrary web script or HTML via unspecified vectors.

- **Vulnerability: CVE-2023-45802**

  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a
    time window were the request's memory resources were not reclaimed
    immediately. Instead, de-allocation was deferred to connection
    close. A client could send new requests and resets, keeping the
    connection busy and open and causing the memory footprint to keep
    on growing. On connection close, all resources were reclaimed, but
    the process might run out of memory before that.This was found by
    the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset
    Exploit) with their own test client. During "normal" HTTP/2 use, the
    probability to hit this bug is very low. The kept memory would not
    become noticeable before the connection closes or times out.Users are
    recommended to upgrade to version 2.4.58, which fixes the issue.

- **Vulnerability: CVE-2022-28615**

  - CVSS Score: 6.4
  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose
    information due to a read beyond bounds in ap_strcmp_match() when
    provided with an extremely large input buffer. While no code
    distributed with the server can be coerced into such a call,
    third-party modules or lua scripts that use ap_strcmp_match() may
    hypothetically be affected.

- **Vulnerability: CVE-2022-28614**

  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier
    may read unintended memory if an attacker can cause the server to
    reflect very large input using ap_rwrite() or ap_rputs(), such as
    with mod_luas r:puts() function. Modules compiled and distributed
    separately from Apache HTTP Server that use the 'ap_rputs' function
    and may pass it a very large (INT_MAX or larger) string must be
    compiled against current headers to resolve the issue.

- **Vulnerability: CVE-2019-0215**

- CVSS Score: 6
- Description: In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in mod_ssl when using per-location client certificate verification with TLSv1.3 allowed a client to bypass configured access control restrictions.

- **Vulnerability: CVE-2013-4365**

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- **Vulnerability: CVE-2022-28330**

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- **Vulnerability: CVE-2021-32791**

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

- **Vulnerability: CVE-2021-32792**

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.

- **Vulnerability: CVE-2023-31122**

  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- **Vulnerability: CVE-2024-38476**

  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- **Vulnerability: CVE-2024-27316**

  - CVSS Score: N/A
  - Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

- **Vulnerability: CVE-2024-38474**

  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- **Vulnerability: CVE-2009-0796**

  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- **Vulnerability: CVE-2022-2068**

  - CVSS Score: 10
  - Description: In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze).

- **Vulnerability: CVE-2021-3449**

  - CVSS Score: 4.3
  - Description: An OpenSSL TLS server may crash if sent a maliciously crafted renegotiation ClientHello message from a client. If a TLSv1.2 renegotiation ClientHello omits the signature_algorithms extension (where it was present in the initial ClientHello), but includes a signature_algorithms_cert extension then a NULL pointer dereference will result, leading to a crash and a denial of service attack. A server is only vulnerable if it has TLSv1.2 and renegotiation enabled (which is the default configuration). OpenSSL TLS clients are not impacted by this issue. All OpenSSL 1.1.1 versions are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1k. OpenSSL 1.0.2 is not impacted by this issue. Fixed in OpenSSL 1.1.1k (Affected 1.1.1-1.1.1j).

- **Vulnerability: CVE-2021-36160**

  - CVSS Score: 5
  - Description: A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS). This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48 (inclusive).

- **Vulnerability: CVE-2020-1927**

- CVSS Score: 5.8
- Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.

- **Vulnerability: CVE-2023-0286**

  - CVSS Score: N/A
  - Description: There is a type confusion vulnerability relating to X.400 address processinginside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING butthe public structure definition for GENERAL_NAME incorrectly specified the typeof the x400Address field as ASN1_TYPE. This field is subsequently interpreted bythe OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than anASN1_STRING.When CRL checking is enabled (i.e. the application sets theX509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to passarbitrary pointers to a memcmp call, enabling them to read memory contents orenact a denial of service. In most cases, the attack requires the attacker toprovide both the certificate chain and CRL, neither of which need to have avalid signature. If the attacker only controls one of these inputs, the otherinput must already contain an X.400 address as a CRL distribution point, whichis uncommon. As such, this vulnerability is most likely to only affectapplications which have implemented their own functionality for retrieving CRLsover a network.

- **Vulnerability: CVE-2023-3817**

  - CVSS Score: N/A
  - Description: Issue summary: Checking excessively long DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH key or DH parameters may experience longdelays. Where the key or parameters that are being checked have been obtainedfrom an untrusted source this may lead to a Denial of Service.The function DH_check() performs various checks on DH parameters. After fixingCVE-2023-3446 it was discovered that a large q parameter value can also triggeran overly long computation during some of these checks. A correct q value,if present, cannot be larger than the modulus p parameter, thus it isunnecessary to perform these checks if q is larger than p.An application that calls DH_check() and supplies a key or parameters obtainedfrom an untrusted source could be vulnerable to a Denial of Service attack.The function DH_check() is itself called by a number of other OpenSSL functions.An application calling any of those other functions may similarly be affected.The other functions affected by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable are the OpenSSL dhparam and pkeyparam command line applicationswhen using the "-check" option.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- **Vulnerability: CVE-2021-32786**

  - CVSS Score: 5.8

- Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, `oidc_validate_redirect_url()` does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring `mod_auth_openidc` to only allow redirection whose destination matches a given regular expression.

- Vulnerability: CVE-2021-32785

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache (`OIDCCacheEncrypt off`, `OIDCSessionType server-cache`, `OIDCCacheType redis`), `mod_auth_openidc` wrongly performed argument interpolation before passing Redis requests to `hiredis`, which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the `hiredis` API. As a workaround, this vulnerability can be mitigated by setting `OIDCCacheEncrypt` to `on`, as cache keys are cryptographically hashed before use when this option is enabled.

- Vulnerability: CVE-2020-9490

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2021-44790

  - CVSS Score: 7.5
  - Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

- **Vulnerability:** CVE-2020-13938

  – CVSS Score: 2.1
  – Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

- **Vulnerability:** CVE-2023-2650

  – CVSS Score: N/A
  – Description: Issue summary: Processing some specially crafted ASN.1 object identifiers ordata containing them may be very slow.Impact summary: Applications that use OBJ_obj2txt() directly, or use any ofthe OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no messagesize limit may experience notable to very long delays when processing thosemessages, which may lead to a Denial of Service.An OBJECT IDENTIFIER is composed of a series of numbers – sub-identifiers -most of which have no size limit. OBJ_obj2txt() may be used to translatean ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSLtype ASN1_OBJECT) to its canonical numeric text form, which are thesub-identifiers of the OBJECT IDENTIFIER in decimal form, separated byperiods.When one of the sub-identifiers in the OBJECT IDENTIFIER is very large(these are sizes that are seen as absurdly large, taking up tens or hundredsof KiBs), the translation to a decimal number in text may take a very longtime. The time complexity is O(n²) with 'n' being the size of thesub-identifiers in bytes (*).With OpenSSL 3.0, support to fetch cryptographic algorithms using names /identifiers in string form was introduced. This includes using OBJECTIDENTIFIERs in canonical numeric text form as identifiers for fetchingalgorithms.Such OBJECT IDENTIFIERs may be received through the ASN.1 structureAlgorithmIdentifier, which is commonly used in multiple protocols to specifywhat cryptographic algorithm should be used to sign or verify, encrypt ordecrypt, or digest passed data.Applications that call OBJ_obj2txt() directly with untrusted data areaffected, with any version of OpenSSL. If the use is for the mere purposeof display, the severity is considered low.In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME,CMS, CMP/CRMF or TS. It also impacts anything that processes X.509certificates, including simple things like verifying its signature.The impact on TLS is relatively low, because all versions of OpenSSL have a100KiB limit on the peer's certificate chain. Additionally, this onlyimpacts clients, or servers that have explicitly enabled clientauthentication.In OpenSSL 1.1.1 and 1.0.2, this only affects displaying diverse objects,such as X.509 certificates. This is assumed to not happen in such a waythat it would cause a Denial of Service, so these versions are considerednot affected by this issue in such a way that it would be cause for concern,and the severity is therefore considered low.

- **Vulnerability:** CVE-2023-0215

  – CVSS Score: N/A

- Description: The public API function BIO_new_NDEF is a helper function used for streamingASN.1 data via a BIO. It is primarily used internally to OpenSSL to support theSMIME, CMS and PKCS7 streaming capabilities, but may also be called directly byend user applications.The function receives a BIO from the caller, prepends a new BIO_f_asn1 filterBIO onto the front of it to form a BIO chain, and then returns the new head ofthe BIO chain to the caller. Under certain conditions, for example if a CMSrecipient public key is invalid, the new filter BIO is freed and the functionreturns a NULL result indicating a failure. However, in this case, the BIO chainis not properly cleaned up and the BIO passed by the caller still retainsinternal pointers to the previously freed filter BIO. If the caller then goes onto call BIO_pop() on the BIO then a use-after-free will occur. This will mostlikely result in a crash.This scenario occurs directly in the internal function B64_write_ASN1() whichmay cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() onthe BIO. This internal function is in turn called by the public API functionsPEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream,SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7.Other public API functions that may be impacted by this includei2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream andi2d_PKCS7_bio_stream.The OpenSSL cms and smime command line applications are similarly affected.

- Vulnerability: CVE-2020-35452

  - CVSS Score: 6.8
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

- Vulnerability: CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2020-1934

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

- Vulnerability: CVE-2022-36760

  - CVSS Score: N/A
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-4304

  - CVSS Score: N/A

- Description: A timing based side channel exists in the OpenSSL RSA Decryption implementationwhich could be sufficient to recover a plaintext across a network in aBleichenbacher style attack. To achieve a successful decryption an attackerwould have to be able to send a very large number of trial messages fordecryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5,RSA-OEAP and RSASVE.For example, in a TLS connection, RSA is commonly used by a client to send anencrypted pre-master secret to the server. An attacker that had observed agenuine connection between a client and a server could use this flaw to sendtrial messages to the server and record the time taken to process them. After asufficiently large number of messages the attacker could recover the pre-mastersecret used for the original connection and thus be able to decrypt theapplication data sent over that connection.

- Vulnerability: CVE-2019-9517

  - CVSS Score: 7.8
  - Description: Some HTTP/2 implementations are vulnerable to unconstrained interal data buffering, potentially leading to a denial of service. The attacker opens the HTTP/2 window so the peer can send without constraint; however, they leave the TCP window closed so the peer cannot actually write (many of) the bytes on the wire. The attacker then sends a stream of requests for a large response object. Depending on how the servers queue the responses, this can consume excess memory, CPU, or both.

- Vulnerability: CVE-2019-0217

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.

- Vulnerability: CVE-2019-0197

  - CVSS Score: 4.9
  - Description: A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue.

- Vulnerability: CVE-2019-0196

  - CVSS Score: 5
  - Description: A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.

- Vulnerability: CVE-2019-0190

  - CVSS Score: 5
  - Description: A bug exists in the way mod_ssl handled client renegotiations. A remote attacker could send a carefully crafted request that would cause mod_ssl to enter a loop leading to a denial of service. This bug can be only triggered with Apache HTTP Server version 2.4.37 when using OpenSSL version 1.1.1 or later, due to an interaction in changes to handling of renegotiation attempts.

- Vulnerability: CVE-2021-33193

  - CVSS Score: 5
  - Description: A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.

- Vulnerability: CVE-2019-0211

  - CVSS Score: 7.2
  - Description: In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.

- Vulnerability: CVE-2019-17567

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

- Vulnerability: CVE-2022-31813

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

- Vulnerability: CVE-2012-4360

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2023-4807

  - CVSS Score: N/A

- Description: Issue summary: The POLY1305 MAC (message authentication code) implementationcontains a bug that might corrupt the internal state of applications on theWindows 64 platform when running on newer X86_64 processors supporting theAVX512-IFMA instructions.Impact summary: If in an application that uses the OpenSSL library an attackercan influence whether the POLY1305 MAC algorithm is used, the applicationstate might be corrupted with various application dependent consequences.The POLY1305 MAC (message authentication code) implementation in OpenSSL doesnot save the contents of non-volatile XMM registers on Windows 64 platformwhen calculating the MAC of data larger than 64 bytes. Before returning tothe caller all the XMM registers are set to zero rather than restoring theirprevious content. The vulnerable code is used only on newer x86_64 processorssupporting the AVX512-IFMA instructions.The consequences of this kind of internal application state corruption canbe various – from no consequences, if the calling application does notdepend on the contents of non-volatile XMM registers at all, to the worstconsequences, where the attacker could get complete control of the applicationprocess. However given the contents of the registers are just zeroized sothe attacker cannot put arbitrary values inside, the most likely consequence,if any, would be an incorrect result of some application dependentcalculations or a crash leading to a denial of service.The POLY1305 MAC algorithm is most frequently used as part of theCHACHA20-POLY1305 AEAD (authenticated encryption with associated data)algorithm. The most common usage of this AEAD cipher is with TLS protocolversions 1.2 and 1.3 and a malicious client can influence whether this AEADcipher is used by the server. This implies that server applications usingOpenSSL can be potentially impacted. However we are currently not aware ofany concrete application that would be affected by this issue therefore weconsider this a Low severity security issue.As a workaround the AVX512-IFMA instructions support can be disabled atruntime by setting the environment variable OPENSSL_ia32cap: OPENSSL_ia32cap=:~0x200000The FIPS provider is not affected by this issue.

- Vulnerability: CVE-2009-3767

  - CVSS Score: 4.3
  - Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other versions, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2021-26690

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service

- Vulnerability: CVE-2021-26691

  - CVSS Score: 7.5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow

- Vulnerability: CVE-2019-0220

- CVSS Score: 5
- Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.

- Vulnerability: CVE-2024-38477

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- Vulnerability: CVE-2021-39275

  - CVSS Score: 7.5
  - Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2018-17189

  - CVSS Score: 5
  - Description: In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 (mod_http2) connections.

- Vulnerability: CVE-2022-29404

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2006-20001

  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2020-11993

  - CVSS Score: 4.3
  - Description: Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2021-3711

  – CVSS Score: 7.5

  – Description: In order to decrypt SM2 encrypted data an application is expected to
                call the API function EVP_PKEY_decrypt(). Typically an application
                will call this function twice. The first time, on entry, the
                "out" parameter can be NULL and, on exit, the "outlen" parameter
                is populated with the buffer size required to hold the decrypted
                plaintext. The application can then allocate a sufficiently sized
                buffer and call EVP_PKEY_decrypt() again, but this time passing a
                non-NULL value for the "out" parameter. A bug in the implementation
                of the SM2 decryption code means that the calculation of the buffer
                size required to hold the plaintext returned by the first call to
                EVP_PKEY_decrypt() can be smaller than the actual size required
                by the second call. This can lead to a buffer overflow when
                EVP_PKEY_decrypt() is called by the application a second time with
                a buffer that is too small. A malicious attacker who is able present
                SM2 content for decryption to an application could cause attacker
                chosen data to overflow the buffer by up to a maximum of 62 bytes
                altering the contents of other data held after the buffer, possibly
                changing application behaviour or causing the application to crash.
                The location of the buffer is application dependent but is typically
                heap allocated. Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k).

- Vulnerability: CVE-2024-0727

  – CVSS Score: N/A

  – Description: Issue summary: Processing a maliciously formatted PKCS12 file
                may lead OpenSSLto crash leading to a potential Denial of Service
                attackImpact summary: Applications loading files in the PKCS12
                format from untrustedsources might terminate abruptly.A file in
                PKCS12 format can contain certificates and keys and may come from
                anuntrusted source. The PKCS12 specification allows certain fields
                to be NULL, butOpenSSL does not correctly check for this case.
                This can lead to a NULL pointerdereference that results in OpenSSL
                crashing. If an application processes PKCS12files from an untrusted
                source using the OpenSSL APIs then that application willbe vulnerable
                to this issue.OpenSSL APIs that are vulnerable to this are:
                PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(),
                PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a
                similar issue in SMIME_write_PKCS7(). However since thisfunction
                is related to writing data we do not consider it security
                significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected
                by this issue.

- Vulnerability: CVE-2009-3766

  – CVSS Score: 6.8

  – Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when
                OpenSSL is used, does not verify the domain name in the subject's
                Common Name (CN) field of an X.509 certificate, which allows
                man-in-the-middle attackers to spoof SSL servers via an arbitrary
                valid certificate.

- Vulnerability: CVE-2021-44224

  – CVSS Score: 6.4

- Description: A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).

- Vulnerability: CVE-2009-3765

  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2022-22721

  - CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2022-22720

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2019-10092

  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

- Vulnerability: CVE-2021-3712

  - CVSS Score: 5.8

- Description: ASN.1 strings are represented internally within OpenSSL as an
  ASN1_STRING structure which contains a buffer holding the string
  data and a field holding the buffer length. This contrasts with
  normal C strings which are repesented as a buffer for the string
  data which is terminated with a NUL (0) byte. Although not a
  strict requirement, ASN.1 strings that are parsed using OpenSSL's
  own "d2i" functions (and other similar parsing functions) as well
  as any string whose value has been set with the ASN1_STRING_set()
  function will additionally NUL terminate the byte array in the
  ASN1_STRING structure. However, it is possible for applications
  to directly construct valid ASN1_STRING structures which do not NUL
  terminate the byte array by directly setting the "data" and "length"
  fields in the ASN1_STRING array. This can also happen by using
  the ASN1_STRING_set0() function. Numerous OpenSSL functions that
  print ASN.1 data have been found to assume that the ASN1_STRING byte
  array will be NUL terminated, even though this is not guaranteed for
  strings that have been directly constructed. Where an application
  requests an ASN.1 structure to be printed, and where that ASN.1
  structure contains ASN1_STRINGs that have been directly constructed
  by the application without NUL terminating the "data" field, then
  a read buffer overrun can occur. The same thing can also occur
  during name constraints processing of certificates (for example
  if a certificate has been directly constructed by the application
  instead of loading it via the OpenSSL parsing functions, and the
  certificate contains non NUL terminated ASN1_STRING structures).
  It can also occur in the X509_get1_email(), X509_REQ_get1_email()
  and X509_get1_ocsp() functions. If a malicious actor can cause an
  application to directly construct an ASN1_STRING and then process it
  through one of the affected OpenSSL functions then this issue could
  be hit. This might result in a crash (causing a Denial of Service
  attack). It could also result in the disclosure of private memory
  contents (such as private keys, or sensitive plaintext). Fixed in
  OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za
  (Affected 1.0.2-1.0.2y).

- Vulnerability: CVE-2023-0464

  - CVSS Score: N/A

  - Description: A security vulnerability has been identified in all supported
    versionsof OpenSSL related to the verification of X.509 certificate
    chainsthat include policy constraints. Attackers may be able to
    exploit thisvulnerability by creating a malicious certificate chain
    that triggersexponential use of computational resources, leading
    to a denial-of-service(DoS) attack on affected systems.Policy
    processing is disabled by default but can be enabled by passingthe
    '-policy' argument to the command line utilities or by calling
    the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0465

  - CVSS Score: N/A

- Description: Applications that use a non-default option when verifying certificates may bevulnerable to an attack from a malicious CA to circumvent certain checks.Invalid certificate policies in leaf certificates are silently ignored byOpenSSL and other certificate policy checks are skipped for that certificate.A malicious CA could use this to deliberately assert invalid certificate policiesin order to circumvent policy checking on the certificate altogether.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.

- **Vulnerability:** CVE-2023-0466

  - CVSS Score: N/A
  - Description: The function X509_VERIFY_PARAM_add0_policy() is documented toimplicitly enable the certificate policy check when doing certificateverification. However the implementation of the function does notenable the check which allows certificates with invalid or incorrectpolicies to pass the certificate verification.As suddenly enabling the policy check could break existing deployments it wasdecided to keep the existing behavior of the X509_VERIFY_PARAM_add0_policy()function.Instead the applications that require OpenSSL to perform certificatepolicy check need to use X509_VERIFY_PARAM_set1_policies() or explicitlyenable the policy check by calling X509_VERIFY_PARAM_set_flags() withthe X509_V_FLAG_POLICY_CHECK flag argument.Certificate policy checks are disabled by default in OpenSSL and are notcommonly used by applications.

- **Vulnerability:** CVE-2019-10098

  - CVSS Score: 5.8
  - Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.

- **Vulnerability:** CVE-2019-10097

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4.32-2.4.39, when mod_remoteip was configured to use a trusted intermediary proxy server using the "PROXY" protocol, a specially crafted PROXY header could trigger a stack buffer overflow or NULL pointer deference. This vulnerability could only be triggered by a trusted proxy and not by untrusted HTTP clients.

- **Vulnerability:** CVE-2021-40438

  - CVSS Score: 6.8
  - Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

- **Vulnerability:** CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2022-23943

  - CVSS Score: 7.5
  - Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

- Vulnerability: CVE-2018-17199

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

- Vulnerability: CVE-2021-23841

  - CVSS Score: 4.3
  - Description: The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack. The function X509_issuer_and_serial_hash() is never directly called by OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on certificates that may have been obtained from untrusted sources. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2021-34798

  - CVSS Score: 5
  - Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2023-25690

  - CVSS Score: N/A
  - Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2020-11984

- CVSS Score: 7.5
- Description: Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE

- Vulnerability: CVE-2021-4160

  - CVSS Score: 4.3
  - Description: There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that is available to premium support customers only. It will be made available in 1.0.2zc when it is released. The issue only affects OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0). Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL 1.0.2zc-dev (Affected 1.0.2-1.0.2zb).

- Vulnerability: CVE-2022-26377

  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2019-10081

  - CVSS Score: 5
  - Description: HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example configured with "H2PushResource", could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client.

- Vulnerability: CVE-2019-10082

  - CVSS Score: 6.4
  - Description: In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.

- Vulnerability: CVE-2024-40898

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2023-27522

  – CVSS Score: N/A

  – Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.Special characters in the origin response header can truncate/split the response forwarded to the client.

- Vulnerability: CVE-2022-0778

  – CVSS Score: 5

  – Description: The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: – TLS clients consuming server certificates – TLS servers consuming client certificates – Hosting providers taking certificates or private keys from customers – Certificate authorities parsing certification requests from subscribers – Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

- Vulnerability: CVE-2022-2097

  – CVSS Score: 5

  – Description: AES OCB mode for 32-bit x86 platforms using the AES-NI assembly optimised implementation will not encrypt the entirety of the data under some circumstances. This could reveal sixteen bytes of data that was preexisting in the memory that wasn't written. In the special case of "in place" encryption, sixteen bytes of the plaintext would be revealed. Since OpenSSL does not support OCB based cipher suites for TLS and DTLS, they are both unaffected. Fixed in OpenSSL 3.0.5 (Affected 3.0.0-3.0.4). Fixed in OpenSSL 1.1.1q (Affected 1.1.1-1.1.1p).

- Vulnerability: CVE-2020-1971

  – CVSS Score: 4.3

- Description: The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s_server, s_client and verify tools have support for the "-crl_download" option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue. Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w).

- Vulnerability: CVE-2009-1390

  - CVSS Score: 6.8
  - Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2) GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS certificate in the chain is accepted instead of verifying the entire chain, which allows remote attackers to spoof trusted servers via a man-in-the-middle attack.

- Vulnerability: CVE-2012-3526

  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2023-5678

  - CVSS Score: N/A

- Description: Issue summary: Generating excessively long X9.42 DH keys or checkingexcessively long X9.42 DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_generate_key() togenerate an X9.42 DH key may experience long delays. Likewise, applicationsthat use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check()to check an X9.42 DH key or X9.42 DH parameters may experience long delays.Where the key or parameters that are being checked have been obtained froman untrusted source this may lead to a Denial of Service.While DH_check() performs all the necessary checks (as of CVE-2023-3817),DH_check_pub_key() doesn't make any of these checks, and is thereforevulnerable for excessively large P and Q parameters.Likewise, while DH_generate_key() performs a check for an excessively largeP, it doesn't check for an excessively large Q.An application that calls DH_generate_key() or DH_check_pub_key() andsupplies a key or parameters obtained from an untrusted source could bevulnerable to a Denial of Service attack.DH_generate_key() and DH_check_pub_key() are also called by a number ofother OpenSSL functions. An application calling any of those otherfunctions may similarly be affected. The other functions affected by thisare DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate().Also vulnerable are the OpenSSL pkey command line application when using the"-pubcheck" option, as well as the OpenSSL genpkey command line application.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2022-1292

  - CVSS Score: 10
  - Description: The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n). Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).

- Vulnerability: CVE-2012-4001

  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2022-37436

  - CVSS Score: N/A

- Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2021-23840

  - CVSS Score: 5
  - Description: Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissable length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2022-4450

  - CVSS Score: N/A
  - Description: The function PEM_read_bio_ex() reads a PEM file from a BIO and parses anddecodes the "name" (e.g. "CERTIFICATE"), any header data and the payload data.If the function succeeds then the "name_out", "header" and "data" arguments arepopulated with pointers to buffers containing the relevant decoded data. Thecaller is responsible for freeing those buffers. It is possible to construct aPEM file that results in 0 bytes of payload data. In this case PEM_read_bio_ex()will return a failure code but will populate the header argument with a pointerto a buffer that has already been freed. If the caller also frees this bufferthen a double free will occur. This will most likely lead to a crash. Thiscould be exploited by an attacker who has the ability to supply malicious PEMfiles for parsing to achieve a denial of service attack.The functions PEM_read_bio() and PEM_read() are simple wrappers aroundPEM_read_bio_ex() and therefore these functions are also directly affected.These functions are also called indirectly by a number of other OpenSSLfunctions including PEM_X509_INFO_read_bio_ex() andSSL_CTX_use_serverinfo_file() which are also vulnerable. Some OpenSSL internaluses of these functions are not vulnerable because the caller does not free theheader argument if PEM_read_bio_ex() returns a failure code. These locationsinclude the PEM_read_bio_TYPE() functions as well as the decoders introduced inOpenSSL 3.0.The OpenSSL asn1parse command line application is also impacted by this issue.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5

- Description: SQL injection vulnerability in mysql/mysql-auth.pl in the
                 mod_authnz_external module 3.2.5 and earlier for the Apache HTTP
                 Server allows remote attackers to execute arbitrary SQL commands
                 via the user field.

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5
                 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM
                 Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows
                 use an improper encryption algorithm and a weak key for maintaining
                 the stored data of the node secret for the SecurID Authentication
                 API, which allows local users to obtain sensitive information via
                 cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication
                 Agent 7.1 before 7.1.1 for Web for Internet Information Services,
                 and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to
                 inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2023-45802

  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a
                 time window were the request's memory resources were not reclaimed
                 immediately. Instead, de-allocation was deferred to connection
                 close. A client could send new requests and resets, keeping the
                 connection busy and open and causing the memory footprint to keep
                 on growing. On connection close, all resources were reclaimed, but
                 the process might run out of memory before that.This was found by
                 the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset
                 Exploit) with their own test client. During "normal" HTTP/2 use, the
                 probability to hit this bug is very low. The kept memory would not
                 become noticeable before the connection closes or times out.Users are
                 recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-28615

  - CVSS Score: 6.4
  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose
                 information due to a read beyond bounds in ap_strcmp_match() when
                 provided with an extremely large input buffer. While no code
                 distributed with the server can be coerced into such a call,
                 third-party modules or lua scripts that use ap_strcmp_match() may
                 hypothetically be affected.

- Vulnerability: CVE-2022-28614

  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier
                 may read unintended memory if an attacker can cause the server to
                 reflect very large input using ap_rwrite() or ap_rputs(), such as
                 with mod_luas r:puts() function. Modules compiled and distributed
                 separately from Apache HTTP Server that use the 'ap_rputs' function
                 and may pass it a very large (INT_MAX or larger) string must be
                 compiled against current headers to resolve the issue.

11.9   IP Address: 159.149.53.221

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 4

- High Vulnerabilities: 26

- Medium Vulnerabilities: 112

- Low Vulnerabilities: 6

- Total Vulnerabilities: 148

Services Running on IP Address

- Service: Apache httpd

    – Port: 80
    – Version: 2.4.37
    – Location: https://work.unimi.it/

- Service: Apache httpd

    – Port: 443
    – Version: 2.4.37
    – Location: /

Vulnerabilities Found

- Vulnerability: CVE-2019-0215

    – CVSS Score: 6
    – Description: In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in
      mod_ssl when using per-location client certificate verification
      with TLSv1.3 allowed a client to bypass configured access control
      restrictions.

- Vulnerability: CVE-2013-4365

    – CVSS Score: 7.5
    – Description: Heap-based buffer overflow in the fcgid_header_bucket_read function
      in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache
      HTTP Server allows remote attackers to have an unspecified impact via
      unknown vectors.

- Vulnerability: CVE-2022-28330

    – CVSS Score: 5
    – Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond
      bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2021-32791

    – CVSS Score: 4.3
    – Description: mod_auth_openidc is an authentication/authorization module for the
      Apache 2.x HTTP server that functions as an OpenID Connect Relying
      Party, authenticating users against an OpenID Connect Provider.
      In mod_auth_openidc before version 2.4.9, the AES GCM encryption in
      mod_auth_openidc uses a static IV and AAD. It is important to fix
      because this creates a static nonce and since aes-gcm is a stream
      cipher, this can lead to known cryptographic issues, since the same
      key is being reused. From 2.4.9 onwards this has been patched to use
      dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2021-32792

  – CVSS Score: 4.3
  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.

- Vulnerability: CVE-2023-31122

  – CVSS Score: N/A
  – Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2024-38476

  – CVSS Score: N/A
  – Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-27316

  – CVSS Score: N/A
  – Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

- Vulnerability: CVE-2024-38474

  – CVSS Score: N/A
  – Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2009-0796

  – CVSS Score: 2.6
  – Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2022-2068

  – CVSS Score: 10

- Description: In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze).

- **Vulnerability: CVE-2021-3449**

  - CVSS Score: 4.3
  - Description: An OpenSSL TLS server may crash if sent a maliciously crafted renegotiation ClientHello message from a client. If a TLSv1.2 renegotiation ClientHello omits the signature_algorithms extension (where it was present in the initial ClientHello), but includes a signature_algorithms_cert extension then a NULL pointer dereference will result, leading to a crash and a denial of service attack. A server is only vulnerable if it has TLSv1.2 and renegotiation enabled (which is the default configuration). OpenSSL TLS clients are not impacted by this issue. All OpenSSL 1.1.1 versions are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1k. OpenSSL 1.0.2 is not impacted by this issue. Fixed in OpenSSL 1.1.1k (Affected 1.1.1-1.1.1j).

- **Vulnerability: CVE-2021-36160**

  - CVSS Score: 5
  - Description: A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS). This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48 (inclusive).

- **Vulnerability: CVE-2020-1927**

  - CVSS Score: 5.8
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.

- **Vulnerability: CVE-2023-0286**

  - CVSS Score: N/A

– Description: There is a type confusion vulnerability relating to X.400 address processinginside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING butthe public structure definition for GENERAL_NAME incorrectly specified the typeof the x400Address field as ASN1_TYPE. This field is subsequently interpreted bythe OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than anASN1_STRING.When CRL checking is enabled (i.e. the application sets theX509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to passarbitrary pointers to a memcmp call, enabling them to read memory contents orenact a denial of service. In most cases, the attack requires the attacker toprovide both the certificate chain and CRL, neither of which need to have avalid signature. If the attacker only controls one of these inputs, the otherinput must already contain an X.400 address as a CRL distribution point, whichis uncommon. As such, this vulnerability is most likely to only affectapplications which have implemented their own functionality for retrieving CRLsover a network.

- Vulnerability: CVE-2023-3817

  – CVSS Score: N/A

  – Description: Issue summary: Checking excessively long DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH key or DH parameters may experience longdelays. Where the key or parameters that are being checked have been obtainedfrom an untrusted source this may lead to a Denial of Service.The function DH_check() performs various checks on DH parameters. After fixingCVE-2023-3446 it was discovered that a large q parameter value can also triggeran overly long computation during some of these checks. A correct q value,if present, cannot be larger than the modulus p parameter, thus it isunnecessary to perform these checks if q is larger than p.An application that calls DH_check() and supplies a key or parameters obtainedfrom an untrusted source could be vulnerable to a Denial of Service attack.The function DH_check() is itself called by a number of other OpenSSL functions.An application calling any of those other functions may similarly be affected.The other functions affected by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable are the OpenSSL dhparam and pkeyparam command line applicationswhen using the "-check" option.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2021-32786

  – CVSS Score: 5.8

  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, 'oidc_validate_redirect_url()' does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring 'mod_auth_openidc' to only allow redirection whose destination matches a given regular expression.

- Vulnerability: CVE-2021-32785

  – CVSS Score: 4.3
  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache ('OIDCCacheEncrypt off', 'OIDCSessionType server-cache', 'OIDCCacheType redis'), 'mod_auth_openidc' wrongly performed argument interpolation before passing Redis requests to 'hiredis', which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the 'hiredis' API. As a workaround, this vulnerability can be mitigated by setting 'OIDCCacheEncrypt' to 'on', as cache keys are cryptographically hashed before use when this option is enabled.

- Vulnerability: CVE-2020-9490

  – CVSS Score: 5
  – Description: Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2007-4723

  – CVSS Score: 7.5
  – Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2021-44790

  – CVSS Score: 7.5
  – Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

- Vulnerability: CVE-2020-13938

  – CVSS Score: 2.1
  – Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

- Vulnerability: CVE-2023-2650

  – CVSS Score: N/A

– Description: Issue summary: Processing some specially crafted ASN.1 object identifiers ordata containing them may be very slow.Impact summary: Applications that use OBJ_obj2txt() directly, or use any ofthe OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no messagesize limit may experience notable to very long delays when processing thosemessages, which may lead to a Denial of Service.An OBJECT IDENTIFIER is composed of a series of numbers – sub-identifiers –most of which have no size limit. OBJ_obj2txt() may be used to translatean ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSLtype ASN1_OBJECT) to its canonical numeric text form, which are thesub-identifiers of the OBJECT IDENTIFIER in decimal form, separated byperiods.When one of the sub-identifiers in the OBJECT IDENTIFIER is very large(these are sizes that are seen as absurdly large, taking up tens or hundredsof KiBs), the translation to a decimal number in text may take a very longtime. The time complexity is $O(n^2)$ with 'n' being the size of thesub-identifiers in bytes (*).With OpenSSL 3.0, support to fetch cryptographic algorithms using names /identifiers in string form was introduced. This includes using OBJECTIDENTIFIERs in canonical numeric text form as identifiers for fetchingalgorithms.Such OBJECT IDENTIFIERs may be received through the ASN.1 structureAlgorithmIdentifier, which is commonly used in multiple protocols to specifywhat cryptographic algorithm should be used to sign or verify, encrypt ordecrypt, or digest passed data.Applications that call OBJ_obj2txt() directly with untrusted data areaffected, with any version of OpenSSL. If the use is for the mere purposeof display, the severity is considered low.In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME,CMS, CMP/CRMF or TS. It also impacts anything that processes X.509certificates, including simple things like verifying its signature.The impact on TLS is relatively low, because all versions of OpenSSL have a100KiB limit on the peer's certificate chain. Additionally, this onlyimpacts clients, or servers that have explicitly enabled clientauthentication.In OpenSSL 1.1.1 and 1.0.2, this only affects displaying diverse objects,such as X.509 certificates. This is assumed to not happen in such a waythat it would cause a Denial of Service, so these versions are considerednot affected by this issue in such a way that it would be cause for concern,and the severity is therefore considered low.

• Vulnerability: CVE-2023-0215

  – CVSS Score: N/A

- Description: The public API function BIO_new_NDEF is a helper function used for
                 streamingASN.1 data via a BIO. It is primarily used internally to
                 OpenSSL to support theSMIME, CMS and PKCS7 streaming capabilities,
                 but may also be called directly byend user applications.The function
                 receives a BIO from the caller, prepends a new BIO_f_asn1 filterBIO
                 onto the front of it to form a BIO chain, and then returns the new
                 head ofthe BIO chain to the caller. Under certain conditions, for
                 example if a CMSrecipient public key is invalid, the new filter
                 BIO is freed and the functionreturns a NULL result indicating a
                 failure. However, in this case, the BIO chainis not properly
                 cleaned up and the BIO passed by the caller still retainsinternal
                 pointers to the previously freed filter BIO. If the caller then
                 goes onto call BIO_pop() on the BIO then a use-after-free will
                 occur. This will mostlikely result in a crash.This scenario occurs
                 directly in the internal function B64_write_ASN1() whichmay cause
                 BIO_new_NDEF() to be called and will subsequently call BIO_pop()
                 onthe BIO. This internal function is in turn called by the public
                 API functionsPEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream,
                 PEM_write_bio_PKCS7_stream,SMIME_write_ASN1, SMIME_write_CMS and
                 SMIME_write_PKCS7.Other public API functions that may be impacted
                 by this includei2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7,
                 i2d_CMS_bio_stream andi2d_PKCS7_bio_stream.The OpenSSL cms and smime
                 command line applications are similarly affected.

- Vulnerability: CVE-2020-35452

  - CVSS Score: 6.8
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted
                  Digest nonce can cause a stack overflow in mod_auth_digest. There
                  is no report of this overflow being exploitable, nor the Apache HTTP
                  Server team could create one, though some particular compiler and/or
                  compilation option might make it possible, with limited consequences
                  anyway due to the size (a single byte) and the value (zero byte) of
                  the overflow

- Vulnerability: CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory
                  area which could cause the process to crash. This issue affects
                  Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2020-1934

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use
                  uninitialized memory when proxying to a malicious FTP server.

- Vulnerability: CVE-2022-36760

  - CVSS Score: N/A
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request
                  Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server
                  allows an attacker to smuggle requests to the AJP server it forwards
                  requests to. This issue affects Apache HTTP Server Apache HTTP
                  Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-4304

  - CVSS Score: N/A

- Description: A timing based side channel exists in the OpenSSL RSA Decryption implementationwhich could be sufficient to recover a plaintext across a network in aBleichenbacher style attack. To achieve a successful decryption an attackerwould have to be able to send a very large number of trial messages fordecryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5,RSA-OEAP and RSASVE.For example, in a TLS connection, RSA is commonly used by a client to send anencrypted pre-master secret to the server. An attacker that had observed agenuine connection between a client and a server could use this flaw to sendtrial messages to the server and record the time taken to process them. After asufficiently large number of messages the attacker could recover the pre-mastersecret used for the original connection and thus be able to decrypt theapplication data sent over that connection.

- **Vulnerability: CVE-2019-9517**

  - CVSS Score: 7.8
  - Description: Some HTTP/2 implementations are vulnerable to unconstrained interal data buffering, potentially leading to a denial of service. The attacker opens the HTTP/2 window so the peer can send without constraint; however, they leave the TCP window closed so the peer cannot actually write (many of) the bytes on the wire. The attacker then sends a stream of requests for a large response object. Depending on how the servers queue the responses, this can consume excess memory, CPU, or both.

- **Vulnerability: CVE-2019-0217**

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.

- **Vulnerability: CVE-2019-0197**

  - CVSS Score: 4.9
  - Description: A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue.

- **Vulnerability: CVE-2019-0196**

  - CVSS Score: 5
  - Description: A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.

- **Vulnerability: CVE-2019-0190**

  - CVSS Score: 5
  - Description: A bug exists in the way mod_ssl handled client renegotiations. A remote attacker could send a carefully crafted request that would cause mod_ssl to enter a loop leading to a denial of service. This bug can be only triggered with Apache HTTP Server version 2.4.37 when using OpenSSL version 1.1.1 or later, due to an interaction in changes to handling of renegotiation attempts.

- Vulnerability: CVE-2021-33193

  - CVSS Score: 5
  - Description: A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.

- Vulnerability: CVE-2019-0211

  - CVSS Score: 7.2
  - Description: In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.

- Vulnerability: CVE-2019-17567

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

- Vulnerability: CVE-2022-31813

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

- Vulnerability: CVE-2012-4360

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2023-4807

  - CVSS Score: N/A

- Description: Issue summary: The POLY1305 MAC (message authentication code) implementationcontains a bug that might corrupt the internal state of applications on theWindows 64 platform when running on newer X86_64 processors supporting theAVX512-IFMA instructions.Impact summary: If in an application that uses the OpenSSL library an attackercan influence whether the POLY1305 MAC algorithm is used, the applicationstate might be corrupted with various application dependent consequences.The POLY1305 MAC (message authentication code) implementation in OpenSSL doesnot save the contents of non-volatile XMM registers on Windows 64 platformwhen calculating the MAC of data larger than 64 bytes. Before returning tothe caller all the XMM registers are set to zero rather than restoring theirprevious content. The vulnerable code is used only on newer x86_64 processorssupporting the AVX512-IFMA instructions.The consequences of this kind of internal application state corruption canbe various – from no consequences, if the calling application does notdepend on the contents of non-volatile XMM registers at all, to the worstconsequences, where the attacker could get complete control of the applicationprocess. However given the contents of the registers are just zeroized sothe attacker cannot put arbitrary values inside, the most likely consequence,if any, would be an incorrect result of some application dependentcalculations or a crash leading to a denial of service.The POLY1305 MAC algorithm is most frequently used as part of theCHACHA20-POLY1305 AEAD (authenticated encryption with associated data)algorithm. The most common usage of this AEAD cipher is with TLS protocolversions 1.2 and 1.3 and a malicious client can influence whether this AEADcipher is used by the server. This implies that server applications usingOpenSSL can be potentially impacted. However we are currently not aware ofany concrete application that would be affected by this issue therefore weconsider this a Low severity security issue.As a workaround the AVX512-IFMA instructions support can be disabled atruntime by setting the environment variable OPENSSL_ia32cap: OPENSSL_ia32cap=:~0x200000The FIPS provider is not affected by this issue.

- Vulnerability: CVE-2009-3767

  - CVSS Score: 4.3
  - Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other versions, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2021-26690

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service

- Vulnerability: CVE-2021-26691

  - CVSS Score: 7.5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow

- Vulnerability: CVE-2019-0220

- CVSS Score: 5
- Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.

- Vulnerability: CVE-2024-38477

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- Vulnerability: CVE-2021-39275

  - CVSS Score: 7.5
  - Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2018-17189

  - CVSS Score: 5
  - Description: In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 (mod_http2) connections.

- Vulnerability: CVE-2022-29404

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2006-20001

  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2020-11993

  - CVSS Score: 4.3
  - Description: Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2021-3711

  – CVSS Score: 7.5
  – Description: In order to decrypt SM2 encrypted data an application is expected to call the API function EVP_PKEY_decrypt(). Typically an application will call this function twice. The first time, on entry, the "out" parameter can be NULL and, on exit, the "outlen" parameter is populated with the buffer size required to hold the decrypted plaintext. The application can then allocate a sufficiently sized buffer and call EVP_PKEY_decrypt() again, but this time passing a non-NULL value for the "out" parameter. A bug in the implementation of the SM2 decryption code means that the calculation of the buffer size required to hold the plaintext returned by the first call to EVP_PKEY_decrypt() can be smaller than the actual size required by the second call. This can lead to a buffer overflow when EVP_PKEY_decrypt() is called by the application a second time with a buffer that is too small. A malicious attacker who is able present SM2 content for decryption to an application could cause attacker chosen data to overflow the buffer by up to a maximum of 62 bytes altering the contents of other data held after the buffer, possibly changing application behaviour or causing the application to crash. The location of the buffer is application dependent but is typically heap allocated. Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k).

- Vulnerability: CVE-2024-0727

  – CVSS Score: N/A
  – Description: Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSLto crash leading to a potential Denial of Service attackImpact summary: Applications loading files in the PKCS12 format from untrustedsources might terminate abruptly.A file in PKCS12 format can contain certificates and keys and may come from anuntrusted source. The PKCS12 specification allows certain fields to be NULL, butOpenSSL does not correctly check for this case. This can lead to a NULL pointerdereference that results in OpenSSL crashing. If an application processes PKCS12files from an untrusted source using the OpenSSL APIs then that application willbe vulnerable to this issue.OpenSSL APIs that are vulnerable to this are: PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a similar issue in SMIME_write_PKCS7(). However since thisfunction is related to writing data we do not consider it security significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.

- Vulnerability: CVE-2009-3766

  – CVSS Score: 6.8
  – Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when OpenSSL is used, does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

- Vulnerability: CVE-2021-44224

  – CVSS Score: 6.4

- Description: A crafted URI sent to httpd configured as a forward proxy
  (ProxyRequests on) can cause a crash (NULL pointer dereference) or,
  for configurations mixing forward and reverse proxy declarations, can
  allow for requests to be directed to a declared Unix Domain Socket
  endpoint (Server Side Request Forgery). This issue affects Apache
  HTTP Server 2.4.7 up to 2.4.51 (included).

- Vulnerability: CVE-2009-3765

  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does
    not properly handle a '\{}0' character in a domain name in the
    subject's Common Name (CN) field of an X.509 certificate, which
    allows man-in-the-middle attackers to spoof arbitrary SSL servers via
    a crafted certificate issued by a legitimate Certification Authority,
    a related issue to CVE-2009-2408.

- Vulnerability: CVE-2022-22721

  - CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than
    350MB (defaults to 1M) on 32 bit systems an integer overflow happens
    which later causes out of bounds writes. This issue affects Apache
    HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2022-22720

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound
    connection when errors are encountered discarding the request body,
    exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2019-10092

  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting
    issue was reported affecting the mod_proxy error page. An attacker
    could cause the link on the error page to be malformed and instead
    point to a page of their choice. This would only be exploitable
    where a server was set up with proxying enabled but was misconfigured
    in such a way that the Proxy Error page was displayed.

- Vulnerability: CVE-2021-3712

  - CVSS Score: 5.8

- Description: ASN.1 strings are represented internally within OpenSSL as an ASN1␣STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own "d2i" functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1␣STRING␣set() function will additionally NUL terminate the byte array in the ASN1␣STRING structure. However, it is possible for applications to directly construct valid ASN1␣STRING structures which do not NUL terminate the byte array by directly setting the "data" and "length" fields in the ASN1␣STRING array. This can also happen by using the ASN1␣STRING␣set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1␣STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1␣STRINGs that have been directly constructed by the application without NUL terminating the "data" field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1␣STRING structures). It can also occur in the X509␣get1␣email(), X509␣REQ␣get1␣email() and X509␣get1␣ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1␣STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y).

- Vulnerability: CVE-2023-0464

  - CVSS Score: N/A

  - Description: A security vulnerability has been identified in all supported versionsof OpenSSL related to the verification of X.509 certificate chainsthat include policy constraints. Attackers may be able to exploit thisvulnerability by creating a malicious certificate chain that triggersexponential use of computational resources, leading to a denial-of-service(DoS) attack on affected systems.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509␣VERIFY␣PARAM␣set1␣policies()' function.

- Vulnerability: CVE-2023-0465

  - CVSS Score: N/A

- Description: Applications that use a non-default option when verifying certificates may bevulnerable to an attack from a malicious CA to circumvent certain checks.Invalid certificate policies in leaf certificates are silently ignored byOpenSSL and other certificate policy checks are skipped for that certificate.A malicious CA could use this to deliberately assert invalid certificate policiesin order to circumvent policy checking on the certificate altogether.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.

- **Vulnerability: CVE-2023-0466**

  - CVSS Score: N/A
  - Description: The function X509_VERIFY_PARAM_add0_policy() is documented toimplicitly enable the certificate policy check when doing certificateverification. However the implementation of the function does notenable the check which allows certificates with invalid or incorrectpolicies to pass the certificate verification.As suddenly enabling the policy check could break existing deployments it wasdecided to keep the existing behavior of the X509_VERIFY_PARAM_add0_policy()function.Instead the applications that require OpenSSL to perform certificatepolicy check need to use X509_VERIFY_PARAM_set1_policies() or explicitlyenable the policy check by calling X509_VERIFY_PARAM_set_flags() withthe X509_V_FLAG_POLICY_CHECK flag argument.Certificate policy checks are disabled by default in OpenSSL and are notcommonly used by applications.

- **Vulnerability: CVE-2019-10098**

  - CVSS Score: 5.8
  - Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.

- **Vulnerability: CVE-2019-10097**

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4.32-2.4.39, when mod_remoteip was configured to use a trusted intermediary proxy server using the "PROXY" protocol, a specially crafted PROXY header could trigger a stack buffer overflow or NULL pointer deference. This vulnerability could only be triggered by a trusted proxy and not by untrusted HTTP clients.

- **Vulnerability: CVE-2021-40438**

  - CVSS Score: 6.8
  - Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

- **Vulnerability: CVE-2011-1176**

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2022-23943

  – CVSS Score: 7.5
  – Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

- Vulnerability: CVE-2018-17199

  – CVSS Score: 5
  – Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

- Vulnerability: CVE-2021-23841

  – CVSS Score: 4.3
  – Description: The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack. The function X509_issuer_and_serial_hash() is never directly called by OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on certificates that may have been obtained from untrusted sources. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2021-34798

  – CVSS Score: 5
  – Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2023-25690

  – CVSS Score: N/A
  – Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2020-11984

- CVSS Score: 7.5
- Description: Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE

- Vulnerability: CVE-2021-4160

  - CVSS Score: 4.3
  - Description: There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that is available to premium support customers only. It will be made available in 1.0.2zc when it is released. The issue only affects OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0). Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL 1.0.2zc-dev (Affected 1.0.2-1.0.2zb).

- Vulnerability: CVE-2022-26377

  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2019-10081

  - CVSS Score: 5
  - Description: HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example configured with "H2PushResource", could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client.

- Vulnerability: CVE-2019-10082

  - CVSS Score: 6.4
  - Description: In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.

- Vulnerability: CVE-2024-40898

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2023-27522

  – CVSS Score: N/A
  – Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via
    mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30
    through 2.4.55.Special characters in the origin response header can
    truncate/split the response forwarded to the client.

- Vulnerability: CVE-2022-0778

  – CVSS Score: 5
  – Description: The BN_mod_sqrt() function, which computes a modular square root,
    contains a bug that can cause it to loop forever for non-prime
    moduli. Internally this function is used when parsing certificates
    that contain elliptic curve public keys in compressed form or
    explicit elliptic curve parameters with a base point encoded in
    compressed form. It is possible to trigger the infinite loop by
    crafting a certificate that has invalid explicit curve parameters.
    Since certificate parsing happens prior to verification of the
    certificate signature, any process that parses an externally supplied
    certificate may thus be subject to a denial of service attack. The
    infinite loop can also be reached when parsing crafted private
    keys as they can contain explicit elliptic curve parameters. Thus
    vulnerable situations include: – TLS clients consuming server
    certificates – TLS servers consuming client certificates – Hosting
    providers taking certificates or private keys from customers
    – Certificate authorities parsing certification requests from
    subscribers – Anything else which parses ASN.1 elliptic curve
    parameters Also any other applications that use the BN_mod_sqrt()
    where the attacker can control the parameter values are vulnerable
    to this DoS issue. In the OpenSSL 1.0.2 version the public key is
    not parsed during initial parsing of the certificate which makes
    it slightly harder to trigger the infinite loop. However any
    operation which requires the public key from the certificate will
    trigger the infinite loop. In particular the attacker can use a
    self-signed certificate to trigger the loop during verification
    of the certificate signature. This issue affects OpenSSL versions
    1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n
    and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected
    3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m).
    Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

- Vulnerability: CVE-2022-2097

  – CVSS Score: 5
  – Description: AES OCB mode for 32-bit x86 platforms using the AES-NI assembly
    optimised implementation will not encrypt the entirety of the data
    under some circumstances. This could reveal sixteen bytes of data
    that was preexisting in the memory that wasn't written. In the
    special case of "in place" encryption, sixteen bytes of the plaintext
    would be revealed. Since OpenSSL does not support OCB based cipher
    suites for TLS and DTLS, they are both unaffected. Fixed in OpenSSL
    3.0.5 (Affected 3.0.0-3.0.4). Fixed in OpenSSL 1.1.1q (Affected
    1.1.1-1.1.1p).

- Vulnerability: CVE-2020-1971

  – CVSS Score: 4.3

– Description: The X.509 GeneralName type is a generic type for representing
                different types of names. One of those name types is known as
                EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which
                compares different instances of a GENERAL_NAME to see if they
                are equal or not. This function behaves incorrectly when both
                GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference
                and a crash may occur leading to a possible denial of service
                attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two
                purposes: 1) Comparing CRL distribution point names between an
                available CRL and a CRL distribution point embedded in an X509
                certificate 2) When verifying that a timestamp response token signer
                matches the timestamp authority name (exposed via the API functions
                TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can
                control both items being compared then that attacker could trigger
                a crash. For example if the attacker can trick a client or server
                into checking a malicious certificate against a malicious CRL then
                this may occur. Note that some applications automatically download
                CRLs based on a URL embedded in a certificate. This checking happens
                prior to the signatures on the certificate and CRL being verified.
                OpenSSL's s_server, s_client and verify tools have support for the
                "-crl_download" option which implements automatic CRL downloading and
                this attack has been demonstrated to work against those tools. Note
                that an unrelated bug means that affected versions of OpenSSL cannot
                parse or construct correct encodings of EDIPARTYNAME. However it is
                possible to construct a malformed EDIPARTYNAME that OpenSSL's parser
                will accept and hence trigger this attack. All OpenSSL 1.1.1 and
                1.0.2 versions are affected by this issue. Other OpenSSL releases
                are out of support and have not been checked. Fixed in OpenSSL
                1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected
                1.0.2-1.0.2w).

- Vulnerability: CVE-2009-1390

  – CVSS Score: 6.8

  – Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2)
                GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS
                certificate in the chain is accepted instead of verifying the entire
                chain, which allows remote attackers to spoof trusted servers via a
                man-in-the-middle attack.

- Vulnerability: CVE-2012-3526

  – CVSS Score: 5

  – Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the
                Apache HTTP Server allows remote attackers to cause a denial of
                service (server or application crash) via multiple X-Forwarded-For
                headers in a request.

- Vulnerability: CVE-2023-5678

  – CVSS Score: N/A

– Description: Issue summary: Generating excessively long X9.42 DH keys or checkingexcessively long X9.42 DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_generate_key() togenerate an X9.42 DH key may experience long delays. Likewise, applicationsthat use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check()to check an X9.42 DH key or X9.42 DH parameters may experience long delays.Where the key or parameters that are being checked have been obtained froman untrusted source this may lead to a Denial of Service.While DH_check() performs all the necessary checks (as of CVE-2023-3817),DH_check_pub_key() doesn't make any of these checks, and is thereforevulnerable for excessively large P and Q parameters.Likewise, while DH_generate_key() performs a check for an excessively largeP, it doesn't check for an excessively large Q.An application that calls DH_generate_key() or DH_check_pub_key() andsupplies a key or parameters obtained from an untrusted source could bevulnerable to a Denial of Service attack.DH_generate_key() and DH_check_pub_key() are also called by a number ofother OpenSSL functions. An application calling any of those otherfunctions may similarly be affected. The other functions affected by thisare DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate().Also vulnerable are the OpenSSL pkey command line application when using the"-pubcheck" option, as well as the OpenSSL genpkey command line application.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2009-2299

  – CVSS Score: 5

  – Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2022-1292

  – CVSS Score: 10

  – Description: The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n). Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).

- Vulnerability: CVE-2012-4001

  – CVSS Score: 5

  – Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2022-37436

  – CVSS Score: N/A

– Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause
                the response headers to be truncated early, resulting in some headers
                being incorporated into the response body. If the later headers have
                any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2021-23840

    – CVSS Score: 5

    – Description: Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate
                    may overflow the output length argument in some cases where the input
                    length is close to the maximum permissable length for an integer on
                    the platform. In such cases the return value from the function call
                    will be 1 (indicating success), but the output length value will be
                    negative. This could cause applications to behave incorrectly or
                    crash. OpenSSL versions 1.1.1i and below are affected by this issue.
                    Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL
                    versions 1.0.2x and below are affected by this issue. However
                    OpenSSL 1.0.2 is out of support and no longer receiving public
                    updates. Premium support customers of OpenSSL 1.0.2 should upgrade
                    to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL
                    1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected
                    1.0.2-1.0.2x).

- Vulnerability: CVE-2022-4450

    – CVSS Score: N/A

    – Description: The function PEM_read_bio_ex() reads a PEM file from a BIO and parses
                    anddecodes the "name" (e.g. "CERTIFICATE"), any header data and the
                    payload data.If the function succeeds then the "name_out", "header"
                    and "data" arguments arepopulated with pointers to buffers containing
                    the relevant decoded data. Thecaller is responsible for freeing
                    those buffers. It is possible to construct aPEM file that results
                    in 0 bytes of payload data. In this case PEM_read_bio_ex()will
                    return a failure code but will populate the header argument with
                    a pointerto a buffer that has already been freed. If the caller
                    also frees this bufferthen a double free will occur. This will
                    most likely lead to a crash. Thiscould be exploited by an attacker
                    who has the ability to supply malicious PEMfiles for parsing to
                    achieve a denial of service attack.The functions PEM_read_bio() and
                    PEM_read() are simple wrappers aroundPEM_read_bio_ex() and therefore
                    these functions are also directly affected.These functions are also
                    called indirectly by a number of other OpenSSLfunctions including
                    PEM_X509_INFO_read_bio_ex() andSSL_CTX_use_serverinfo_file() which are
                    also vulnerable. Some OpenSSL internaluses of these functions are
                    not vulnerable because the caller does not free theheader argument
                    if PEM_read_bio_ex() returns a failure code. These locationsinclude
                    the PEM_read_bio_TYPE() functions as well as the decoders introduced
                    inOpenSSL 3.0.The OpenSSL asn1parse command line application is also
                    impacted by this issue.

- Vulnerability: CVE-2013-2765

    – CVSS Score: 5

    – Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server
                    allows remote attackers to cause a denial of service (NULL pointer
                    dereference, process crash, and disk consumption) via a POST request
                    with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2011-2688

    – CVSS Score: 7.5

- Description: SQL injection vulnerability in mysql/mysql-auth.pl in the
  mod_authnz_external module 3.2.5 and earlier for the Apache HTTP
  Server allows remote attackers to execute arbitrary SQL commands
  via the user field.

- **Vulnerability:** CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5
    for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM
    Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows
    use an improper encryption algorithm and a weak key for maintaining
    the stored data of the node secret for the SecurID Authentication
    API, which allows local users to obtain sensitive information via
    cryptographic attacks on this data.

- **Vulnerability:** CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication
    Agent 7.1 before 7.1.1 for Web for Internet Information Services,
    and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to
    inject arbitrary web script or HTML via unspecified vectors.

- **Vulnerability:** CVE-2023-45802

  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a
    time window were the request's memory resources were not reclaimed
    immediately. Instead, de-allocation was deferred to connection
    close. A client could send new requests and resets, keeping the
    connection busy and open and causing the memory footprint to keep
    on growing. On connection close, all resources were reclaimed, but
    the process might run out of memory before that.This was found by
    the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset
    Exploit) with their own test client. During "normal" HTTP/2 use, the
    probability to hit this bug is very low. The kept memory would not
    become noticeable before the connection closes or times out.Users are
    recommended to upgrade to version 2.4.58, which fixes the issue.

- **Vulnerability:** CVE-2022-28615

  - CVSS Score: 6.4
  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose
    information due to a read beyond bounds in ap_strcmp_match() when
    provided with an extremely large input buffer. While no code
    distributed with the server can be coerced into such a call,
    third-party modules or lua scripts that use ap_strcmp_match() may
    hypothetically be affected.

- **Vulnerability:** CVE-2022-28614

  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier
    may read unintended memory if an attacker can cause the server to
    reflect very large input using ap_rwrite() or ap_rputs(), such as
    with mod_luas r:puts() function. Modules compiled and distributed
    separately from Apache HTTP Server that use the 'ap_rputs' function
    and may pass it a very large (INT_MAX or larger) string must be
    compiled against current headers to resolve the issue.

- **Vulnerability:** CVE-2019-0215

- CVSS Score: 6
- Description: In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in mod_ssl when using per-location client certificate verification with TLSv1.3 allowed a client to bypass configured access control restrictions.

- Vulnerability: CVE-2013-4365

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2022-28330

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2021-32791

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2021-32792

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.

- Vulnerability: CVE-2023-31122

  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2024-38476

  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-27316

  - CVSS Score: N/A
  - Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

- Vulnerability: CVE-2024-38474

    - CVSS Score: N/A
    - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server
      2.4.59 and earlier allows attacker to execute scripts indirectories
      permitted by the configuration but not directly reachable by anyURL
      or source disclosure of scripts meant to only to be executed as
      CGI.Users are recommended to upgrade to version 2.4.60, which fixes
      this issue.Some RewriteRules that capture and substitute unsafely
      will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2009-0796

    - CVSS Score: 2.6
    - Description: Cross-site scripting (XSS) vulnerability in Status.pm in
      Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the
      Apache HTTP Server, when /perl-status is accessible, allows remote
      attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2022-2068

    - CVSS Score: 10
    - Description: In addition to the c_rehash shell command injection identified in
      CVE-2022-1292, further circumstances where the c_rehash script
      does not properly sanitise shell metacharacters to prevent command
      injection were found by code review. When the CVE-2022-1292 was
      fixed it was not discovered that there are other places in the
      script where the file names of certificates being hashed were
      possibly passed to a command executed through the shell. This
      script is distributed by some operating systems in a manner where
      it is automatically executed. On such operating systems, an
      attacker could execute arbitrary commands with the privileges of
      the script. Use of the c_rehash script is considered obsolete and
      should be replaced by the OpenSSL rehash command line tool. Fixed in
      OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL
      1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected
      1.0.2-1.0.2ze).

- Vulnerability: CVE-2021-3449

    - CVSS Score: 4.3
    - Description: An OpenSSL TLS server may crash if sent a maliciously crafted
      renegotiation ClientHello message from a client. If a TLSv1.2
      renegotiation ClientHello omits the signature_algorithms extension
      (where it was present in the initial ClientHello), but includes a
      signature_algorithms_cert extension then a NULL pointer dereference
      will result, leading to a crash and a denial of service attack. A
      server is only vulnerable if it has TLSv1.2 and renegotiation enabled
      (which is the default configuration). OpenSSL TLS clients are not
      impacted by this issue. All OpenSSL 1.1.1 versions are affected
      by this issue. Users of these versions should upgrade to OpenSSL
      1.1.1k. OpenSSL 1.0.2 is not impacted by this issue. Fixed in
      OpenSSL 1.1.1k (Affected 1.1.1-1.1.1j).

- Vulnerability: CVE-2021-36160

    - CVSS Score: 5
    - Description: A carefully crafted request uri-path can cause mod_proxy_uwsgi to read
      above the allocated memory and crash (DoS). This issue affects Apache
      HTTP Server versions 2.4.30 to 2.4.48 (inclusive).

- Vulnerability: CVE-2020-1927

– CVSS Score: 5.8

– Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with
mod_rewrite that were intended to be self-referential might be fooled
by encoded newlines and redirect instead to an an unexpected URL
within the request URL.

- Vulnerability: CVE-2023-0286

– CVSS Score: N/A

– Description: There is a type confusion vulnerability relating to X.400 address
processinginside an X.509 GeneralName. X.400 addresses were
parsed as an ASN1_STRING butthe public structure definition for
GENERAL_NAME incorrectly specified the typeof the x400Address
field as ASN1_TYPE. This field is subsequently interpreted bythe
OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than
anASN1_STRING.When CRL checking is enabled (i.e. the application
sets theX509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an
attacker to passarbitrary pointers to a memcmp call, enabling them to
read memory contents orenact a denial of service. In most cases,
the attack requires the attacker toprovide both the certificate
chain and CRL, neither of which need to have avalid signature. If
the attacker only controls one of these inputs, the otherinput
must already contain an X.400 address as a CRL distribution point,
whichis uncommon. As such, this vulnerability is most likely to only
affectapplications which have implemented their own functionality for
retrieving CRLsover a network.

- Vulnerability: CVE-2023-3817

– CVSS Score: N/A

– Description: Issue summary: Checking excessively long DH keys or parameters may
be very slow.Impact summary: Applications that use the functions
DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH
key or DH parameters may experience longdelays. Where the key or
parameters that are being checked have been obtainedfrom an untrusted
source this may lead to a Denial of Service.The function DH_check()
performs various checks on DH parameters. After fixingCVE-2023-3446
it was discovered that a large q parameter value can also triggeran
overly long computation during some of these checks. A correct q
value,if present, cannot be larger than the modulus p parameter, thus
it isunnecessary to perform these checks if q is larger than p.An
application that calls DH_check() and supplies a key or parameters
obtainedfrom an untrusted source could be vulnerable to a Denial of
Service attack.The function DH_check() is itself called by a number
of other OpenSSL functions.An application calling any of those other
functions may similarly be affected.The other functions affected
by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable
are the OpenSSL dhparam and pkeyparam command line applicationswhen
using the "-check" option.The OpenSSL SSL/TLS implementation is not
affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not
affected by this issue.

- Vulnerability: CVE-2021-32786

– CVSS Score: 5.8

– Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, `oidc_validate_redirect_url()` does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring `mod_auth_openidc` to only allow redirection whose destination matches a given regular expression.

- Vulnerability: CVE-2021-32785

  – CVSS Score: 4.3

  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache (`OIDCCacheEncrypt off`, `OIDCSessionType server-cache`, `OIDCCacheType redis`), `mod_auth_openidc` wrongly performed argument interpolation before passing Redis requests to `hiredis`, which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the `hiredis` API. As a workaround, this vulnerability can be mitigated by setting `OIDCCacheEncrypt` to `on`, as cache keys are cryptographically hashed before use when this option is enabled.

- Vulnerability: CVE-2020-9490

  – CVSS Score: 5

  – Description: Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2007-4723

  – CVSS Score: 7.5

  – Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2021-44790

  – CVSS Score: 7.5

  – Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

- Vulnerability: CVE-2020-13938
    - CVSS Score: 2.1
    - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows
- Vulnerability: CVE-2023-2650
    - CVSS Score: N/A
    - Description: Issue summary: Processing some specially crafted ASN.1 object identifiers ordata containing them may be very slow.Impact summary: Applications that use OBJ_obj2txt() directly, or use any ofthe OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no messagesize limit may experience notable to very long delays when processing thosemessages, which may lead to a Denial of Service.An OBJECT IDENTIFIER is composed of a series of numbers - sub-identifiers -most of which have no size limit. OBJ_obj2txt() may be used to translatean ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSLtype ASN1_OBJECT) to its canonical numeric text form, which are thesub-identifiers of the OBJECT IDENTIFIER in decimal form, separated byperiods.When one of the sub-identifiers in the OBJECT IDENTIFIER is very large(these are sizes that are seen as absurdly large, taking up tens or hundredsof KiBs), the translation to a decimal number in text may take a very longtime. The time complexity is $O(n^2)$ with 'n' being the size of thesub-identifiers in bytes (*).With OpenSSL 3.0, support to fetch cryptographic algorithms using names /identifiers in string form was introduced. This includes using OBJECTIDENTIFIERs in canonical numeric text form as identifiers for fetchingalgorithms.Such OBJECT IDENTIFIERs may be received through the ASN.1 structureAlgorithmIdentifier, which is commonly used in multiple protocols to specifywhat cryptographic algorithm should be used to sign or verify, encrypt ordecrypt, or digest passed data.Applications that call OBJ_obj2txt() directly with untrusted data areaffected, with any version of OpenSSL. If the use is for the mere purposeof display, the severity is considered low.In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME,CMS, CMP/CRMF or TS. It also impacts anything that processes X.509certificates, including simple things like verifying its signature.The impact on TLS is relatively low, because all versions of OpenSSL have a100KiB limit on the peer's certificate chain. Additionally, this onlyimpacts clients, or servers that have explicitly enabled clientauthentication.In OpenSSL 1.1.1 and 1.0.2, this only affects displaying diverse objects,such as X.509 certificates. This is assumed to not happen in such a waythat it would cause a Denial of Service, so these versions are considerednot affected by this issue in such a way that it would be cause for concern,and the severity is therefore considered low.
- Vulnerability: CVE-2023-0215
    - CVSS Score: N/A

– Description: The public API function BIO_new_NDEF is a helper function used for streamingASN.1 data via a BIO. It is primarily used internally to OpenSSL to support theSMIME, CMS and PKCS7 streaming capabilities, but may also be called directly byend user applications.The function receives a BIO from the caller, prepends a new BIO_f_asn1 filterBIO onto the front of it to form a BIO chain, and then returns the new head ofthe BIO chain to the caller. Under certain conditions, for example if a CMSrecipient public key is invalid, the new filter BIO is freed and the functionreturns a NULL result indicating a failure. However, in this case, the BIO chainis not properly cleaned up and the BIO passed by the caller still retainsinternal pointers to the previously freed filter BIO. If the caller then goes onto call BIO_pop() on the BIO then a use-after-free will occur. This will mostlikely result in a crash.This scenario occurs directly in the internal function B64_write_ASN1() whichmay cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() onthe BIO. This internal function is in turn called by the public API functionsPEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream,SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7.Other public API functions that may be impacted by this includei2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream andi2d_PKCS7_bio_stream.The OpenSSL cms and smime command line applications are similarly affected.

- Vulnerability: CVE-2020-35452

    – CVSS Score: 6.8
    – Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

- Vulnerability: CVE-2022-22719

    – CVSS Score: 5
    – Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2020-1934

    – CVSS Score: 5
    – Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

- Vulnerability: CVE-2022-36760

    – CVSS Score: N/A
    – Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-4304

    – CVSS Score: N/A

– Description: A timing based side channel exists in the OpenSSL RSA Decryption implementationwhich could be sufficient to recover a plaintext across a network in aBleichenbacher style attack. To achieve a successful decryption an attackerwould have to be able to send a very large number of trial messages fordecryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5,RSA-OEAP and RSASVE.For example, in a TLS connection, RSA is commonly used by a client to send anencrypted pre-master secret to the server. An attacker that had observed agenuine connection between a client and a server could use this flaw to sendtrial messages to the server and record the time taken to process them. After asufficiently large number of messages the attacker could recover the pre-mastersecret used for the original connection and thus be able to decrypt theapplication data sent over that connection.

- Vulnerability: CVE-2019-9517

  – CVSS Score: 7.8
  – Description: Some HTTP/2 implementations are vulnerable to unconstrained interal data buffering, potentially leading to a denial of service. The attacker opens the HTTP/2 window so the peer can send without constraint; however, they leave the TCP window closed so the peer cannot actually write (many of) the bytes on the wire. The attacker then sends a stream of requests for a large response object. Depending on how the servers queue the responses, this can consume excess memory, CPU, or both.

- Vulnerability: CVE-2019-0217

  – CVSS Score: 6
  – Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.

- Vulnerability: CVE-2019-0197

  – CVSS Score: 4.9
  – Description: A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue.

- Vulnerability: CVE-2019-0196

  – CVSS Score: 5
  – Description: A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.

- Vulnerability: CVE-2019-0190

  – CVSS Score: 5
  – Description: A bug exists in the way mod_ssl handled client renegotiations. A remote attacker could send a carefully crafted request that would cause mod_ssl to enter a loop leading to a denial of service. This bug can be only triggered with Apache HTTP Server version 2.4.37 when using OpenSSL version 1.1.1 or later, due to an interaction in changes to handling of renegotiation attempts.

- Vulnerability: CVE-2021-33193

  - CVSS Score: 5
  - Description: A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.

- Vulnerability: CVE-2019-0211

  - CVSS Score: 7.2
  - Description: In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.

- Vulnerability: CVE-2019-17567

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

- Vulnerability: CVE-2022-31813

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

- Vulnerability: CVE-2012-4360

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2023-4807

  - CVSS Score: N/A

- Description: Issue summary: The POLY1305 MAC (message authentication code) implementationcontains a bug that might corrupt the internal state of applications on theWindows 64 platform when running on newer X86_64 processors supporting theAVX512-IFMA instructions.Impact summary: If in an application that uses the OpenSSL library an attackercan influence whether the POLY1305 MAC algorithm is used, the applicationstate might be corrupted with various application dependent consequences.The POLY1305 MAC (message authentication code) implementation in OpenSSL doesnot save the contents of non-volatile XMM registers on Windows 64 platformwhen calculating the MAC of data larger than 64 bytes. Before returning tothe caller all the XMM registers are set to zero rather than restoring theirprevious content. The vulnerable code is used only on newer x86_64 processorssupporting the AVX512-IFMA instructions.The consequences of this kind of internal application state corruption canbe various – from no consequences, if the calling application does notdepend on the contents of non-volatile XMM registers at all, to the worstconsequences, where the attacker could get complete control of the applicationprocess. However given the contents of the registers are just zeroized sothe attacker cannot put arbitrary values inside, the most likely consequence,if any, would be an incorrect result of some application dependentcalculations or a crash leading to a denial of service.The POLY1305 MAC algorithm is most frequently used as part of theCHACHA20-POLY1305 AEAD (authenticated encryption with associated data)algorithm. The most common usage of this AEAD cipher is with TLS protocolversions 1.2 and 1.3 and a malicious client can influence whether this AEADcipher is used by the server. This implies that server applications usingOpenSSL can be potentially impacted. However we are currently not aware ofany concrete application that would be affected by this issue therefore weconsider this a Low severity security issue.As a workaround the AVX512-IFMA instructions support can be disabled atruntime by setting the environment variable OPENSSL_ia32cap: OPENSSL_ia32cap=:~0x200000The FIPS provider is not affected by this issue.

- Vulnerability: CVE-2009-3767

  - CVSS Score: 4.3
  - Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other versions, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2021-26690

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service

- Vulnerability: CVE-2021-26691

  - CVSS Score: 7.5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow

- Vulnerability: CVE-2019-0220

- – CVSS Score: 5
- – Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.

- Vulnerability: CVE-2024-38477

  - – CVSS Score: N/A
  - – Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2022-30556

  - – CVSS Score: 5
  - – Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- Vulnerability: CVE-2021-39275

  - – CVSS Score: 7.5
  - – Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2018-17189

  - – CVSS Score: 5
  - – Description: In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 (mod_http2) connections.

- Vulnerability: CVE-2022-29404

  - – CVSS Score: 5
  - – Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2006-20001

  - – CVSS Score: N/A
  - – Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2020-11993

  - – CVSS Score: 4.3
  - – Description: Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2021-3711

  - CVSS Score: 7.5
  - Description: In order to decrypt SM2 encrypted data an application is expected to
                  call the API function EVP_PKEY_decrypt(). Typically an application
                  will call this function twice. The first time, on entry, the
                  "out" parameter can be NULL and, on exit, the "outlen" parameter
                  is populated with the buffer size required to hold the decrypted
                  plaintext. The application can then allocate a sufficiently sized
                  buffer and call EVP_PKEY_decrypt() again, but this time passing a
                  non-NULL value for the "out" parameter. A bug in the implementation
                  of the SM2 decryption code means that the calculation of the buffer
                  size required to hold the plaintext returned by the first call to
                  EVP_PKEY_decrypt() can be smaller than the actual size required
                  by the second call. This can lead to a buffer overflow when
                  EVP_PKEY_decrypt() is called by the application a second time with
                  a buffer that is too small. A malicious attacker who is able present
                  SM2 content for decryption to an application could cause attacker
                  chosen data to overflow the buffer by up to a maximum of 62 bytes
                  altering the contents of other data held after the buffer, possibly
                  changing application behaviour or causing the application to crash.
                  The location of the buffer is application dependent but is typically
                  heap allocated. Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k).

- Vulnerability: CVE-2024-0727

  - CVSS Score: N/A
  - Description: Issue summary: Processing a maliciously formatted PKCS12 file
                  may lead OpenSSLto crash leading to a potential Denial of Service
                  attackImpact summary: Applications loading files in the PKCS12
                  format from untrustedsources might terminate abruptly.A file in
                  PKCS12 format can contain certificates and keys and may come from
                  anuntrusted source. The PKCS12 specification allows certain fields
                  to be NULL, butOpenSSL does not correctly check for this case.
                  This can lead to a NULL pointerdereference that results in OpenSSL
                  crashing. If an application processes PKCS12files from an untrusted
                  source using the OpenSSL APIs then that application willbe vulnerable
                  to this issue.OpenSSL APIs that are vulnerable to this are:
                  PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(),
                  PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a
                  similar issue in SMIME_write_PKCS7(). However since thisfunction
                  is related to writing data we do not consider it security
                  significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected
                  by this issue.

- Vulnerability: CVE-2009-3766

  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when
                  OpenSSL is used, does not verify the domain name in the subject's
                  Common Name (CN) field of an X.509 certificate, which allows
                  man-in-the-middle attackers to spoof SSL servers via an arbitrary
                  valid certificate.

- Vulnerability: CVE-2021-44224

  - CVSS Score: 6.4

- Description: A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).

- Vulnerability: CVE-2009-3765

  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2022-22721

  - CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2022-22720

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2019-10092

  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

- Vulnerability: CVE-2021-3712

  - CVSS Score: 5.8

– Description: ASN.1 strings are represented internally within OpenSSL as an
    ASN1␣STRING structure which contains a buffer holding the string
    data and a field holding the buffer length. This contrasts with
    normal C strings which are repesented as a buffer for the string
    data which is terminated with a NUL (0) byte. Although not a
    strict requirement, ASN.1 strings that are parsed using OpenSSL's
    own "d2i" functions (and other similar parsing functions) as well
    as any string whose value has been set with the ASN1␣STRING␣set()
    function will additionally NUL terminate the byte array in the
    ASN1␣STRING structure. However, it is possible for applications
    to directly construct valid ASN1␣STRING structures which do not NUL
    terminate the byte array by directly setting the "data" and "length"
    fields in the ASN1␣STRING array. This can also happen by using
    the ASN1␣STRING␣set0() function. Numerous OpenSSL functions that
    print ASN.1 data have been found to assume that the ASN1␣STRING byte
    array will be NUL terminated, even though this is not guaranteed for
    strings that have been directly constructed. Where an application
    requests an ASN.1 structure to be printed, and where that ASN.1
    structure contains ASN1␣STRINGs that have been directly constructed
    by the application without NUL terminating the "data" field, then
    a read buffer overrun can occur. The same thing can also occur
    during name constraints processing of certificates (for example
    if a certificate has been directly constructed by the application
    instead of loading it via the OpenSSL parsing functions, and the
    certificate contains non NUL terminated ASN1␣STRING structures).
    It can also occur in the X509␣get1␣email(), X509␣REQ␣get1␣email()
    and X509␣get1␣ocsp() functions. If a malicious actor can cause an
    application to directly construct an ASN1␣STRING and then process it
    through one of the affected OpenSSL functions then this issue could
    be hit. This might result in a crash (causing a Denial of Service
    attack). It could also result in the disclosure of private memory
    contents (such as private keys, or sensitive plaintext). Fixed in
    OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za
    (Affected 1.0.2-1.0.2y).

- Vulnerability: CVE-2023-0464

  – CVSS Score: N/A

  – Description: A security vulnerability has been identified in all supported
    versionsof OpenSSL related to the verification of X.509 certificate
    chainsthat include policy constraints. Attackers may be able to
    exploit thisvulnerability by creating a malicious certificate chain
    that triggersexponential use of computational resources, leading
    to a denial-of-service(DoS) attack on affected systems.Policy
    processing is disabled by default but can be enabled by passingthe
    '-policy' argument to the command line utilities or by calling
    the'X509␣VERIFY␣PARAM␣set1␣policies()' function.

- Vulnerability: CVE-2023-0465

  – CVSS Score: N/A

- Description: Applications that use a non-default option when verifying
  certificates may bevulnerable to an attack from a malicious CA
  to circumvent certain checks.Invalid certificate policies in leaf
  certificates are silently ignored byOpenSSL and other certificate
  policy checks are skipped for that certificate.A malicious CA could
  use this to deliberately assert invalid certificate policiesin order
  to circumvent policy checking on the certificate altogether.Policy
  processing is disabled by default but can be enabled by passingthe
  '-policy' argument to the command line utilities or by calling
  the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0466

  - CVSS Score: N/A
  - Description: The function X509_VERIFY_PARAM_add0_policy() is documented
    toimplicitly enable the certificate policy check when doing
    certificateverification. However the implementation of the
    function does notenable the check which allows certificates
    with invalid or incorrectpolicies to pass the certificate
    verification.As suddenly enabling the policy check could break
    existing deployments it wasdecided to keep the existing behavior of
    the X509_VERIFY_PARAM_add0_policy()function.Instead the applications
    that require OpenSSL to perform certificatepolicy check need
    to use X509_VERIFY_PARAM_set1_policies() or explicitlyenable the
    policy check by calling X509_VERIFY_PARAM_set_flags() withthe
    X509_V_FLAG_POLICY_CHECK flag argument.Certificate policy checks
    are disabled by default in OpenSSL and are notcommonly used by
    applications.

- Vulnerability: CVE-2019-10098

  - CVSS Score: 5.8
  - Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with
    mod_rewrite that were intended to be self-referential might be fooled
    by encoded newlines and redirect instead to an unexpected URL within
    the request URL.

- Vulnerability: CVE-2019-10097

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4.32-2.4.39, when mod_remoteip was configured
    to use a trusted intermediary proxy server using the "PROXY"
    protocol, a specially crafted PROXY header could trigger a stack
    buffer overflow or NULL pointer deference. This vulnerability
    could only be triggered by a trusted proxy and not by untrusted HTTP
    clients.

- Vulnerability: CVE-2021-40438

  - CVSS Score: 6.8
  - Description: A crafted request uri-path can cause mod_proxy to forward the request
    to an origin server choosen by the remote user. This issue affects
    Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk
    Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP
    Server does not properly handle certain configuration sections that
    specify NiceValue but not AssignUserID, which might allow remote
    attackers to gain privileges by leveraging the root uid and root gid
    of an mpm-itk process.

- Vulnerability: CVE-2022-23943

  – CVSS Score: 7.5

  – Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

- Vulnerability: CVE-2018-17199

  – CVSS Score: 5

  – Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

- Vulnerability: CVE-2021-23841

  – CVSS Score: 4.3

  – Description: The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack. The function X509_issuer_and_serial_hash() is never directly called by OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on certificates that may have been obtained from untrusted sources. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2021-34798

  – CVSS Score: 5

  – Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2023-25690

  – CVSS Score: N/A

  – Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2020-11984

- CVSS Score: 7.5
- Description: Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE

- **Vulnerability: CVE-2021-4160**

  - CVSS Score: 4.3
  - Description: There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that is available to premium support customers only. It will be made available in 1.0.2zc when it is released. The issue only affects OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0). Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL 1.0.2zc-dev (Affected 1.0.2-1.0.2zb).

- **Vulnerability: CVE-2022-26377**

  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- **Vulnerability: CVE-2019-10081**

  - CVSS Score: 5
  - Description: HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example configured with "H2PushResource", could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client.

- **Vulnerability: CVE-2019-10082**

  - CVSS Score: 6.4
  - Description: In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.

- **Vulnerability: CVE-2024-40898**

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2023-27522

  – CVSS Score: N/A

  – Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.Special characters in the origin response header can truncate/split the response forwarded to the client.

- Vulnerability: CVE-2022-0778

  – CVSS Score: 5

  – Description: The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - TLS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

- Vulnerability: CVE-2022-2097

  – CVSS Score: 5

  – Description: AES OCB mode for 32-bit x86 platforms using the AES-NI assembly optimised implementation will not encrypt the entirety of the data under some circumstances. This could reveal sixteen bytes of data that was preexisting in the memory that wasn't written. In the special case of "in place" encryption, sixteen bytes of the plaintext would be revealed. Since OpenSSL does not support OCB based cipher suites for TLS and DTLS, they are both unaffected. Fixed in OpenSSL 3.0.5 (Affected 3.0.0-3.0.4). Fixed in OpenSSL 1.1.1q (Affected 1.1.1-1.1.1p).

- Vulnerability: CVE-2020-1971

  – CVSS Score: 4.3

– Description: The X.509 GeneralName type is a generic type for representing
               different types of names. One of those name types is known as
               EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which
               compares different instances of a GENERAL_NAME to see if they
               are equal or not. This function behaves incorrectly when both
               GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference
               and a crash may occur leading to a possible denial of service
               attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two
               purposes: 1) Comparing CRL distribution point names between an
               available CRL and a CRL distribution point embedded in an X509
               certificate 2) When verifying that a timestamp response token signer
               matches the timestamp authority name (exposed via the API functions
               TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can
               control both items being compared then that attacker could trigger
               a crash. For example if the attacker can trick a client or server
               into checking a malicious certificate against a malicious CRL then
               this may occur. Note that some applications automatically download
               CRLs based on a URL embedded in a certificate. This checking happens
               prior to the signatures on the certificate and CRL being verified.
               OpenSSL's s_server, s_client and verify tools have support for the
               "-crl_download" option which implements automatic CRL downloading and
               this attack has been demonstrated to work against those tools. Note
               that an unrelated bug means that affected versions of OpenSSL cannot
               parse or construct correct encodings of EDIPARTYNAME. However it is
               possible to construct a malformed EDIPARTYNAME that OpenSSL's parser
               will accept and hence trigger this attack. All OpenSSL 1.1.1 and
               1.0.2 versions are affected by this issue. Other OpenSSL releases
               are out of support and have not been checked. Fixed in OpenSSL
               1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected
               1.0.2-1.0.2w).

- Vulnerability: CVE-2009-1390

  – CVSS Score: 6.8

  – Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2)
               GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS
               certificate in the chain is accepted instead of verifying the entire
               chain, which allows remote attackers to spoof trusted servers via a
               man-in-the-middle attack.

- Vulnerability: CVE-2012-3526

  – CVSS Score: 5

  – Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the
               Apache HTTP Server allows remote attackers to cause a denial of
               service (server or application crash) via multiple X-Forwarded-For
               headers in a request.

- Vulnerability: CVE-2023-5678

  – CVSS Score: N/A

- Description: Issue summary: Generating excessively long X9.42 DH keys or checkingexcessively long X9.42 DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_generate_key() togenerate an X9.42 DH key may experience long delays. Likewise, applicationsthat use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check()to check an X9.42 DH key or X9.42 DH parameters may experience long delays.Where the key or parameters that are being checked have been obtained froman untrusted source this may lead to a Denial of Service.While DH_check() performs all the necessary checks (as of CVE-2023-3817),DH_check_pub_key() doesn't make any of these checks, and is thereforevulnerable for excessively large P and Q parameters.Likewise, while DH_generate_key() performs a check for an excessively largeP, it doesn't check for an excessively large Q.An application that calls DH_generate_key() or DH_check_pub_key() andsupplies a key or parameters obtained from an untrusted source could bevulnerable to a Denial of Service attack.DH_generate_key() and DH_check_pub_key() are also called by a number ofother OpenSSL functions. An application calling any of those otherfunctions may similarly be affected. The other functions affected by thisare DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate().Also vulnerable are the OpenSSL pkey command line application when using the"-pubcheck" option, as well as the OpenSSL genpkey command line application.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- **Vulnerability: CVE-2009-2299**

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- **Vulnerability: CVE-2022-1292**

  - CVSS Score: 10
  - Description: The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n). Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).

- **Vulnerability: CVE-2012-4001**

  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- **Vulnerability: CVE-2022-37436**

  - CVSS Score: N/A

– Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

• Vulnerability: CVE-2021-23840

  – CVSS Score: 5

  – Description: Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissable length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

• Vulnerability: CVE-2022-4450

  – CVSS Score: N/A

  – Description: The function PEM_read_bio_ex() reads a PEM file from a BIO and parses anddecodes the "name" (e.g. "CERTIFICATE"), any header data and the payload data.If the function succeeds then the "name_out", "header" and "data" arguments arepopulated with pointers to buffers containing the relevant decoded data. Thecaller is responsible for freeing those buffers. It is possible to construct aPEM file that results in 0 bytes of payload data. In this case PEM_read_bio_ex()will return a failure code but will populate the header argument with a pointerto a buffer that has already been freed. If the caller also frees this bufferthen a double free will occur. This will most likely lead to a crash. Thiscould be exploited by an attacker who has the ability to supply malicious PEMfiles for parsing to achieve a denial of service attack.The functions PEM_read_bio() and PEM_read() are simple wrappers aroundPEM_read_bio_ex() and therefore these functions are also directly affected.These functions are also called indirectly by a number of other OpenSSLfunctions including PEM_X509_INFO_read_bio_ex() andSSL_CTX_use_serverinfo_file() which are also vulnerable. Some OpenSSL internaluses of these functions are not vulnerable because the caller does not free theheader argument if PEM_read_bio_ex() returns a failure code. These locationsinclude the PEM_read_bio_TYPE() functions as well as the decoders introduced inOpenSSL 3.0.The OpenSSL asn1parse command line application is also impacted by this issue.

• Vulnerability: CVE-2013-2765

  – CVSS Score: 5

  – Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

• Vulnerability: CVE-2011-2688

  – CVSS Score: 7.5

- Description: SQL injection vulnerability in mysql/mysql-auth.pl in the
  mod_authnz_external module 3.2.5 and earlier for the Apache HTTP
  Server allows remote attackers to execute arbitrary SQL commands
  via the user field.

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5
    for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM
    Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows
    use an improper encryption algorithm and a weak key for maintaining
    the stored data of the node secret for the SecurID Authentication
    API, which allows local users to obtain sensitive information via
    cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication
    Agent 7.1 before 7.1.1 for Web for Internet Information Services,
    and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to
    inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2023-45802

  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a
    time window were the request's memory resources were not reclaimed
    immediately. Instead, de-allocation was deferred to connection
    close. A client could send new requests and resets, keeping the
    connection busy and open and causing the memory footprint to keep
    on growing. On connection close, all resources were reclaimed, but
    the process might run out of memory before that.This was found by
    the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset
    Exploit) with their own test client. During "normal" HTTP/2 use, the
    probability to hit this bug is very low. The kept memory would not
    become noticeable before the connection closes or times out.Users are
    recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-28615

  - CVSS Score: 6.4
  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose
    information due to a read beyond bounds in ap_strcmp_match() when
    provided with an extremely large input buffer. While no code
    distributed with the server can be coerced into such a call,
    third-party modules or lua scripts that use ap_strcmp_match() may
    hypothetically be affected.

- Vulnerability: CVE-2022-28614

  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier
    may read unintended memory if an attacker can cause the server to
    reflect very large input using ap_rwrite() or ap_rputs(), such as
    with mod_luas r:puts() function. Modules compiled and distributed
    separately from Apache HTTP Server that use the 'ap_rputs' function
    and may pass it a very large (INT_MAX or larger) string must be
    compiled against current headers to resolve the issue.

11.10 IP Address: 159.149.53.140

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 4

- High Vulnerabilities: 22

- Medium Vulnerabilities: 164

- Low Vulnerabilities: 16

- Total Vulnerabilities: 206

Services Running on IP Address

- Service: Apache httpd

    - Port: 80
    - Version: 2.4.6
    - Location: https://unimi.it/

- Service: Apache httpd

    - Port: 443
    - Version: 2.4.6
    - Location: https://www.unimi.it//

Vulnerabilities Found

- Vulnerability: CVE-2014-0117

    - CVSS Score: 4.3
    - Description: The mod_proxy module in the Apache HTTP Server 2.4.x before 2.4.10, when a reverse proxy is enabled, allows remote attackers to cause a denial of service (child-process crash) via a crafted HTTP Connection header.

- Vulnerability: CVE-2017-7679

    - CVSS Score: 7.5
    - Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

- Vulnerability: CVE-2017-9798

    - CVSS Score: 5
    - Description: Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.

- Vulnerability: CVE-2015-3185

    - CVSS Score: 4.3

- Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

- Vulnerability: CVE-2015-3184

  - CVSS Score: 5
  - Description: mod_authz_svn in Apache Subversion 1.7.x before 1.7.21 and 1.8.x before 1.8.14, when using Apache httpd 2.4.x, does not properly restrict anonymous access, which allows remote anonymous users to read hidden files via the path name.

- Vulnerability: CVE-2015-3183

  - CVSS Score: 5
  - Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

- Vulnerability: CVE-2013-4365

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2018-5407

  - CVSS Score: 1.9
  - Description: Simultaneous Multi-threading (SMT) in processors can enable local users to exploit software vulnerable to timing attacks via a side-channel timing attack on 'port contention'.

- Vulnerability: CVE-2022-28330

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2021-32791

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2021-32792

  - CVSS Score: 4.3

- Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.

- Vulnerability: CVE-2024-38476

  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-38477

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2023-31122

  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2009-0796

  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2022-2068

  - CVSS Score: 10
  - Description: In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze).

- Vulnerability: CVE-2014-0118

  - CVSS Score: 4.3
  - Description: The deflate_in_filter function in mod_deflate.c in the mod_deflate module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.

- Vulnerability: CVE-2013-6438

    - CVSS Score: 5
    - Description: The dav_xml_get_cdata function in main/util.c in the mod_dav module
                    in the Apache HTTP Server before 2.4.8 does not properly remove
                    whitespace characters from CDATA sections, which allows remote
                    attackers to cause a denial of service (daemon crash) via a crafted
                    DAV WRITE request.

- Vulnerability: CVE-2020-1927

    - CVSS Score: 5.8
    - Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with
                    mod_rewrite that were intended to be self-referential might be fooled
                    by encoded newlines and redirect instead to an an unexpected URL
                    within the request URL.

- Vulnerability: CVE-2023-0286

    - CVSS Score: N/A
    - Description: There is a type confusion vulnerability relating to X.400 address
                    processinginside an X.509 GeneralName. X.400 addresses were
                    parsed as an ASN1_STRING butthe public structure definition for
                    GENERAL_NAME incorrectly specified the typeof the x400Address
                    field as ASN1_TYPE. This field is subsequently interpreted bythe
                    OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than
                    anASN1_STRING.When CRL checking is enabled (i.e. the application
                    sets theX509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an
                    attacker to passarbitrary pointers to a memcmp call, enabling them to
                    read memory contents orenact a denial of service. In most cases,
                    the attack requires the attacker toprovide both the certificate
                    chain and CRL, neither of which need to have avalid signature. If
                    the attacker only controls one of these inputs, the otherinput
                    must already contain an X.400 address as a CRL distribution point,
                    whichis uncommon. As such, this vulnerability is most likely to only
                    affectapplications which have implemented their own functionality for
                    retrieving CRLsover a network.

- Vulnerability: CVE-2023-3817

    - CVSS Score: N/A
    - Description: Issue summary: Checking excessively long DH keys or parameters may
                    be very slow.Impact summary: Applications that use the functions
                    DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH
                    key or DH parameters may experience longdelays. Where the key or
                    parameters that are being checked have been obtainedfrom an untrusted
                    source this may lead to a Denial of Service.The function DH_check()
                    performs various checks on DH parameters. After fixingCVE-2023-3446
                    it was discovered that a large q parameter value can also triggeran
                    overly long computation during some of these checks. A correct q
                    value,if present, cannot be larger than the modulus p parameter, thus
                    it isunnecessary to perform these checks if q is larger than p.An
                    application that calls DH_check() and supplies a key or parameters
                    obtainedfrom an untrusted source could be vulnerable to a Denial of
                    Service attack.The function DH_check() is itself called by a number
                    of other OpenSSL functions.An application calling any of those other
                    functions may similarly be affected.The other functions affected
                    by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable
                    are the OpenSSL dhparam and pkeyparam command line applicationswhen
                    using the "-check" option.The OpenSSL SSL/TLS implementation is not
                    affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not
                    affected by this issue.

- Vulnerability: CVE-2017-3167

  - CVSS Score: 7.5
  - Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use
    of the ap_get_basic_auth_pw() by third-party modules outside of the
    authentication phase may lead to authentication requirements being
    bypassed.

- Vulnerability: CVE-2021-32786

  - CVSS Score: 5.8
  - Description: mod_auth_openidc is an authentication/authorization module for the
    Apache 2.x HTTP server that functions as an OpenID Connect Relying
    Party, authenticating users against an OpenID Connect Provider. In
    versions prior to 2.4.9, 'oidc_validate_redirect_url()' does not parse
    URLs the same way as most browsers do. As a result, this function
    can be bypassed and leads to an Open Redirect vulnerability in the
    logout functionality. This bug has been fixed in version 2.4.9
    by replacing any backslash of the URL to redirect with slashes
    to address a particular breaking change between the different
    specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this
    vulnerability can be mitigated by configuring 'mod_auth_openidc' to
    only allow redirection whose destination matches a given regular
    expression.

- Vulnerability: CVE-2021-32785

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the
    Apache 2.x HTTP server that functions as an OpenID Connect Relying
    Party, authenticating users against an OpenID Connect Provider. When
    mod_auth_openidc versions prior to 2.4.9 are configured to use an
    unencrypted Redis cache ('OIDCCacheEncrypt off', 'OIDCSessionType
    server-cache', 'OIDCCacheType redis'), 'mod_auth_openidc' wrongly
    performed argument interpolation before passing Redis requests to
    'hiredis', which would perform it again and lead to an uncontrolled
    format string bug. Initial assessment shows that this bug does
    not appear to allow gaining arbitrary code execution, but can
    reliably provoke a denial of service by repeatedly crashing the
    Apache workers. This bug has been corrected in version 2.4.9 by
    performing argument interpolation only once, using the 'hiredis'
    API. As a workaround, this vulnerability can be mitigated by setting
    'OIDCCacheEncrypt' to 'on', as cache keys are cryptographically
    hashed before use when this option is enabled.

- Vulnerability: CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel
    4.3.4a, when the Apache HTTP Server is used, allows remote attackers
    to bypass authentication via directory traversal sequences in a URI
    that ends with the name of a publicly available page, as demonstrated
    by a "/...../" sequence and an account_manage.php/login.php final
    component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2021-44790

  - CVSS Score: 7.5
  - Description: A carefully crafted request body can cause a buffer overflow in the
    mod_lua multipart parser (r:parsebody() called from Lua scripts).
    The Apache httpd team is not aware of an exploit for the vulnerabilty
    though it might be possible to craft one. This issue affects Apache
    HTTP Server 2.4.51 and earlier.

- Vulnerability: CVE-2016-4975

  – CVSS Score: 4.3
  – Description: Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).

- Vulnerability: CVE-2020-13938

  – CVSS Score: 2.1
  – Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

- Vulnerability: CVE-2023-2650

  – CVSS Score: N/A
  – Description: Issue summary: Processing some specially crafted ASN.1 object identifiers ordata containing them may be very slow.Impact summary: Applications that use OBJ_obj2txt() directly, or use any ofthe OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no messagesize limit may experience notable to very long delays when processing thosemessages, which may lead to a Denial of Service.An OBJECT IDENTIFIER is composed of a series of numbers - sub-identifiers -most of which have no size limit. OBJ_obj2txt() may be used to translatean ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSLtype ASN1_OBJECT) to its canonical numeric text form, which are thesub-identifiers of the OBJECT IDENTIFIER in decimal form, separated byperiods.When one of the sub-identifiers in the OBJECT IDENTIFIER is very large(these are sizes that are seen as absurdly large, taking up tens or hundredsof KiBs), the translation to a decimal number in text may take a very longtime. The time complexity is O(n$\hat{2}$) with 'n' being the size of thesub-identifiers in bytes (*).With OpenSSL 3.0, support to fetch cryptographic algorithms using names /identifiers in string form was introduced. This includes using OBJECTIDENTIFIERs in canonical numeric text form as identifiers for fetchingalgorithms.Such OBJECT IDENTIFIERs may be received through the ASN.1 structureAlgorithmIdentifier, which is commonly used in multiple protocols to specifywhat cryptographic algorithm should be used to sign or verify, encrypt ordecrypt, or digest passed data.Applications that call OBJ_obj2txt() directly with untrusted data areaffected, with any version of OpenSSL. If the use is for the mere purposeof display, the severity is considered low.In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME,CMS, CMP/CRMF or TS. It also impacts anything that processes X.509certificates, including simple things like verifying its signature.The impact on TLS is relatively low, because all versions of OpenSSL have a100KiB limit on the peer's certificate chain. Additionally, this onlyimpacts clients, or servers that have explicitly enabled clientauthentication.In OpenSSL 1.1.1 and 1.0.2, this only affects displaying diverse objects,such as X.509 certificates. This is assumed to not happen in such a waythat it would cause a Denial of Service, so these versions are considerednot affected by this issue in such a way that it would be cause for concern,and the severity is therefore considered low.

- Vulnerability: CVE-2023-0215

  – CVSS Score: N/A

- Description: The public API function BIO_new_NDEF is a helper function used for streamingASN.1 data via a BIO. It is primarily used internally to OpenSSL to support theSMIME, CMS and PKCS7 streaming capabilities, but may also be called directly byend user applications.The function receives a BIO from the caller, prepends a new BIO_f_asn1 filterBIO onto the front of it to form a BIO chain, and then returns the new head ofthe BIO chain to the caller. Under certain conditions, for example if a CMSrecipient public key is invalid, the new filter BIO is freed and the functionreturns a NULL result indicating a failure. However, in this case, the BIO chainis not properly cleaned up and the BIO passed by the caller still retainsinternal pointers to the previously freed filter BIO. If the caller then goes onto call BIO_pop() on the BIO then a use-after-free will occur. This will mostlikely result in a crash.This scenario occurs directly in the internal function B64_write_ASN1() whichmay cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() onthe BIO. This internal function is in turn called by the public API functionsPEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream,SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7.Other public API functions that may be impacted by this includei2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream andi2d_PKCS7_bio_stream.The OpenSSL cms and smime command line applications are similarly affected.

- Vulnerability: CVE-2020-35452

  - CVSS Score: 6.8
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

- Vulnerability: CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2020-1934

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

- Vulnerability: CVE-2022-36760

  - CVSS Score: N/A
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-4304

  - CVSS Score: N/A

- Description: A timing based side channel exists in the OpenSSL RSA Decryption
  implementationwhich could be sufficient to recover a plaintext
  across a network in aBleichenbacher style attack. To achieve a
  successful decryption an attackerwould have to be able to send a
  very large number of trial messages fordecryption. The vulnerability
  affects all RSA padding modes: PKCS#1 v1.5,RSA-OEAP and RSASVE.For
  example, in a TLS connection, RSA is commonly used by a client to
  send anencrypted pre-master secret to the server. An attacker that
  had observed agenuine connection between a client and a server could
  use this flaw to sendtrial messages to the server and record the time
  taken to process them. After asufficiently large number of messages
  the attacker could recover the pre-mastersecret used for the original
  connection and thus be able to decrypt theapplication data sent over
  that connection.

- Vulnerability: CVE-2019-1563

  - CVSS Score: 4.3
  - Description: In situations where an attacker receives automated notification
    of the success or failure of a decryption attempt an attacker,
    after sending a very large number of messages to be decrypted, can
    recover a CMS/PKCS7 transported encryption key or decrypt any RSA
    encrypted message that was encrypted with the public RSA key, using a
    Bleichenbacher padding oracle attack. Applications are not affected
    if they use a certificate together with the private RSA key to the
    CMS_decrypt or PKCS7_decrypt functions to select the correct recipient
    info to decrypt. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c).
    Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL
    1.0.2t (Affected 1.0.2-1.0.2s).

- Vulnerability: CVE-2014-3523

  - CVSS Score: 5
  - Description: Memory leak in the winnt_accept function in server/mpm/winnt/child.c
    in the WinNT MPM in the Apache HTTP Server 2.4.x before 2.4.10 on
    Windows, when the default AcceptFilter is enabled, allows remote
    attackers to cause a denial of service (memory consumption) via
    crafted requests.

- Vulnerability: CVE-2013-5704

  - CVSS Score: 5
  - Description: The mod_headers module in the Apache HTTP Server 2.2.22 allows remote
    attackers to bypass "RequestHeader unset" directives by placing a
    header in the trailer portion of data sent with chunked transfer
    coding. NOTE: the vendor states "this is not a security issue in
    httpd as such."

- Vulnerability: CVE-2019-17567

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel
    configured on an URL that is not necessarily Upgraded by the origin
    server was tunneling the whole connection regardless, thus allowing
    for subsequent requests on the same connection to pass through
    with no HTTP validation, authentication or authorization possibly
    configured.

- Vulnerability: CVE-2022-31813

  - CVSS Score: 7.5

- Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-*
    headers to the origin server based on client side Connection
    header hop-by-hop mechanism. This may be used to bypass IP based
    authentication on the origin server/application.

- Vulnerability: CVE-2012-4360

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module
    0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote
    attackers to inject arbitrary web script or HTML via unspecified
    vectors.

- Vulnerability: CVE-2014-0231

  - CVSS Score: 5
  - Description: The mod_cgid module in the Apache HTTP Server before 2.4.10 does not
    have a timeout mechanism, which allows remote attackers to cause a
    denial of service (process hang) via a request to a CGI script that
    does not read from its stdin file descriptor.

- Vulnerability: CVE-2021-26690

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted
    Cookie header handled by mod_session can cause a NULL pointer
    dereference and crash, leading to a possible Denial Of Service

- Vulnerability: CVE-2021-26691

  - CVSS Score: 7.5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted
    SessionHeader sent by an origin server could cause a heap overflow

- Vulnerability: CVE-2019-0220

  - CVSS Score: 5
  - Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38.
    When the path component of a request URL contains multiple
    consecutive slashes ('/'), directives such as LocationMatch and
    RewriteRule must account for duplicates in regular expressions while
    other aspects of the servers processing will implicitly collapse
    them.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to
    applications calling r:wsread() that point past the end of the
    storage allocated for the buffer.

- Vulnerability: CVE-2021-39275

  - CVSS Score: 7.5
  - Description: ap_escape_quotes() may write beyond the end of a buffer when given
    malicious input. No included modules pass untrusted data to these
    functions, but third-party / external modules may. This issue
    affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2014-3581

  - CVSS Score: 5

- Description: The cache_merge_headers_out function in modules/cache/cache_util.c in the mod_cache module in the Apache HTTP Server before 2.4.11 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty HTTP Content-Type header.

- **Vulnerability:** CVE-2016-0736

  - CVSS Score: 5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.23, mod_session_crypto was encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This made it vulnerable to padding oracle attacks, particularly with CBC.

- **Vulnerability:** CVE-2022-29404

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- **Vulnerability:** CVE-2018-1312

  - CVSS Score: 6.8
  - Description: In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

- **Vulnerability:** CVE-2006-20001

  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- **Vulnerability:** CVE-2017-15710

  - CVSS Score: 5
  - Description: In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.

- **Vulnerability:** CVE-2014-0226

  - CVSS Score: 6.8

- Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

- **Vulnerability:** CVE-2024-0727

  - CVSS Score: N/A
  - Description: Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSLto crash leading to a potential Denial of Service attackImpact summary: Applications loading files in the PKCS12 format from untrustedsources might terminate abruptly.A file in PKCS12 format can contain certificates and keys and may come from anuntrusted source. The PKCS12 specification allows certain fields to be NULL, butOpenSSL does not correctly check for this case. This can lead to a NULL pointerdereference that results in OpenSSL crashing. If an application processes PKCS12files from an untrusted source using the OpenSSL APIs then that application willbe vulnerable to this issue.OpenSSL APIs that are vulnerable to this are: PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a similar issue in SMIME_write_PKCS7(). However since thisfunction is related to writing data we do not consider it security significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.

- **Vulnerability:** CVE-2009-3766

  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when OpenSSL is used, does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

- **Vulnerability:** CVE-2009-3767

  - CVSS Score: 4.3
  - Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other versions, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- **Vulnerability:** CVE-2009-3765

  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- **Vulnerability:** CVE-2022-22721

  - CVSS Score: 5.8

- Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2022-22720

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2019-10092

  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

- Vulnerability: CVE-2021-3712

  - CVSS Score: 5.8
  - Description: ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own "d2i" functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the "data" and "length" fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the "data" field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). It can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y).

- Vulnerability: CVE-2023-0464

- CVSS Score: N/A

- Description: A security vulnerability has been identified in all supported versionsof OpenSSL related to the verification of X.509 certificate chainsthat include policy constraints. Attackers may be able to exploit thisvulnerability by creating a malicious certificate chain that triggersexponential use of computational resources, leading to a denial-of-service(DoS) attack on affected systems.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.

- **Vulnerability: CVE-2023-0465**

  - CVSS Score: N/A

  - Description: Applications that use a non-default option when verifying certificates may bevulnerable to an attack from a malicious CA to circumvent certain checks.Invalid certificate policies in leaf certificates are silently ignored byOpenSSL and other certificate policy checks are skipped for that certificate.A malicious CA could use this to deliberately assert invalid certificate policiesin order to circumvent policy checking on the certificate altogether.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.

- **Vulnerability: CVE-2023-0466**

  - CVSS Score: N/A

  - Description: The function X509_VERIFY_PARAM_add0_policy() is documented toimplicitly enable the certificate policy check when doing certificateverification. However the implementation of the function does notenable the check which allows certificates with invalid or incorrectpolicies to pass the certificate verification.As suddenly enabling the policy check could break existing deployments it wasdecided to keep the existing behavior of the X509_VERIFY_PARAM_add0_policy()function.Instead the applications that require OpenSSL to perform certificatepolicy check need to use X509_VERIFY_PARAM_set1_policies() or explicitlyenable the policy check by calling X509_VERIFY_PARAM_set_flags() withthe X509_V_FLAG_POLICY_CHECK flag argument.Certificate policy checks are disabled by default in OpenSSL and are notcommonly used by applications.

- **Vulnerability: CVE-2019-10098**

  - CVSS Score: 5.8

  - Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.

- **Vulnerability: CVE-2015-0228**

  - CVSS Score: 5

  - Description: The lua_websocket_read function in lua_request.c in the mod_lua module in the Apache HTTP Server through 2.4.12 allows remote attackers to cause a denial of service (child-process crash) by sending a crafted WebSocket Ping frame after a Lua script has called the wsupgrade function.

- **Vulnerability: CVE-2016-5387**

- CVSS Score: 6.8
- Description: The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.

- Vulnerability: CVE-2017-15715

  - CVSS Score: 6.8
  - Description: In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.

- Vulnerability: CVE-2021-40438

  - CVSS Score: 6.8
  - Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2022-23943

  - CVSS Score: 7.5
  - Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

- Vulnerability: CVE-2018-17199

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

- Vulnerability: CVE-2021-23841

  - CVSS Score: 4.3

– Description: The OpenSSL public API function X509_issuer_and_serial_hash() attempts
to create a unique hash value based on the issuer and serial number
data contained within an X509 certificate. However it fails to
correctly handle any errors that may occur while parsing the
issuer field (which might occur if the issuer field is maliciously
constructed). This may subsequently result in a NULL pointer deref
and a crash leading to a potential denial of service attack. The
function X509_issuer_and_serial_hash() is never directly called by
OpenSSL itself so applications are only vulnerable if they use this
function directly and they use it on certificates that may have been
obtained from untrusted sources. OpenSSL versions 1.1.1i and below
are affected by this issue. Users of these versions should upgrade
to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected
by this issue. However OpenSSL 1.0.2 is out of support and no longer
receiving public updates. Premium support customers of OpenSSL 1.0.2
should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j.
Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL
1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2018-1301

  – CVSS Score: 4.3
  – Description: A specially crafted request could have crashed the Apache HTTP Server
  prior to version 2.4.30, due to an out of bound access after a size
  limit is reached by reading the HTTP header. This vulnerability
  is considered very hard if not impossible to trigger in non-debug
  mode (both log and build level), so it is classified as low risk for
  common server usage.

- Vulnerability: CVE-2018-1302

  – CVSS Score: 4.3
  – Description: When an HTTP/2 stream was destroyed after being handled, the Apache
  HTTP Server prior to version 2.4.30 could have written a NULL pointer
  potentially to an already freed memory. The memory pools maintained
  by the server make this vulnerability hard to trigger in usual
  configurations, the reporter and the team could not reproduce it
  outside debug builds, so it is classified as low risk.

- Vulnerability: CVE-2018-1303

  – CVSS Score: 5
  – Description: A specially crafted HTTP request header could have crashed the Apache
  HTTP Server prior to version 2.4.30 due to an out of bound read while
  preparing data to be cached in shared memory. It could be used as
  a Denial of Service attack against users of mod_cache_socache. The
  vulnerability is considered as low risk since mod_cache_socache is not
  widely used, mod_cache_disk is not concerned by this vulnerability.

- Vulnerability: CVE-2021-34798

  – CVSS Score: 5
  – Description: Malformed requests may cause the server to dereference a NULL
  pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2023-25690

  – CVSS Score: N/A

- Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0
  through 2.4.55 allow a HTTP Request Smuggling attack.Configurations
  are affected when mod_proxy is enabled along with some form of
  RewriteRule or ProxyPassMatch in which a non-specific pattern
  matches some portion of the user-supplied request-target (URL)
  data and is then re-inserted into the proxied request-target using
  variable substitution. For example, something like:RewriteEngine
  onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1";
  [P]ProxyPassReverse /here/ http://example.com:8080/Request
  splitting/smuggling could result in bypass of access controls in the
  proxy server, proxying unintended URLs to existing origin servers,
  and cache poisoning. Users are recommended to update to at least
  version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2020-11985

  - CVSS Score: 4.3
  - Description: IP address spoofing when proxying using mod_remoteip and mod_rewrite
    For configurations using proxying with mod_remoteip and certain
    mod_rewrite rules, an attacker could spoof their IP address for
    logging and PHP scripts. Note this issue was fixed in Apache HTTP
    Server 2.4.24 but was retrospectively allocated a low severity CVE in
    2020.

- Vulnerability: CVE-2021-4160

  - CVSS Score: 4.3
  - Description: There is a carry propagation bug in the MIPS32 and MIPS64 squaring
    procedure. Many EC algorithms are affected, including some of the
    TLS 1.3 default curves. Impact was not analyzed in detail, because
    the pre-requisites for attack are considered unlikely and include
    reusing private keys. Analysis suggests that attacks against RSA and
    DSA as a result of this defect would be very difficult to perform
    and are not believed likely. Attacks against DH are considered
    just feasible (although very difficult) because most of the work
    necessary to deduce information about a private key may be performed
    offline. The amount of resources required for such an attack would
    be significant. However, for an attack on TLS to be meaningful, the
    server would have to share the DH private key among multiple clients,
    which is no longer an option since CVE-2016-0701. This issue affects
    OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the
    releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For
    the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that
    is available to premium support customers only. It will be made
    available in 1.0.2zc when it is released. The issue only affects
    OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0).
    Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL
    1.0.2zc-dev (Affected 1.0.2-1.0.2zb).

- Vulnerability: CVE-2013-4352

  - CVSS Score: 4.3
  - Description: The cache_invalidate function in modules/cache/cache_storage.c in the
    mod_cache module in the Apache HTTP Server 2.4.6, when a caching
    forward proxy is enabled, allows remote HTTP servers to cause a
    denial of service (NULL pointer dereference and daemon crash) via
    vectors that trigger a missing hostname value.

- Vulnerability: CVE-2022-26377

  - CVSS Score: 5

- Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request
  Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server
  allows an attacker to smuggle requests to the AJP server it forwards
  requests to. This issue affects Apache HTTP Server Apache HTTP
  Server 2.4 version 2.4.53 and prior versions.

- **Vulnerability: CVE-2014-0098**

  - CVSS Score: 5
  - Description: The log_cookie function in mod_log_config.c in the mod_log_config
    module in the Apache HTTP Server before 2.4.8 allows remote attackers
    to cause a denial of service (segmentation fault and daemon crash)
    via a crafted cookie that is not properly handled during truncation.

- **Vulnerability: CVE-2016-8743**

  - CVSS Score: 5
  - Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was
    liberal in the whitespace accepted from requests and sent in response
    lines and headers. Accepting these different behaviors represented a
    security concern when httpd participates in any chain of proxies or
    interacts with back-end application servers, either through mod_proxy
    or using conventional CGI mechanisms, and may result in request
    smuggling, response splitting and cache pollution.

- **Vulnerability: CVE-2024-40898**

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in
    server/vhost context, allows to potentially leak NTML hashes to
    a malicious server via SSRF and malicious requests.Users are
    recommended to upgrade to version 2.4.62 which fixes this issue.

- **Vulnerability: CVE-2024-38474**

  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server
    2.4.59 and earlier allows attacker to execute scripts indirectories
    permitted by the configuration but not directly reachable by anyURL
    or source disclosure of scripts meant to only to be executed as
    CGI.Users are recommended to upgrade to version 2.4.60, which fixes
    this issue.Some RewriteRules that capture and substitute unsafely
    will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- **Vulnerability: CVE-2022-0778**

  - CVSS Score: 5

- Description: The BN_mod_sqrt() function, which computes a modular square root,
  contains a bug that can cause it to loop forever for non-prime
  moduli. Internally this function is used when parsing certificates
  that contain elliptic curve public keys in compressed form or
  explicit elliptic curve parameters with a base point encoded in
  compressed form. It is possible to trigger the infinite loop by
  crafting a certificate that has invalid explicit curve parameters.
  Since certificate parsing happens prior to verification of the
  certificate signature, any process that parses an externally supplied
  certificate may thus be subject to a denial of service attack. The
  infinite loop can also be reached when parsing crafted private
  keys as they can contain explicit elliptic curve parameters. Thus
  vulnerable situations include: - TLS clients consuming server
  certificates - TLS servers consuming client certificates - Hosting
  providers taking certificates or private keys from customers
  - Certificate authorities parsing certification requests from
  subscribers - Anything else which parses ASN.1 elliptic curve
  parameters Also any other applications that use the BN_mod_sqrt()
  where the attacker can control the parameter values are vulnerable
  to this DoS issue. In the OpenSSL 1.0.2 version the public key is
  not parsed during initial parsing of the certificate which makes
  it slightly harder to trigger the infinite loop. However any
  operation which requires the public key from the certificate will
  trigger the infinite loop. In particular the attacker can use a
  self-signed certificate to trigger the loop during verification
  of the certificate signature. This issue affects OpenSSL versions
  1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n
  and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected
  3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m).
  Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

- Vulnerability: CVE-2020-1971

  - CVSS Score: 4.3

- Description: The X.509 GeneralName type is a generic type for representing
  different types of names. One of those name types is known as
  EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which
  compares different instances of a GENERAL_NAME to see if they
  are equal or not. This function behaves incorrectly when both
  GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference
  and a crash may occur leading to a possible denial of service
  attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two
  purposes: 1) Comparing CRL distribution point names between an
  available CRL and a CRL distribution point embedded in an X509
  certificate 2) When verifying that a timestamp response token signer
  matches the timestamp authority name (exposed via the API functions
  TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can
  control both items being compared then that attacker could trigger
  a crash. For example if the attacker can trick a client or server
  into checking a malicious certificate against a malicious CRL then
  this may occur. Note that some applications automatically download
  CRLs based on a URL embedded in a certificate. This checking happens
  prior to the signatures on the certificate and CRL being verified.
  OpenSSL's s_server, s_client and verify tools have support for the
  "-crl_download" option which implements automatic CRL downloading and
  this attack has been demonstrated to work against those tools. Note
  that an unrelated bug means that affected versions of OpenSSL cannot
  parse or construct correct encodings of EDIPARTYNAME. However it is
  possible to construct a malformed EDIPARTYNAME that OpenSSL's parser
  will accept and hence trigger this attack. All OpenSSL 1.1.1 and
  1.0.2 versions are affected by this issue. Other OpenSSL releases
  are out of support and have not been checked. Fixed in OpenSSL
  1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected
  1.0.2-1.0.2w).

- Vulnerability: CVE-2009-1390

  - CVSS Score: 6.8
  - Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2)
    GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS
    certificate in the chain is accepted instead of verifying the entire
    chain, which allows remote attackers to spoof trusted servers via a
    man-in-the-middle attack.

- Vulnerability: CVE-2012-3526

  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the
    Apache HTTP Server allows remote attackers to cause a denial of
    service (server or application crash) via multiple X-Forwarded-For
    headers in a request.

- Vulnerability: CVE-2023-5678

  - CVSS Score: N/A

– Description: Issue summary: Generating excessively long X9.42 DH keys or checkingexcessively long X9.42 DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_generate_key() togenerate an X9.42 DH key may experience long delays. Likewise, applicationsthat use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check()to check an X9.42 DH key or X9.42 DH parameters may experience long delays.Where the key or parameters that are being checked have been obtained froman untrusted source this may lead to a Denial of Service.While DH_check() performs all the necessary checks (as of CVE-2023-3817),DH_check_pub_key() doesn't make any of these checks, and is thereforevulnerable for excessively large P and Q parameters.Likewise, while DH_generate_key() performs a check for an excessively largeP, it doesn't check for an excessively large Q.An application that calls DH_generate_key() or DH_check_pub_key() andsupplies a key or parameters obtained from an untrusted source could bevulnerable to a Denial of Service attack.DH_generate_key() and DH_check_pub_key() are also called by a number ofother OpenSSL functions. An application calling any of those otherfunctions may similarly be affected. The other functions affected by thisare DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate().Also vulnerable are the OpenSSL pkey command line application when using the"-pubcheck" option, as well as the OpenSSL genpkey command line application.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2017-3736

  – CVSS Score: 4

  – Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

- Vulnerability: CVE-2017-3737

  – CVSS Score: 4.3

- Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

- Vulnerability: CVE-2019-1547

  - CVSS Score: 1.9

  - Description: Normally in OpenSSL EC groups always have a co-factor present and this is used in side channel resistant code paths. However, in some cases, it is possible to construct a group using explicit parameters (instead of using a named curve). In those cases it is possible that such a group does not have the cofactor present. This can occur even where all the parameters match a known named curve. If such a curve is used then OpenSSL falls back to non-side channel resistant code paths which may result in full key recovery during an ECDSA signature operation. In order to be vulnerable an attacker would have to have the ability to time the creation of a large number of signatures where explicit parameters with no co-factor present are in use by an application using libcrypto. For the avoidance of doubt libssl is not vulnerable because explicit parameters are never used. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).

- Vulnerability: CVE-2017-3735

  - CVSS Score: 5

  - Description: While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL before 1.0.2m and 1.1.0g.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5

  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2022-1292

  - CVSS Score: 10

- Description: The c_rehash script does not properly sanitise shell metacharacters
  to prevent command injection. This script is distributed by
  some operating systems in a manner where it is automatically
  executed. On such operating systems, an attacker could execute
  arbitrary commands with the privileges of the script. Use of the
  c_rehash script is considered obsolete and should be replaced by the
  OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected
  3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n).
  Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).

- Vulnerability: CVE-2017-3738

  - CVSS Score: 4.3
  - Description: There is an overflow bug in the AVX2 Montgomery multiplication
    procedure used in exponentiation with 1024-bit moduli. No EC
    algorithms are affected. Analysis suggests that attacks against
    RSA and DSA as a result of this defect would be very difficult to
    perform and are not believed likely. Attacks against DH1024 are
    considered just feasible, because most of the work necessary to
    deduce information about a private key may be performed offline. The
    amount of resources required for such an attack would be significant.
    However, for an attack on TLS to be meaningful, the server would have
    to share the DH1024 private key among multiple clients, which is no
    longer an option since CVE-2016-0701. This only affects processors
    that support the AVX2 but not ADX extensions like Intel Haswell
    (4th generation). Note: The impact from this issue is similar to
    CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version
    1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n.
    Due to the low severity of this issue we are not issuing a new
    release of OpenSSL 1.1.0 at this time. The fix will be included in
    OpenSSL 1.1.0h when it becomes available. The fix is also available
    in commit e502cc86d in the OpenSSL git repository.

- Vulnerability: CVE-2012-4001

  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server
    does not properly verify its host name, which allows remote attackers
    to trigger HTTP requests to arbitrary hosts via unspecified vectors,
    as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2022-37436

  - CVSS Score: N/A
  - Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause
    the response headers to be truncated early, resulting in some headers
    being incorporated into the response body. If the later headers have
    any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2021-23840

  - CVSS Score: 5

- Description: Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissable length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2018-0737

  - CVSS Score: 4.3
  - Description: The OpenSSL RSA Key generation algorithm has been shown to be vulnerable to a cache timing side channel attack. An attacker with sufficient access to mount cache timing attacks during the RSA key generation process could recover the private key. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2b-1.0.2o).

- Vulnerability: CVE-2018-0734

  - CVSS Score: 4.3
  - Description: The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.1a (Affected 1.1.1). Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.0.2q (Affected 1.0.2-1.0.2p).

- Vulnerability: CVE-2018-0732

  - CVSS Score: 5
  - Description: During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime value to the client. This will cause the client to spend an unreasonably long period of time generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2-1.0.2o).

- Vulnerability: CVE-2017-9788

  - CVSS Score: 6.4
  - Description: In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.

- Vulnerability: CVE-2018-0739

  - CVSS Score: 4.3

- Description: Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o (Affected 1.0.2b-1.0.2n).

- Vulnerability: CVE-2014-8109

  - CVSS Score: 4.3
  - Description: mod_lua.c in the mod_lua module in the Apache HTTP Server 2.3.x and 2.4.x through 2.4.10 does not support an httpd configuration in which the same Lua authorization provider is used with different arguments within different contexts, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives, as demonstrated by a configuration that specifies authorization for one group to access a certain directory, and authorization for a second group to access a second directory.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2016-2161

  - CVSS Score: 5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.23, malicious input to mod_auth_digest can cause the server to crash, and each instance continues to crash even for subsequently valid requests.

- Vulnerability: CVE-2016-8612

  - CVSS Score: 3.3
  - Description: Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.

- Vulnerability: CVE-2019-1552

  - CVSS Score: 1.9

- Description: OpenSSL has internal defaults for a directory tree where it
             can find a configuration file as well as certificates used for
             verification in TLS. This directory is most commonly referred to
             as OPENSSLDIR, and is configurable with the --prefix / --openssldir
             configuration options. For OpenSSL versions 1.1.0 and 1.1.1, the
             mingw configuration targets assume that resulting programs and
             libraries are installed in a Unix-like environment and the default
             prefix for program installation as well as for OPENSSLDIR should be
             '/usr/local'. However, mingw programs are Windows programs, and as
             such, find themselves looking at sub-directories of 'C:/usr/local',
             which may be world writable, which enables untrusted users to modify
             OpenSSL's default configuration, insert CA certificates, modify (or
             even replace) existing engine modules, etc. For OpenSSL 1.0.2,
             '/usr/local/ssl' is used as default for OPENSSLDIR on all Unix and
             Windows targets, including Visual C builds. However, some build
             instructions for the diverse Windows targets on 1.0.2 encourage
             you to specify your own --prefix. OpenSSL versions 1.1.1, 1.1.0
             and 1.0.2 are affected by this issue. Due to the limited scope
             of affected deployments this has been assessed as low severity and
             therefore we are not creating new releases at this time. Fixed
             in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL
             1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected
             1.0.2-1.0.2s).

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5
             for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM
             Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows
             use an improper encryption algorithm and a weak key for maintaining
             the stored data of the node secret for the SecurID Authentication
             API, which allows local users to obtain sensitive information via
             cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication
             Agent 7.1 before 7.1.1 for Web for Internet Information Services,
             and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to
             inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2019-1551

  - CVSS Score: 5
  - Description: There is an overflow bug in the x64_64 Montgomery squaring procedure
             used in exponentiation with 512-bit moduli. No EC algorithms are
             affected. Analysis suggests that attacks against 2-prime RSA1024,
             3-prime RSA1536, and DSA1024 as a result of this defect would be
             very difficult to perform and are not believed likely. Attacks
             against DH512 are considered just feasible. However, for an attack
             the target would have to re-use the DH512 private key, which is not
             recommended anyway. Also applications directly using the low level
             API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME. Fixed
             in OpenSSL 1.1.1e (Affected 1.1.1-1.1.1d). Fixed in OpenSSL 1.0.2u
             (Affected 1.0.2-1.0.2t).

- Vulnerability: CVE-2019-1559

  - CVSS Score: 4.3

- Description: If an application encounters a fatal protocol error and then calls SSL_shutdown() twice (once to send a close_notify, and once to receive one) then OpenSSL can respond differently to the calling application if a 0 byte record is received with invalid padding compared to if a 0 byte record is received with an invalid MAC. If the application then behaves differently based on that in a way that is detectable to the remote peer, then this amounts to a padding oracle that could be used to decrypt data. In order for this to be exploitable "non-stitched" ciphersuites must be in use. Stitched ciphersuites are optimised implementations of certain commonly used ciphersuites. Also the application must call SSL_shutdown() twice even if a protocol error has occurred (applications should not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected 1.0.2-1.0.2q).

- Vulnerability: CVE-2023-45802

  - CVSS Score: N/A

  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2018-1283

  - CVSS Score: 3.5

  - Description: In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to forward its session data to CGI applications (SessionEnv on, not the default), a remote user may influence their content by using a "Session" header. This comes from the "HTTP_SESSION" variable name used by mod_session to forward its data to CGIs, since the prefix "HTTP_" is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications.

- Vulnerability: CVE-2020-1968

  - CVSS Score: 4.3

  - Description: The Raccoon attack exploits a flaw in the TLS specification which can lead to an attacker being able to compute the pre-master secret in connections which have used a Diffie-Hellman (DH) based ciphersuite. In such a case this would result in the attacker being able to eavesdrop on all encrypted communications sent over that TLS connection. The attack can only be exploited if an implementation re-uses a DH secret across multiple TLS connections. Note that this issue only impacts DH ciphersuites and not ECDH ciphersuites. This issue affects OpenSSL 1.0.2 which is out of support and no longer receiving public updates. OpenSSL 1.1.1 is not vulnerable to this issue. Fixed in OpenSSL 1.0.2w (Affected 1.0.2-1.0.2v).

- Vulnerability: CVE-2019-0217

  - CVSS Score: 6

– Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.

- Vulnerability: CVE-2022-28615

    – CVSS Score: 6.4
    – Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- Vulnerability: CVE-2022-28614

    – CVSS Score: 5
    – Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

- Vulnerability: CVE-2014-0117

    – CVSS Score: 4.3
    – Description: The mod_proxy module in the Apache HTTP Server 2.4.x before 2.4.10, when a reverse proxy is enabled, allows remote attackers to cause a denial of service (child-process crash) via a crafted HTTP Connection header.

- Vulnerability: CVE-2017-7679

    – CVSS Score: 7.5
    – Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

- Vulnerability: CVE-2017-9798

    – CVSS Score: 5
    – Description: Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.

- Vulnerability: CVE-2015-3185

    – CVSS Score: 4.3
    – Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

- Vulnerability: CVE-2015-3184
  - CVSS Score: 5
  - Description: mod_authz_svn in Apache Subversion 1.7.x before 1.7.21 and 1.8.x before 1.8.14, when using Apache httpd 2.4.x, does not properly restrict anonymous access, which allows remote anonymous users to read hidden files via the path name.
- Vulnerability: CVE-2015-3183
  - CVSS Score: 5
  - Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.
- Vulnerability: CVE-2013-4365
  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.
- Vulnerability: CVE-2018-5407
  - CVSS Score: 1.9
  - Description: Simultaneous Multi-threading (SMT) in processors can enable local users to exploit software vulnerable to timing attacks via a side-channel timing attack on 'port contention'.
- Vulnerability: CVE-2022-28330
  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.
- Vulnerability: CVE-2021-32791
  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.
- Vulnerability: CVE-2021-32792
  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.
- Vulnerability: CVE-2024-38476

- CVSS Score: N/A
- Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are
    vulnerably to information disclosure, SSRF or local script execution
    viabackend applications whose response headers are malicious or
    exploitable.Users are recommended to upgrade to version 2.4.60, which
    fixes this issue.

• Vulnerability: CVE-2024-38477

- CVSS Score: N/A
- Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59
    and earlier allows an attacker to crash the server via a malicious
    request.Users are recommended to upgrade to version 2.4.60, which
    fixes this issue.

• Vulnerability: CVE-2023-31122

- CVSS Score: N/A
- Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP
    Server.This issue affects Apache HTTP Server: through 2.4.57.

• Vulnerability: CVE-2009-0796

- CVSS Score: 2.6
- Description: Cross-site scripting (XSS) vulnerability in Status.pm in
    Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the
    Apache HTTP Server, when /perl-status is accessible, allows remote
    attackers to inject arbitrary web script or HTML via the URI.

• Vulnerability: CVE-2022-2068

- CVSS Score: 10
- Description: In addition to the c_rehash shell command injection identified in
    CVE-2022-1292, further circumstances where the c_rehash script
    does not properly sanitise shell metacharacters to prevent command
    injection were found by code review. When the CVE-2022-1292 was
    fixed it was not discovered that there are other places in the
    script where the file names of certificates being hashed were
    possibly passed to a command executed through the shell. This
    script is distributed by some operating systems in a manner where
    it is automatically executed. On such operating systems, an
    attacker could execute arbitrary commands with the privileges of
    the script. Use of the c_rehash script is considered obsolete and
    should be replaced by the OpenSSL rehash command line tool. Fixed in
    OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL
    1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected
    1.0.2-1.0.2ze).

• Vulnerability: CVE-2014-0118

- CVSS Score: 4.3
- Description: The deflate_in_filter function in mod_deflate.c in the mod_deflate
    module in the Apache HTTP Server before 2.4.10, when request body
    decompression is enabled, allows remote attackers to cause a denial
    of service (resource consumption) via crafted request data that
    decompresses to a much larger size.

• Vulnerability: CVE-2013-6438

- CVSS Score: 5

- Description: The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.

- Vulnerability: CVE-2020-1927

  - CVSS Score: 5.8
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.

- Vulnerability: CVE-2023-0286

  - CVSS Score: N/A
  - Description: There is a type confusion vulnerability relating to X.400 address processinginside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING butthe public structure definition for GENERAL_NAME incorrectly specified the typeof the x400Address field as ASN1_TYPE. This field is subsequently interpreted bythe OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than anASN1_STRING.When CRL checking is enabled (i.e. the application sets theX509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to passarbitrary pointers to a memcmp call, enabling them to read memory contents orenact a denial of service. In most cases, the attack requires the attacker toprovide both the certificate chain and CRL, neither of which need to have avalid signature. If the attacker only controls one of these inputs, the otherinput must already contain an X.400 address as a CRL distribution point, whichis uncommon. As such, this vulnerability is most likely to only affectapplications which have implemented their own functionality for retrieving CRLsover a network.

- Vulnerability: CVE-2023-3817

  - CVSS Score: N/A
  - Description: Issue summary: Checking excessively long DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH key or DH parameters may experience longdelays. Where the key or parameters that are being checked have been obtainedfrom an untrusted source this may lead to a Denial of Service.The function DH_check() performs various checks on DH parameters. After fixingCVE-2023-3446 it was discovered that a large q parameter value can also triggeran overly long computation during some of these checks. A correct q value,if present, cannot be larger than the modulus p parameter, thus it isunnecessary to perform these checks if q is larger than p.An application that calls DH_check() and supplies a key or parameters obtainedfrom an untrusted source could be vulnerable to a Denial of Service attack.The function DH_check() is itself called by a number of other OpenSSL functions.An application calling any of those other functions may similarly be affected.The other functions affected by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable are the OpenSSL dhparam and pkeyparam command line applicationswhen using the "-check" option.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2017-3167

- CVSS Score: 7.5
- Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.

- Vulnerability: CVE-2021-32786

  - CVSS Score: 5.8
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, 'oidc_validate_redirect_url()' does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring 'mod_auth_openidc' to only allow redirection whose destination matches a given regular expression.

- Vulnerability: CVE-2021-32785

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache ('OIDCCacheEncrypt off', 'OIDCSessionType server-cache', 'OIDCCacheType redis'), 'mod_auth_openidc' wrongly performed argument interpolation before passing Redis requests to 'hiredis', which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the 'hiredis' API. As a workaround, this vulnerability can be mitigated by setting 'OIDCCacheEncrypt' to 'on', as cache keys are cryptographically hashed before use when this option is enabled.

- Vulnerability: CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2021-44790

  - CVSS Score: 7.5
  - Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

- Vulnerability: CVE-2016-4975

  – CVSS Score: 4.3

  – Description: Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).

- Vulnerability: CVE-2020-13938

  – CVSS Score: 2.1

  – Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

- Vulnerability: CVE-2023-2650

  – CVSS Score: N/A

  – Description: Issue summary: Processing some specially crafted ASN.1 object identifiers ordata containing them may be very slow.Impact summary: Applications that use OBJ_obj2txt() directly, or use any ofthe OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no messagesize limit may experience notable to very long delays when processing thosemessages, which may lead to a Denial of Service.An OBJECT IDENTIFIER is composed of a series of numbers - sub-identifiers -most of which have no size limit. OBJ_obj2txt() may be used to translatean ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSLtype ASN1_OBJECT) to its canonical numeric text form, which are thesub-identifiers of the OBJECT IDENTIFIER in decimal form, separated byperiods.When one of the sub-identifiers in the OBJECT IDENTIFIER is very large(these are sizes that are seen as absurdly large, taking up tens or hundredsof KiBs), the translation to a decimal number in text may take a very longtime. The time complexity is $O(n^2)$ with 'n' being the size of thesub-identifiers in bytes (*).With OpenSSL 3.0, support to fetch cryptographic algorithms using names /identifiers in string form was introduced. This includes using OBJECTIDENTIFIERs in canonical numeric text form as identifiers for fetchingalgorithms.Such OBJECT IDENTIFIERs may be received through the ASN.1 structureAlgorithmIdentifier, which is commonly used in multiple protocols to specifywhat cryptographic algorithm should be used to sign or verify, encrypt ordecrypt, or digest passed data.Applications that call OBJ_obj2txt() directly with untrusted data areaffected, with any version of OpenSSL. If the use is for the mere purposeof display, the severity is considered low.In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME,CMS, CMP/CRMF or TS. It also impacts anything that processes X.509certificates, including simple things like verifying its signature.The impact on TLS is relatively low, because all versions of OpenSSL have a100KiB limit on the peer's certificate chain. Additionally, this onlyimpacts clients, or servers that have explicitly enabled clientauthentication.In OpenSSL 1.1.1 and 1.0.2, this only affects displaying diverse objects,such as X.509 certificates. This is assumed to not happen in such a waythat it would cause a Denial of Service, so these versions are considerednot affected by this issue in such a way that it would be cause for concern,and the severity is therefore considered low.

- Vulnerability: CVE-2023-0215

  – CVSS Score: N/A

- Description: The public API function BIO_new_NDEF is a helper function used for streamingASN.1 data via a BIO. It is primarily used internally to OpenSSL to support theSMIME, CMS and PKCS7 streaming capabilities, but may also be called directly byend user applications.The function receives a BIO from the caller, prepends a new BIO_f_asn1 filterBIO onto the front of it to form a BIO chain, and then returns the new head ofthe BIO chain to the caller. Under certain conditions, for example if a CMSrecipient public key is invalid, the new filter BIO is freed and the functionreturns a NULL result indicating a failure. However, in this case, the BIO chainis not properly cleaned up and the BIO passed by the caller still retainsinternal pointers to the previously freed filter BIO. If the caller then goes onto call BIO_pop() on the BIO then a use-after-free will occur. This will mostlikely result in a crash.This scenario occurs directly in the internal function B64_write_ASN1() whichmay cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() onthe BIO. This internal function is in turn called by the public API functionsPEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream,SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7.Other public API functions that may be impacted by this includei2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream andi2d_PKCS7_bio_stream.The OpenSSL cms and smime command line applications are similarly affected.

- **Vulnerability:** CVE-2020-35452

  - CVSS Score: 6.8
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

- **Vulnerability:** CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- **Vulnerability:** CVE-2020-1934

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

- **Vulnerability:** CVE-2022-36760

  - CVSS Score: N/A
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- **Vulnerability:** CVE-2022-4304

  - CVSS Score: N/A

- Description: A timing based side channel exists in the OpenSSL RSA Decryption implementationwhich could be sufficient to recover a plaintext across a network in aBleichenbacher style attack. To achieve a successful decryption an attackerwould have to be able to send a very large number of trial messages fordecryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5,RSA-OEAP and RSASVE.For example, in a TLS connection, RSA is commonly used by a client to send anencrypted pre-master secret to the server. An attacker that had observed agenuine connection between a client and a server could use this flaw to sendtrial messages to the server and record the time taken to process them. After asufficiently large number of messages the attacker could recover the pre-mastersecret used for the original connection and thus be able to decrypt theapplication data sent over that connection.

- Vulnerability: CVE-2019-1563

  - CVSS Score: 4.3
  - Description: In situations where an attacker receives automated notification of the success or failure of a decryption attempt an attacker, after sending a very large number of messages to be decrypted, can recover a CMS/PKCS7 transported encryption key or decrypt any RSA encrypted message that was encrypted with the public RSA key, using a Bleichenbacher padding oracle attack. Applications are not affected if they use a certificate together with the private RSA key to the CMS_decrypt or PKCS7_decrypt functions to select the correct recipient info to decrypt. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).

- Vulnerability: CVE-2014-3523

  - CVSS Score: 5
  - Description: Memory leak in the winnt_accept function in server/mpm/winnt/child.c in the WinNT MPM in the Apache HTTP Server 2.4.x before 2.4.10 on Windows, when the default AcceptFilter is enabled, allows remote attackers to cause a denial of service (memory consumption) via crafted requests.

- Vulnerability: CVE-2013-5704

  - CVSS Score: 5
  - Description: The mod_headers module in the Apache HTTP Server 2.2.22 allows remote attackers to bypass "RequestHeader unset" directives by placing a header in the trailer portion of data sent with chunked transfer coding. NOTE: the vendor states "this is not a security issue in httpd as such."

- Vulnerability: CVE-2019-17567

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

- Vulnerability: CVE-2022-31813

  - CVSS Score: 7.5

- Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-*
  headers to the origin server based on client side Connection
  header hop-by-hop mechanism. This may be used to bypass IP based
  authentication on the origin server/application.

- Vulnerability: CVE-2012-4360

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module
    0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote
    attackers to inject arbitrary web script or HTML via unspecified
    vectors.

- Vulnerability: CVE-2014-0231

  - CVSS Score: 5
  - Description: The mod_cgid module in the Apache HTTP Server before 2.4.10 does not
    have a timeout mechanism, which allows remote attackers to cause a
    denial of service (process hang) via a request to a CGI script that
    does not read from its stdin file descriptor.

- Vulnerability: CVE-2021-26690

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted
    Cookie header handled by mod_session can cause a NULL pointer
    dereference and crash, leading to a possible Denial Of Service

- Vulnerability: CVE-2021-26691

  - CVSS Score: 7.5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted
    SessionHeader sent by an origin server could cause a heap overflow

- Vulnerability: CVE-2019-0220

  - CVSS Score: 5
  - Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38.
    When the path component of a request URL contains multiple
    consecutive slashes ('/'), directives such as LocationMatch and
    RewriteRule must account for duplicates in regular expressions while
    other aspects of the servers processing will implicitly collapse
    them.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to
    applications calling r:wsread() that point past the end of the
    storage allocated for the buffer.

- Vulnerability: CVE-2021-39275

  - CVSS Score: 7.5
  - Description: ap_escape_quotes() may write beyond the end of a buffer when given
    malicious input. No included modules pass untrusted data to these
    functions, but third-party / external modules may. This issue
    affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2014-3581

  - CVSS Score: 5

- Description: The cache_merge_headers_out function in modules/cache/cache_util.c in the mod_cache module in the Apache HTTP Server before 2.4.11 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty HTTP Content-Type header.

- **Vulnerability:** CVE-2016-0736

  - CVSS Score: 5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.23, mod_session_crypto was encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This made it vulnerable to padding oracle attacks, particularly with CBC.

- **Vulnerability:** CVE-2022-29404

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- **Vulnerability:** CVE-2018-1312

  - CVSS Score: 6.8
  - Description: In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

- **Vulnerability:** CVE-2006-20001

  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- **Vulnerability:** CVE-2017-15710

  - CVSS Score: 5
  - Description: In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.

- **Vulnerability:** CVE-2014-0226

  - CVSS Score: 6.8

- Description: Race condition in the mod_status module in the Apache HTTP Server
                 before 2.4.10 allows remote attackers to cause a denial of
                 service (heap-based buffer overflow), or possibly obtain sensitive
                 credential information or execute arbitrary code, via a crafted
                 request that triggers improper scoreboard handling within the
                 status_handler function in modules/generators/mod_status.c and the
                 lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

- Vulnerability: CVE-2024-0727

  - CVSS Score: N/A

  - Description: Issue summary: Processing a maliciously formatted PKCS12 file
                 may lead OpenSSLto crash leading to a potential Denial of Service
                 attackImpact summary: Applications loading files in the PKCS12
                 format from untrustedsources might terminate abruptly.A file in
                 PKCS12 format can contain certificates and keys and may come from
                 anuntrusted source. The PKCS12 specification allows certain fields
                 to be NULL, butOpenSSL does not correctly check for this case.
                 This can lead to a NULL pointerdereference that results in OpenSSL
                 crashing. If an application processes PKCS12files from an untrusted
                 source using the OpenSSL APIs then that application willbe vulnerable
                 to this issue.OpenSSL APIs that are vulnerable to this are:
                 PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(),
                 PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a
                 similar issue in SMIME_write_PKCS7(). However since thisfunction
                 is related to writing data we do not consider it security
                 significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected
                 by this issue.

- Vulnerability: CVE-2009-3766

  - CVSS Score: 6.8

  - Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when
                 OpenSSL is used, does not verify the domain name in the subject's
                 Common Name (CN) field of an X.509 certificate, which allows
                 man-in-the-middle attackers to spoof SSL servers via an arbitrary
                 valid certificate.

- Vulnerability: CVE-2009-3767

  - CVSS Score: 4.3

  - Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other
                 versions, when OpenSSL is used, does not properly handle a '\{}0'
                 character in a domain name in the subject's Common Name (CN) field
                 of an X.509 certificate, which allows man-in-the-middle attackers
                 to spoof arbitrary SSL servers via a crafted certificate issued by a
                 legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2009-3765

  - CVSS Score: 6.8

  - Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does
                 not properly handle a '\{}0' character in a domain name in the
                 subject's Common Name (CN) field of an X.509 certificate, which
                 allows man-in-the-middle attackers to spoof arbitrary SSL servers via
                 a crafted certificate issued by a legitimate Certification Authority,
                 a related issue to CVE-2009-2408.

- Vulnerability: CVE-2022-22721

  - CVSS Score: 5.8

- Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- **Vulnerability:** CVE-2022-22720

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- **Vulnerability:** CVE-2019-10092

  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

- **Vulnerability:** CVE-2021-3712

  - CVSS Score: 5.8
  - Description: ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own "d2i" functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the "data" and "length" fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the "data" field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). It can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y).

- **Vulnerability:** CVE-2023-0464

- CVSS Score: N/A
- Description: A security vulnerability has been identified in all supported versionsof OpenSSL related to the verification of X.509 certificate chainsthat include policy constraints. Attackers may be able to exploit thisvulnerability by creating a malicious certificate chain that triggersexponential use of computational resources, leading to a denial-of-service(DoS) attack on affected systems.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0465

  - CVSS Score: N/A
  - Description: Applications that use a non-default option when verifying certificates may bevulnerable to an attack from a malicious CA to circumvent certain checks.Invalid certificate policies in leaf certificates are silently ignored byOpenSSL and other certificate policy checks are skipped for that certificate.A malicious CA could use this to deliberately assert invalid certificate policiesin order to circumvent policy checking on the certificate altogether.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0466

  - CVSS Score: N/A
  - Description: The function X509_VERIFY_PARAM_add0_policy() is documented toimplicitly enable the certificate policy check when doing certificateverification. However the implementation of the function does notenable the check which allows certificates with invalid or incorrectpolicies to pass the certificate verification.As suddenly enabling the policy check could break existing deployments it wasdecided to keep the existing behavior of the X509_VERIFY_PARAM_add0_policy()function.Instead the applications that require OpenSSL to perform certificatepolicy check need to use X509_VERIFY_PARAM_set1_policies() or explicitlyenable the policy check by calling X509_VERIFY_PARAM_set_flags() withthe X509_V_FLAG_POLICY_CHECK flag argument.Certificate policy checks are disabled by default in OpenSSL and are notcommonly used by applications.

- Vulnerability: CVE-2019-10098

  - CVSS Score: 5.8
  - Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.

- Vulnerability: CVE-2015-0228

  - CVSS Score: 5
  - Description: The lua_websocket_read function in lua_request.c in the mod_lua module in the Apache HTTP Server through 2.4.12 allows remote attackers to cause a denial of service (child-process crash) by sending a crafted WebSocket Ping frame after a Lua script has called the wsupgrade function.

- Vulnerability: CVE-2016-5387

– CVSS Score: 6.8

– Description: The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.

- **Vulnerability: CVE-2017-15715**

  – CVSS Score: 6.8

  – Description: In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.

- **Vulnerability: CVE-2021-40438**

  – CVSS Score: 6.8

  – Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

- **Vulnerability: CVE-2011-1176**

  – CVSS Score: 4.3

  – Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- **Vulnerability: CVE-2022-23943**

  – CVSS Score: 7.5

  – Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

- **Vulnerability: CVE-2018-17199**

  – CVSS Score: 5

  – Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

- **Vulnerability: CVE-2021-23841**

  – CVSS Score: 4.3

- Description: The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack. The function X509_issuer_and_serial_hash() is never directly called by OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on certificates that may have been obtained from untrusted sources. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2018-1301

  - CVSS Score: 4.3
  - Description: A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.

- Vulnerability: CVE-2018-1302

  - CVSS Score: 4.3
  - Description: When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.

- Vulnerability: CVE-2018-1303

  - CVSS Score: 5
  - Description: A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache. The vulnerability is considered as low risk since mod_cache_socache is not widely used, mod_cache_disk is not concerned by this vulnerability.

- Vulnerability: CVE-2021-34798

  - CVSS Score: 5
  - Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2023-25690

  - CVSS Score: N/A

- Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- **Vulnerability: CVE-2020-11985**

  - CVSS Score: 4.3
  - Description: IP address spoofing when proxying using mod_remoteip and mod_rewrite For configurations using proxying with mod_remoteip and certain mod_rewrite rules, an attacker could spoof their IP address for logging and PHP scripts. Note this issue was fixed in Apache HTTP Server 2.4.24 but was retrospectively allocated a low severity CVE in 2020.

- **Vulnerability: CVE-2021-4160**

  - CVSS Score: 4.3
  - Description: There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that is available to premium support customers only. It will be made available in 1.0.2zc when it is released. The issue only affects OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0). Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL 1.0.2zc-dev (Affected 1.0.2-1.0.2zb).

- **Vulnerability: CVE-2013-4352**

  - CVSS Score: 4.3
  - Description: The cache_invalidate function in modules/cache/cache_storage.c in the mod_cache module in the Apache HTTP Server 2.4.6, when a caching forward proxy is enabled, allows remote HTTP servers to cause a denial of service (NULL pointer dereference and daemon crash) via vectors that trigger a missing hostname value.

- **Vulnerability: CVE-2022-26377**

  - CVSS Score: 5

– Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request
    Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server
    allows an attacker to smuggle requests to the AJP server it forwards
    requests to. This issue affects Apache HTTP Server Apache HTTP
    Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2014-0098

  – CVSS Score: 5

  – Description: The log_cookie function in mod_log_config.c in the mod_log_config
    module in the Apache HTTP Server before 2.4.8 allows remote attackers
    to cause a denial of service (segmentation fault and daemon crash)
    via a crafted cookie that is not properly handled during truncation.

- Vulnerability: CVE-2016-8743

  – CVSS Score: 5

  – Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was
    liberal in the whitespace accepted from requests and sent in response
    lines and headers. Accepting these different behaviors represented a
    security concern when httpd participates in any chain of proxies or
    interacts with back-end application servers, either through mod_proxy
    or using conventional CGI mechanisms, and may result in request
    smuggling, response splitting and cache pollution.

- Vulnerability: CVE-2024-40898

  – CVSS Score: N/A

  – Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in
    server/vhost context, allows to potentially leak NTML hashes to
    a malicious server via SSRF and malicious requests.Users are
    recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2024-38474

  – CVSS Score: N/A

  – Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server
    2.4.59 and earlier allows attacker to execute scripts indirectories
    permitted by the configuration but not directly reachable by anyURL
    or source disclosure of scripts meant to only to be executed as
    CGI.Users are recommended to upgrade to version 2.4.60, which fixes
    this issue.Some RewriteRules that capture and substitute unsafely
    will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2022-0778

  – CVSS Score: 5

– Description: The BN_mod_sqrt() function, which computes a modular square root,
                 contains a bug that can cause it to loop forever for non-prime
                 moduli. Internally this function is used when parsing certificates
                 that contain elliptic curve public keys in compressed form or
                 explicit elliptic curve parameters with a base point encoded in
                 compressed form. It is possible to trigger the infinite loop by
                 crafting a certificate that has invalid explicit curve parameters.
                 Since certificate parsing happens prior to verification of the
                 certificate signature, any process that parses an externally supplied
                 certificate may thus be subject to a denial of service attack. The
                 infinite loop can also be reached when parsing crafted private
                 keys as they can contain explicit elliptic curve parameters. Thus
                 vulnerable situations include: - TLS clients consuming server
                 certificates - TLS servers consuming client certificates - Hosting
                 providers taking certificates or private keys from customers
                 - Certificate authorities parsing certification requests from
                 subscribers - Anything else which parses ASN.1 elliptic curve
                 parameters Also any other applications that use the BN_mod_sqrt()
                 where the attacker can control the parameter values are vulnerable
                 to this DoS issue. In the OpenSSL 1.0.2 version the public key is
                 not parsed during initial parsing of the certificate which makes
                 it slightly harder to trigger the infinite loop. However any
                 operation which requires the public key from the certificate will
                 trigger the infinite loop. In particular the attacker can use a
                 self-signed certificate to trigger the loop during verification
                 of the certificate signature. This issue affects OpenSSL versions
                 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n
                 and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected
                 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m).
                 Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

• Vulnerability: CVE-2020-1971

   – CVSS Score: 4.3

- Description: The X.509 GeneralName type is a generic type for representing
  different types of names. One of those name types is known as
  EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which
  compares different instances of a GENERAL_NAME to see if they
  are equal or not. This function behaves incorrectly when both
  GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference
  and a crash may occur leading to a possible denial of service
  attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two
  purposes: 1) Comparing CRL distribution point names between an
  available CRL and a CRL distribution point embedded in an X509
  certificate 2) When verifying that a timestamp response token signer
  matches the timestamp authority name (exposed via the API functions
  TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can
  control both items being compared then that attacker could trigger
  a crash. For example if the attacker can trick a client or server
  into checking a malicious certificate against a malicious CRL then
  this may occur. Note that some applications automatically download
  CRLs based on a URL embedded in a certificate. This checking happens
  prior to the signatures on the certificate and CRL being verified.
  OpenSSL's s_server, s_client and verify tools have support for the
  "-crl_download" option which implements automatic CRL downloading and
  this attack has been demonstrated to work against those tools. Note
  that an unrelated bug means that affected versions of OpenSSL cannot
  parse or construct correct encodings of EDIPARTYNAME. However it is
  possible to construct a malformed EDIPARTYNAME that OpenSSL's parser
  will accept and hence trigger this attack. All OpenSSL 1.1.1 and
  1.0.2 versions are affected by this issue. Other OpenSSL releases
  are out of support and have not been checked. Fixed in OpenSSL
  1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected
  1.0.2-1.0.2w).

- **Vulnerability: CVE-2009-1390**

  - CVSS Score: 6.8
  - Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2)
    GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS
    certificate in the chain is accepted instead of verifying the entire
    chain, which allows remote attackers to spoof trusted servers via a
    man-in-the-middle attack.

- **Vulnerability: CVE-2012-3526**

  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the
    Apache HTTP Server allows remote attackers to cause a denial of
    service (server or application crash) via multiple X-Forwarded-For
    headers in a request.

- **Vulnerability: CVE-2023-5678**

  - CVSS Score: N/A

- Description: Issue summary: Generating excessively long X9.42 DH keys or checkingexcessively long X9.42 DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_generate_key() togenerate an X9.42 DH key may experience long delays. Likewise, applicationsthat use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check()to check an X9.42 DH key or X9.42 DH parameters may experience long delays.Where the key or parameters that are being checked have been obtained froman untrusted source this may lead to a Denial of Service.While DH_check() performs all the necessary checks (as of CVE-2023-3817),DH_check_pub_key() doesn't make any of these checks, and is thereforevulnerable for excessively large P and Q parameters.Likewise, while DH_generate_key() performs a check for an excessively largeP, it doesn't check for an excessively large Q.An application that calls DH_generate_key() or DH_check_pub_key() andsupplies a key or parameters obtained from an untrusted source could bevulnerable to a Denial of Service attack.DH_generate_key() and DH_check_pub_key() are also called by a number ofother OpenSSL functions. An application calling any of those otherfunctions may similarly be affected. The other functions affected by thisare DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate().Also vulnerable are the OpenSSL pkey command line application when using the"-pubcheck" option, as well as the OpenSSL genpkey command line application.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2017-3736

  - CVSS Score: 4

  - Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

- Vulnerability: CVE-2017-3737

  - CVSS Score: 4.3

– Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

- Vulnerability: CVE-2019-1547

  – CVSS Score: 1.9

  – Description: Normally in OpenSSL EC groups always have a co-factor present and this is used in side channel resistant code paths. However, in some cases, it is possible to construct a group using explicit parameters (instead of using a named curve). In those cases it is possible that such a group does not have the cofactor present. This can occur even where all the parameters match a known named curve. If such a curve is used then OpenSSL falls back to non-side channel resistant code paths which may result in full key recovery during an ECDSA signature operation. In order to be vulnerable an attacker would have to have the ability to time the creation of a large number of signatures where explicit parameters with no co-factor present are in use by an application using libcrypto. For the avoidance of doubt libssl is not vulnerable because explicit parameters are never used. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).

- Vulnerability: CVE-2017-3735

  – CVSS Score: 5

  – Description: While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL before 1.0.2m and 1.1.0g.

- Vulnerability: CVE-2009-2299

  – CVSS Score: 5

  – Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2022-1292

  – CVSS Score: 10

– Description: The c_rehash script does not properly sanitise shell metacharacters
to prevent command injection. This script is distributed by
some operating systems in a manner where it is automatically
executed. On such operating systems, an attacker could execute
arbitrary commands with the privileges of the script. Use of the
c_rehash script is considered obsolete and should be replaced by the
OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected
3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n).
Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).

- Vulnerability: CVE-2017-3738

  – CVSS Score: 4.3

  – Description: There is an overflow bug in the AVX2 Montgomery multiplication
  procedure used in exponentiation with 1024-bit moduli. No EC
  algorithms are affected. Analysis suggests that attacks against
  RSA and DSA as a result of this defect would be very difficult to
  perform and are not believed likely. Attacks against DH1024 are
  considered just feasible, because most of the work necessary to
  deduce information about a private key may be performed offline. The
  amount of resources required for such an attack would be significant.
  However, for an attack on TLS to be meaningful, the server would have
  to share the DH1024 private key among multiple clients, which is no
  longer an option since CVE-2016-0701. This only affects processors
  that support the AVX2 but not ADX extensions like Intel Haswell
  (4th generation). Note: The impact from this issue is similar to
  CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version
  1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n.
  Due to the low severity of this issue we are not issuing a new
  release of OpenSSL 1.1.0 at this time. The fix will be included in
  OpenSSL 1.1.0h when it becomes available. The fix is also available
  in commit e502cc86d in the OpenSSL git repository.

- Vulnerability: CVE-2012-4001

  – CVSS Score: 5

  – Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server
  does not properly verify its host name, which allows remote attackers
  to trigger HTTP requests to arbitrary hosts via unspecified vectors,
  as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2022-37436

  – CVSS Score: N/A

  – Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause
  the response headers to be truncated early, resulting in some headers
  being incorporated into the response body. If the later headers have
  any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2021-23840

  – CVSS Score: 5

- Description: Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate
  may overflow the output length argument in some cases where the input
  length is close to the maximum permissable length for an integer on
  the platform. In such cases the return value from the function call
  will be 1 (indicating success), but the output length value will be
  negative. This could cause applications to behave incorrectly or
  crash. OpenSSL versions 1.1.1i and below are affected by this issue.
  Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL
  versions 1.0.2x and below are affected by this issue. However
  OpenSSL 1.0.2 is out of support and no longer receiving public
  updates. Premium support customers of OpenSSL 1.0.2 should upgrade
  to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL
  1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected
  1.0.2-1.0.2x).

- Vulnerability: CVE-2018-0737

  - CVSS Score: 4.3
  - Description: The OpenSSL RSA Key generation algorithm has been shown to be
    vulnerable to a cache timing side channel attack. An attacker with
    sufficient access to mount cache timing attacks during the RSA key
    generation process could recover the private key. Fixed in OpenSSL
    1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev
    (Affected 1.0.2b-1.0.2o).

- Vulnerability: CVE-2018-0734

  - CVSS Score: 4.3
  - Description: The OpenSSL DSA signature algorithm has been shown to be vulnerable
    to a timing side channel attack. An attacker could use variations
    in the signing algorithm to recover the private key. Fixed in
    OpenSSL 1.1.1a (Affected 1.1.1). Fixed in OpenSSL 1.1.0j (Affected
    1.1.0-1.1.0i). Fixed in OpenSSL 1.0.2q (Affected 1.0.2-1.0.2p).

- Vulnerability: CVE-2018-0732

  - CVSS Score: 5
  - Description: During key agreement in a TLS handshake using a DH(E) based
    ciphersuite a malicious server can send a very large prime value
    to the client. This will cause the client to spend an unreasonably
    long period of time generating a key for this prime resulting in a
    hang until the client has finished. This could be exploited in a
    Denial Of Service attack. Fixed in OpenSSL 1.1.0i-dev (Affected
    1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2-1.0.2o).

- Vulnerability: CVE-2017-9788

  - CVSS Score: 6.4
  - Description: In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value
    placeholder in [Proxy-]Authorization headers of type 'Digest' was
    not initialized or reset before or between successive key=value
    assignments by mod_auth_digest. Providing an initial key with no
    '=' assignment could reflect the stale value of uninitialized pool
    memory used by the prior request, leading to leakage of potentially
    confidential information, and a segfault in other cases resulting in
    denial of service.

- Vulnerability: CVE-2018-0739

  - CVSS Score: 4.3

- Description: Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o (Affected 1.0.2b-1.0.2n).

- Vulnerability: CVE-2014-8109

  - CVSS Score: 4.3
  - Description: mod_lua.c in the mod_lua module in the Apache HTTP Server 2.3.x and 2.4.x through 2.4.10 does not support an httpd configuration in which the same Lua authorization provider is used with different arguments within different contexts, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives, as demonstrated by a configuration that specifies authorization for one group to access a certain directory, and authorization for a second group to access a second directory.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2016-2161

  - CVSS Score: 5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.23, malicious input to mod_auth_digest can cause the server to crash, and each instance continues to crash even for subsequently valid requests.

- Vulnerability: CVE-2016-8612

  - CVSS Score: 3.3
  - Description: Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.

- Vulnerability: CVE-2019-1552

  - CVSS Score: 1.9

- Description: OpenSSL has internal defaults for a directory tree where it
             can find a configuration file as well as certificates used for
             verification in TLS. This directory is most commonly referred to
             as OPENSSLDIR, and is configurable with the --prefix / --openssldir
             configuration options. For OpenSSL versions 1.1.0 and 1.1.1, the
             mingw configuration targets assume that resulting programs and
             libraries are installed in a Unix-like environment and the default
             prefix for program installation as well as for OPENSSLDIR should be
             '/usr/local'. However, mingw programs are Windows programs, and as
             such, find themselves looking at sub-directories of 'C:/usr/local',
             which may be world writable, which enables untrusted users to modify
             OpenSSL's default configuration, insert CA certificates, modify (or
             even replace) existing engine modules, etc. For OpenSSL 1.0.2,
             '/usr/local/ssl' is used as default for OPENSSLDIR on all Unix and
             Windows targets, including Visual C builds. However, some build
             instructions for the diverse Windows targets on 1.0.2 encourage
             you to specify your own --prefix. OpenSSL versions 1.1.1, 1.1.0
             and 1.0.2 are affected by this issue. Due to the limited scope
             of affected deployments this has been assessed as low severity and
             therefore we are not creating new releases at this time. Fixed
             in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL
             1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected
             1.0.2-1.0.2s).

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5
             for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM
             Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows
             use an improper encryption algorithm and a weak key for maintaining
             the stored data of the node secret for the SecurID Authentication
             API, which allows local users to obtain sensitive information via
             cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication
             Agent 7.1 before 7.1.1 for Web for Internet Information Services,
             and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to
             inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2019-1551

  - CVSS Score: 5
  - Description: There is an overflow bug in the x64_64 Montgomery squaring procedure
             used in exponentiation with 512-bit moduli. No EC algorithms are
             affected. Analysis suggests that attacks against 2-prime RSA1024,
             3-prime RSA1536, and DSA1024 as a result of this defect would be
             very difficult to perform and are not believed likely. Attacks
             against DH512 are considered just feasible. However, for an attack
             the target would have to re-use the DH512 private key, which is not
             recommended anyway. Also applications directly using the low level
             API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME. Fixed
             in OpenSSL 1.1.1e (Affected 1.1.1-1.1.1d). Fixed in OpenSSL 1.0.2u
             (Affected 1.0.2-1.0.2t).

- Vulnerability: CVE-2019-1559

  - CVSS Score: 4.3

- Description: If an application encounters a fatal protocol error and then calls
  SSL_shutdown() twice (once to send a close_notify, and once to
  receive one) then OpenSSL can respond differently to the calling
  application if a 0 byte record is received with invalid padding
  compared to if a 0 byte record is received with an invalid MAC. If
  the application then behaves differently based on that in a way that
  is detectable to the remote peer, then this amounts to a padding
  oracle that could be used to decrypt data. In order for this to be
  exploitable "non-stitched" ciphersuites must be in use. Stitched
  ciphersuites are optimised implementations of certain commonly
  used ciphersuites. Also the application must call SSL_shutdown()
  twice even if a protocol error has occurred (applications should
  not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected
  1.0.2-1.0.2q).

- **Vulnerability:** CVE-2023-45802

  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a
    time window were the request's memory resources were not reclaimed
    immediately. Instead, de-allocation was deferred to connection
    close. A client could send new requests and resets, keeping the
    connection busy and open and causing the memory footprint to keep
    on growing. On connection close, all resources were reclaimed, but
    the process might run out of memory before that.This was found by
    the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset
    Exploit) with their own test client. During "normal" HTTP/2 use, the
    probability to hit this bug is very low. The kept memory would not
    become noticeable before the connection closes or times out.Users are
    recommended to upgrade to version 2.4.58, which fixes the issue.

- **Vulnerability:** CVE-2018-1283

  - CVSS Score: 3.5
  - Description: In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to
    forward its session data to CGI applications (SessionEnv on, not
    the default), a remote user may influence their content by using a
    "Session" header. This comes from the "HTTP_SESSION" variable name
    used by mod_session to forward its data to CGIs, since the prefix
    "HTTP_" is also used by the Apache HTTP Server to pass HTTP header
    fields, per CGI specifications.

- **Vulnerability:** CVE-2020-1968

  - CVSS Score: 4.3
  - Description: The Raccoon attack exploits a flaw in the TLS specification which
    can lead to an attacker being able to compute the pre-master
    secret in connections which have used a Diffie-Hellman (DH) based
    ciphersuite. In such a case this would result in the attacker being
    able to eavesdrop on all encrypted communications sent over that TLS
    connection. The attack can only be exploited if an implementation
    re-uses a DH secret across multiple TLS connections. Note that this
    issue only impacts DH ciphersuites and not ECDH ciphersuites. This
    issue affects OpenSSL 1.0.2 which is out of support and no longer
    receiving public updates. OpenSSL 1.1.1 is not vulnerable to this
    issue. Fixed in OpenSSL 1.0.2w (Affected 1.0.2-1.0.2v).

- **Vulnerability:** CVE-2019-0217

  - CVSS Score: 6

– Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.

- Vulnerability: CVE-2022-28615

  – CVSS Score: 6.4
  – Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- Vulnerability: CVE-2022-28614

  – CVSS Score: 5
  – Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

11.11 IP Address: 159.149.53.215

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 4

- High Vulnerabilities: 22

- Medium Vulnerabilities: 164

- Low Vulnerabilities: 16

- Total Vulnerabilities: 206

Services Running on IP Address

- Service: Apache httpd

  - Port: 80
  - Version: 2.4.6
  - Location: https://www.alessandromanzoni.org/

- Service: Apache httpd

  - Port: 443
  - Version: 2.4.6
  - Location: http://www.alessandromanzoni.org/

Vulnerabilities Found

- Vulnerability: CVE-2014-0117

  - CVSS Score: 4.3
  - Description: The mod_proxy module in the Apache HTTP Server 2.4.x before 2.4.10, when a reverse proxy is enabled, allows remote attackers to cause a denial of service (child-process crash) via a crafted HTTP Connection header.

- Vulnerability: CVE-2017-7679

  - CVSS Score: 7.5
  - Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

- Vulnerability: CVE-2017-9798

  - CVSS Score: 5
  - Description: Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.

- Vulnerability: CVE-2015-3185

  - CVSS Score: 4.3

- Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

- Vulnerability: CVE-2015-3184

  - CVSS Score: 5
  - Description: mod_authz_svn in Apache Subversion 1.7.x before 1.7.21 and 1.8.x before 1.8.14, when using Apache httpd 2.4.x, does not properly restrict anonymous access, which allows remote anonymous users to read hidden files via the path name.

- Vulnerability: CVE-2015-3183

  - CVSS Score: 5
  - Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

- Vulnerability: CVE-2013-4365

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2018-5407

  - CVSS Score: 1.9
  - Description: Simultaneous Multi-threading (SMT) in processors can enable local users to exploit software vulnerable to timing attacks via a side-channel timing attack on 'port contention'.

- Vulnerability: CVE-2022-28330

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2021-32791

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2021-32792

  - CVSS Score: 4.3

– Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.

- **Vulnerability: CVE-2024-38476**

  – CVSS Score: N/A

  – Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- **Vulnerability: CVE-2024-38477**

  – CVSS Score: N/A

  – Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- **Vulnerability: CVE-2023-31122**

  – CVSS Score: N/A

  – Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- **Vulnerability: CVE-2009-0796**

  – CVSS Score: 2.6

  – Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- **Vulnerability: CVE-2022-2068**

  – CVSS Score: 10

  – Description: In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze).

- **Vulnerability: CVE-2014-0118**

  – CVSS Score: 4.3

  – Description: The deflate_in_filter function in mod_deflate.c in the mod_deflate module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.

- Vulnerability: CVE-2013-6438

  - CVSS Score: 5
  - Description: The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.

- Vulnerability: CVE-2020-1927

  - CVSS Score: 5.8
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.

- Vulnerability: CVE-2023-0286

  - CVSS Score: N/A
  - Description: There is a type confusion vulnerability relating to X.400 address processinginside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING butthe public structure definition for GENERAL_NAME incorrectly specified the typeof the x400Address field as ASN1_TYPE. This field is subsequently interpreted bythe OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than anASN1_STRING.When CRL checking is enabled (i.e. the application sets theX509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to passarbitrary pointers to a memcmp call, enabling them to read memory contents orenact a denial of service. In most cases, the attack requires the attacker toprovide both the certificate chain and CRL, neither of which need to have avalid signature. If the attacker only controls one of these inputs, the otherinput must already contain an X.400 address as a CRL distribution point, whichis uncommon. As such, this vulnerability is most likely to only affectapplications which have implemented their own functionality for retrieving CRLsover a network.

- Vulnerability: CVE-2023-3817

  - CVSS Score: N/A
  - Description: Issue summary: Checking excessively long DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH key or DH parameters may experience longdelays. Where the key or parameters that are being checked have been obtainedfrom an untrusted source this may lead to a Denial of Service.The function DH_check() performs various checks on DH parameters. After fixingCVE-2023-3446 it was discovered that a large q parameter value can also triggeran overly long computation during some of these checks. A correct q value,if present, cannot be larger than the modulus p parameter, thus it isunnecessary to perform these checks if q is larger than p.An application that calls DH_check() and supplies a key or parameters obtainedfrom an untrusted source could be vulnerable to a Denial of Service attack.The function DH_check() is itself called by a number of other OpenSSL functions.An application calling any of those other functions may similarly be affected.The other functions affected by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable are the OpenSSL dhparam and pkeyparam command line applicationswhen using the "-check" option.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2017-3167
  - CVSS Score: 7.5
  - Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.

- Vulnerability: CVE-2021-32786
  - CVSS Score: 5.8
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, `oidc_validate_redirect_url()` does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring `mod_auth_openidc` to only allow redirection whose destination matches a given regular expression.

- Vulnerability: CVE-2021-32785
  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache (`OIDCCacheEncrypt off`, `OIDCSessionType server-cache`, `OIDCCacheType redis`), `mod_auth_openidc` wrongly performed argument interpolation before passing Redis requests to `hiredis`, which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the `hiredis` API. As a workaround, this vulnerability can be mitigated by setting `OIDCCacheEncrypt` to `on`, as cache keys are cryptographically hashed before use when this option is enabled.

- Vulnerability: CVE-2007-4723
  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2021-44790
  - CVSS Score: 7.5
  - Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

615

- Vulnerability: CVE-2016-4975

  - CVSS Score: 4.3
  - Description: Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).

- Vulnerability: CVE-2020-13938

  - CVSS Score: 2.1
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

- Vulnerability: CVE-2023-2650

  - CVSS Score: N/A
  - Description: Issue summary: Processing some specially crafted ASN.1 object identifiers ordata containing them may be very slow.Impact summary: Applications that use OBJ_obj2txt() directly, or use any ofthe OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no messagesize limit may experience notable to very long delays when processing thosemessages, which may lead to a Denial of Service.An OBJECT IDENTIFIER is composed of a series of numbers - sub-identifiers -most of which have no size limit. OBJ_obj2txt() may be used to translatean ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSLtype ASN1_OBJECT) to its canonical numeric text form, which are thesub-identifiers of the OBJECT IDENTIFIER in decimal form, separated byperiods.When one of the sub-identifiers in the OBJECT IDENTIFIER is very large(these are sizes that are seen as absurdly large, taking up tens or hundredsof KiBs), the translation to a decimal number in text may take a very longtime. The time complexity is $O(n^2)$ with 'n' being the size of thesub-identifiers in bytes (*).With OpenSSL 3.0, support to fetch cryptographic algorithms using names /identifiers in string form was introduced. This includes using OBJECTIDENTIFIERs in canonical numeric text form as identifiers for fetchingalgorithms.Such OBJECT IDENTIFIERs may be received through the ASN.1 structureAlgorithmIdentifier, which is commonly used in multiple protocols to specifywhat cryptographic algorithm should be used to sign or verify, encrypt ordecrypt, or digest passed data.Applications that call OBJ_obj2txt() directly with untrusted data areaffected, with any version of OpenSSL. If the use is for the mere purposeof display, the severity is considered low.In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME,CMS, CMP/CRMF or TS. It also impacts anything that processes X.509certificates, including simple things like verifying its signature.The impact on TLS is relatively low, because all versions of OpenSSL have a100KiB limit on the peer's certificate chain. Additionally, this onlyimpacts clients, or servers that have explicitly enabled clientauthentication.In OpenSSL 1.1.1 and 1.0.2, this only affects displaying diverse objects,such as X.509 certificates. This is assumed to not happen in such a waythat it would cause a Denial of Service, so these versions are considerednot affected by this issue in such a way that it would be cause for concern,and the severity is therefore considered low.

- Vulnerability: CVE-2023-0215

  - CVSS Score: N/A

- Description: The public API function BIO_new_NDEF is a helper function used for streamingASN.1 data via a BIO. It is primarily used internally to OpenSSL to support theSMIME, CMS and PKCS7 streaming capabilities, but may also be called directly byend user applications.The function receives a BIO from the caller, prepends a new BIO_f_asn1 filterBIO onto the front of it to form a BIO chain, and then returns the new head ofthe BIO chain to the caller. Under certain conditions, for example if a CMSrecipient public key is invalid, the new filter BIO is freed and the functionreturns a NULL result indicating a failure. However, in this case, the BIO chainis not properly cleaned up and the BIO passed by the caller still retainsinternal pointers to the previously freed filter BIO. If the caller then goes onto call BIO_pop() on the BIO then a use-after-free will occur. This will mostlikely result in a crash.This scenario occurs directly in the internal function B64_write_ASN1() whichmay cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() onthe BIO. This internal function is in turn called by the public API functionsPEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream,SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7.Other public API functions that may be impacted by this includei2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream andi2d_PKCS7_bio_stream.The OpenSSL cms and smime command line applications are similarly affected.

- Vulnerability: CVE-2020-35452

  - CVSS Score: 6.8
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

- Vulnerability: CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2020-1934

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

- Vulnerability: CVE-2022-36760

  - CVSS Score: N/A
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-4304

  - CVSS Score: N/A

– Description: A timing based side channel exists in the OpenSSL RSA Decryption
            implementationwhich could be sufficient to recover a plaintext
            across a network in aBleichenbacher style attack. To achieve a
            successful decryption an attackerwould have to be able to send a
            very large number of trial messages fordecryption. The vulnerability
            affects all RSA padding modes: PKCS#1 v1.5,RSA-OEAP and RSASVE.For
            example, in a TLS connection, RSA is commonly used by a client to
            send anencrypted pre-master secret to the server. An attacker that
            had observed agenuine connection between a client and a server could
            use this flaw to sendtrial messages to the server and record the time
            taken to process them. After asufficiently large number of messages
            the attacker could recover the pre-mastersecret used for the original
            connection and thus be able to decrypt theapplication data sent over
            that connection.

- Vulnerability: CVE-2019-1563

    – CVSS Score: 4.3

    – Description: In situations where an attacker receives automated notification
            of the success or failure of a decryption attempt an attacker,
            after sending a very large number of messages to be decrypted, can
            recover a CMS/PKCS7 transported encryption key or decrypt any RSA
            encrypted message that was encrypted with the public RSA key, using a
            Bleichenbacher padding oracle attack. Applications are not affected
            if they use a certificate together with the private RSA key to the
            CMS_decrypt or PKCS7_decrypt functions to select the correct recipient
            info to decrypt. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c).
            Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL
            1.0.2t (Affected 1.0.2-1.0.2s).

- Vulnerability: CVE-2014-3523

    – CVSS Score: 5

    – Description: Memory leak in the winnt_accept function in server/mpm/winnt/child.c
            in the WinNT MPM in the Apache HTTP Server 2.4.x before 2.4.10 on
            Windows, when the default AcceptFilter is enabled, allows remote
            attackers to cause a denial of service (memory consumption) via
            crafted requests.

- Vulnerability: CVE-2013-5704

    – CVSS Score: 5

    – Description: The mod_headers module in the Apache HTTP Server 2.2.22 allows remote
            attackers to bypass "RequestHeader unset" directives by placing a
            header in the trailer portion of data sent with chunked transfer
            coding. NOTE: the vendor states "this is not a security issue in
            httpd as such."

- Vulnerability: CVE-2019-17567

    – CVSS Score: 5

    – Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel
            configured on an URL that is not necessarily Upgraded by the origin
            server was tunneling the whole connection regardless, thus allowing
            for subsequent requests on the same connection to pass through
            with no HTTP validation, authentication or authorization possibly
            configured.

- Vulnerability: CVE-2022-31813

    – CVSS Score: 7.5

– Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-*
headers to the origin server based on client side Connection
header hop-by-hop mechanism. This may be used to bypass IP based
authentication on the origin server/application.

- Vulnerability: CVE-2012-4360

  – CVSS Score: 4.3
  – Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module
0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote
attackers to inject arbitrary web script or HTML via unspecified
vectors.

- Vulnerability: CVE-2014-0231

  – CVSS Score: 5
  – Description: The mod_cgid module in the Apache HTTP Server before 2.4.10 does not
have a timeout mechanism, which allows remote attackers to cause a
denial of service (process hang) via a request to a CGI script that
does not read from its stdin file descriptor.

- Vulnerability: CVE-2021-26690

  – CVSS Score: 5
  – Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted
Cookie header handled by mod_session can cause a NULL pointer
dereference and crash, leading to a possible Denial Of Service

- Vulnerability: CVE-2021-26691

  – CVSS Score: 7.5
  – Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted
SessionHeader sent by an origin server could cause a heap overflow

- Vulnerability: CVE-2019-0220

  – CVSS Score: 5
  – Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38.
When the path component of a request URL contains multiple
consecutive slashes ('/'), directives such as LocationMatch and
RewriteRule must account for duplicates in regular expressions while
other aspects of the servers processing will implicitly collapse
them.

- Vulnerability: CVE-2022-30556

  – CVSS Score: 5
  – Description: Apache HTTP Server 2.4.53 and earlier may return lengths to
applications calling r:wsread() that point past the end of the
storage allocated for the buffer.

- Vulnerability: CVE-2021-39275

  – CVSS Score: 7.5
  – Description: ap_escape_quotes() may write beyond the end of a buffer when given
malicious input. No included modules pass untrusted data to these
functions, but third-party / external modules may. This issue
affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2014-3581

  – CVSS Score: 5

- Description: The cache_merge_headers_out function in modules/cache/cache_util.c in the mod_cache module in the Apache HTTP Server before 2.4.11 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty HTTP Content-Type header.

- Vulnerability: CVE-2016-0736

  - CVSS Score: 5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.23, mod_session_crypto was encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This made it vulnerable to padding oracle attacks, particularly with CBC.

- Vulnerability: CVE-2022-29404

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2018-1312

  - CVSS Score: 6.8
  - Description: In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

- Vulnerability: CVE-2006-20001

  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2017-15710

  - CVSS Score: 5
  - Description: In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.

- Vulnerability: CVE-2014-0226

  - CVSS Score: 6.8

- Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

- Vulnerability: CVE-2024-0727

  - CVSS Score: N/A

  - Description: Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSLto crash leading to a potential Denial of Service attackImpact summary: Applications loading files in the PKCS12 format from untrustedsources might terminate abruptly.A file in PKCS12 format can contain certificates and keys and may come from anuntrusted source. The PKCS12 specification allows certain fields to be NULL, butOpenSSL does not correctly check for this case. This can lead to a NULL pointerdereference that results in OpenSSL crashing. If an application processes PKCS12files from an untrusted source using the OpenSSL APIs then that application willbe vulnerable to this issue.OpenSSL APIs that are vulnerable to this are: PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a similar issue in SMIME_write_PKCS7(). However since thisfunction is related to writing data we do not consider it security significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.

- Vulnerability: CVE-2009-3766

  - CVSS Score: 6.8

  - Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when OpenSSL is used, does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

- Vulnerability: CVE-2009-3767

  - CVSS Score: 4.3

  - Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other versions, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2009-3765

  - CVSS Score: 6.8

  - Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2022-22721

  - CVSS Score: 5.8

– Description: If LimitXMLRequestBody is set to allow request bodies larger than
350MB (defaults to 1M) on 32 bit systems an integer overflow happens
which later causes out of bounds writes. This issue affects Apache
HTTP Server 2.4.52 and earlier.

• Vulnerability: CVE-2022-22720

   – CVSS Score: 7.5

   – Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound
connection when errors are encountered discarding the request body,
exposing the server to HTTP Request Smuggling

• Vulnerability: CVE-2019-10092

   – CVSS Score: 4.3

   – Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting
issue was reported affecting the mod_proxy error page. An attacker
could cause the link on the error page to be malformed and instead
point to a page of their choice. This would only be exploitable
where a server was set up with proxying enabled but was misconfigured
in such a way that the Proxy Error page was displayed.

• Vulnerability: CVE-2021-3712

   – CVSS Score: 5.8

   – Description: ASN.1 strings are represented internally within OpenSSL as an
ASN1_STRING structure which contains a buffer holding the string
data and a field holding the buffer length. This contrasts with
normal C strings which are repesented as a buffer for the string
data which is terminated with a NUL (0) byte. Although not a
strict requirement, ASN.1 strings that are parsed using OpenSSL's
own "d2i" functions (and other similar parsing functions) as well
as any string whose value has been set with the ASN1_STRING_set()
function will additionally NUL terminate the byte array in the
ASN1_STRING structure. However, it is possible for applications
to directly construct valid ASN1_STRING structures which do not NUL
terminate the byte array by directly setting the "data" and "length"
fields in the ASN1_STRING array. This can also happen by using
the ASN1_STRING_set0() function. Numerous OpenSSL functions that
print ASN.1 data have been found to assume that the ASN1_STRING byte
array will be NUL terminated, even though this is not guaranteed for
strings that have been directly constructed. Where an application
requests an ASN.1 structure to be printed, and where that ASN.1
structure contains ASN1_STRINGs that have been directly constructed
by the application without NUL terminating the "data" field, then
a read buffer overrun can occur. The same thing can also occur
during name constraints processing of certificates (for example
if a certificate has been directly constructed by the application
instead of loading it via the OpenSSL parsing functions, and the
certificate contains non NUL terminated ASN1_STRING structures).
It can also occur in the X509_get1_email(), X509_REQ_get1_email()
and X509_get1_ocsp() functions. If a malicious actor can cause an
application to directly construct an ASN1_STRING and then process it
through one of the affected OpenSSL functions then this issue could
be hit. This might result in a crash (causing a Denial of Service
attack). It could also result in the disclosure of private memory
contents (such as private keys, or sensitive plaintext). Fixed in
OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za
(Affected 1.0.2-1.0.2y).

• Vulnerability: CVE-2023-0464

- CVSS Score: N/A
- Description: A security vulnerability has been identified in all supported versionsof OpenSSL related to the verification of X.509 certificate chainsthat include policy constraints. Attackers may be able to exploit thisvulnerability by creating a malicious certificate chain that triggersexponential use of computational resources, leading to a denial-of-service(DoS) attack on affected systems.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.

- **Vulnerability: CVE-2023-0465**

  - CVSS Score: N/A
  - Description: Applications that use a non-default option when verifying certificates may bevulnerable to an attack from a malicious CA to circumvent certain checks.Invalid certificate policies in leaf certificates are silently ignored byOpenSSL and other certificate policy checks are skipped for that certificate.A malicious CA could use this to deliberately assert invalid certificate policiesin order to circumvent policy checking on the certificate altogether.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.

- **Vulnerability: CVE-2023-0466**

  - CVSS Score: N/A
  - Description: The function X509_VERIFY_PARAM_add0_policy() is documented toimplicitly enable the certificate policy check when doing certificateverification. However the implementation of the function does notenable the check which allows certificates with invalid or incorrectpolicies to pass the certificate verification.As suddenly enabling the policy check could break existing deployments it wasdecided to keep the existing behavior of the X509_VERIFY_PARAM_add0_policy()function.Instead the applications that require OpenSSL to perform certificatepolicy check need to use X509_VERIFY_PARAM_set1_policies() or explicitlyenable the policy check by calling X509_VERIFY_PARAM_set_flags() withthe X509_V_FLAG_POLICY_CHECK flag argument.Certificate policy checks are disabled by default in OpenSSL and are notcommonly used by applications.

- **Vulnerability: CVE-2019-10098**

  - CVSS Score: 5.8
  - Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.

- **Vulnerability: CVE-2015-0228**

  - CVSS Score: 5
  - Description: The lua_websocket_read function in lua_request.c in the mod_lua module in the Apache HTTP Server through 2.4.12 allows remote attackers to cause a denial of service (child-process crash) by sending a crafted WebSocket Ping frame after a Lua script has called the wsupgrade function.

- **Vulnerability: CVE-2016-5387**

- CVSS Score: 6.8
- Description: The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.

• Vulnerability: CVE-2017-15715

- CVSS Score: 6.8
- Description: In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.

• Vulnerability: CVE-2021-40438

- CVSS Score: 6.8
- Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

• Vulnerability: CVE-2011-1176

- CVSS Score: 4.3
- Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

• Vulnerability: CVE-2022-23943

- CVSS Score: 7.5
- Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

• Vulnerability: CVE-2018-17199

- CVSS Score: 5
- Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

• Vulnerability: CVE-2021-23841

- CVSS Score: 4.3

- Description: The OpenSSL public API function X509_issuer_and_serial_hash() attempts
    to create a unique hash value based on the issuer and serial number
    data contained within an X509 certificate. However it fails to
    correctly handle any errors that may occur while parsing the
    issuer field (which might occur if the issuer field is maliciously
    constructed). This may subsequently result in a NULL pointer deref
    and a crash leading to a potential denial of service attack. The
    function X509_issuer_and_serial_hash() is never directly called by
    OpenSSL itself so applications are only vulnerable if they use this
    function directly and they use it on certificates that may have been
    obtained from untrusted sources. OpenSSL versions 1.1.1i and below
    are affected by this issue. Users of these versions should upgrade
    to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected
    by this issue. However OpenSSL 1.0.2 is out of support and no longer
    receiving public updates. Premium support customers of OpenSSL 1.0.2
    should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j.
    Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL
    1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2018-1301

  - CVSS Score: 4.3
  - Description: A specially crafted request could have crashed the Apache HTTP Server
    prior to version 2.4.30, due to an out of bound access after a size
    limit is reached by reading the HTTP header. This vulnerability
    is considered very hard if not impossible to trigger in non-debug
    mode (both log and build level), so it is classified as low risk for
    common server usage.

- Vulnerability: CVE-2018-1302

  - CVSS Score: 4.3
  - Description: When an HTTP/2 stream was destroyed after being handled, the Apache
    HTTP Server prior to version 2.4.30 could have written a NULL pointer
    potentially to an already freed memory. The memory pools maintained
    by the server make this vulnerability hard to trigger in usual
    configurations, the reporter and the team could not reproduce it
    outside debug builds, so it is classified as low risk.

- Vulnerability: CVE-2018-1303

  - CVSS Score: 5
  - Description: A specially crafted HTTP request header could have crashed the Apache
    HTTP Server prior to version 2.4.30 due to an out of bound read while
    preparing data to be cached in shared memory. It could be used as
    a Denial of Service attack against users of mod_cache_socache. The
    vulnerability is considered as low risk since mod_cache_socache is not
    widely used, mod_cache_disk is not concerned by this vulnerability.

- Vulnerability: CVE-2021-34798

  - CVSS Score: 5
  - Description: Malformed requests may cause the server to dereference a NULL
    pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2023-25690

  - CVSS Score: N/A

- Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0
  through 2.4.55 allow a HTTP Request Smuggling attack.Configurations
  are affected when mod_proxy is enabled along with some form of
  RewriteRule or ProxyPassMatch in which a non-specific pattern
  matches some portion of the user-supplied request-target (URL)
  data and is then re-inserted into the proxied request-target using
  variable substitution. For example, something like:RewriteEngine
  onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1";
  [P]ProxyPassReverse /here/ http://example.com:8080/Request
  splitting/smuggling could result in bypass of access controls in the
  proxy server, proxying unintended URLs to existing origin servers,
  and cache poisoning. Users are recommended to update to at least
  version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2020-11985

  - CVSS Score: 4.3
  - Description: IP address spoofing when proxying using mod_remoteip and mod_rewrite
    For configurations using proxying with mod_remoteip and certain
    mod_rewrite rules, an attacker could spoof their IP address for
    logging and PHP scripts. Note this issue was fixed in Apache HTTP
    Server 2.4.24 but was retrospectively allocated a low severity CVE in
    2020.

- Vulnerability: CVE-2021-4160

  - CVSS Score: 4.3
  - Description: There is a carry propagation bug in the MIPS32 and MIPS64 squaring
    procedure. Many EC algorithms are affected, including some of the
    TLS 1.3 default curves. Impact was not analyzed in detail, because
    the pre-requisites for attack are considered unlikely and include
    reusing private keys. Analysis suggests that attacks against RSA and
    DSA as a result of this defect would be very difficult to perform
    and are not believed likely. Attacks against DH are considered
    just feasible (although very difficult) because most of the work
    necessary to deduce information about a private key may be performed
    offline. The amount of resources required for such an attack would
    be significant. However, for an attack on TLS to be meaningful, the
    server would have to share the DH private key among multiple clients,
    which is no longer an option since CVE-2016-0701. This issue affects
    OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the
    releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For
    the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that
    is available to premium support customers only. It will be made
    available in 1.0.2zc when it is released. The issue only affects
    OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0).
    Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL
    1.0.2zc-dev (Affected 1.0.2-1.0.2zb).

- Vulnerability: CVE-2013-4352

  - CVSS Score: 4.3
  - Description: The cache_invalidate function in modules/cache/cache_storage.c in the
    mod_cache module in the Apache HTTP Server 2.4.6, when a caching
    forward proxy is enabled, allows remote HTTP servers to cause a
    denial of service (NULL pointer dereference and daemon crash) via
    vectors that trigger a missing hostname value.

- Vulnerability: CVE-2022-26377

  - CVSS Score: 5

- Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2014-0098

  - CVSS Score: 5
  - Description: The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.

- Vulnerability: CVE-2016-8743

  - CVSS Score: 5
  - Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

- Vulnerability: CVE-2024-40898

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2024-38474

  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2022-0778

  - CVSS Score: 5

- Description: The BN_mod_sqrt() function, which computes a modular square root,
  contains a bug that can cause it to loop forever for non-prime
  moduli. Internally this function is used when parsing certificates
  that contain elliptic curve public keys in compressed form or
  explicit elliptic curve parameters with a base point encoded in
  compressed form. It is possible to trigger the infinite loop by
  crafting a certificate that has invalid explicit curve parameters.
  Since certificate parsing happens prior to verification of the
  certificate signature, any process that parses an externally supplied
  certificate may thus be subject to a denial of service attack. The
  infinite loop can also be reached when parsing crafted private
  keys as they can contain explicit elliptic curve parameters. Thus
  vulnerable situations include: - TLS clients consuming server
  certificates - TLS servers consuming client certificates - Hosting
  providers taking certificates or private keys from customers
  - Certificate authorities parsing certification requests from
  subscribers - Anything else which parses ASN.1 elliptic curve
  parameters Also any other applications that use the BN_mod_sqrt()
  where the attacker can control the parameter values are vulnerable
  to this DoS issue. In the OpenSSL 1.0.2 version the public key is
  not parsed during initial parsing of the certificate which makes
  it slightly harder to trigger the infinite loop. However any
  operation which requires the public key from the certificate will
  trigger the infinite loop. In particular the attacker can use a
  self-signed certificate to trigger the loop during verification
  of the certificate signature. This issue affects OpenSSL versions
  1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n
  and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected
  3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m).
  Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

- Vulnerability: CVE-2020-1971

  - CVSS Score: 4.3

- Description: The X.509 GeneralName type is a generic type for representing
    different types of names. One of those name types is known as
    EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which
    compares different instances of a GENERAL_NAME to see if they
    are equal or not. This function behaves incorrectly when both
    GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference
    and a crash may occur leading to a possible denial of service
    attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two
    purposes: 1) Comparing CRL distribution point names between an
    available CRL and a CRL distribution point embedded in an X509
    certificate 2) When verifying that a timestamp response token signer
    matches the timestamp authority name (exposed via the API functions
    TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can
    control both items being compared then that attacker could trigger
    a crash. For example if the attacker can trick a client or server
    into checking a malicious certificate against a malicious CRL then
    this may occur. Note that some applications automatically download
    CRLs based on a URL embedded in a certificate. This checking happens
    prior to the signatures on the certificate and CRL being verified.
    OpenSSL's s_server, s_client and verify tools have support for the
    "-crl_download" option which implements automatic CRL downloading and
    this attack has been demonstrated to work against those tools. Note
    that an unrelated bug means that affected versions of OpenSSL cannot
    parse or construct correct encodings of EDIPARTYNAME. However it is
    possible to construct a malformed EDIPARTYNAME that OpenSSL's parser
    will accept and hence trigger this attack. All OpenSSL 1.1.1 and
    1.0.2 versions are affected by this issue. Other OpenSSL releases
    are out of support and have not been checked. Fixed in OpenSSL
    1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected
    1.0.2-1.0.2w).

- Vulnerability: CVE-2009-1390

  - CVSS Score: 6.8
  - Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2)
    GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS
    certificate in the chain is accepted instead of verifying the entire
    chain, which allows remote attackers to spoof trusted servers via a
    man-in-the-middle attack.

- Vulnerability: CVE-2012-3526

  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the
    Apache HTTP Server allows remote attackers to cause a denial of
    service (server or application crash) via multiple X-Forwarded-For
    headers in a request.

- Vulnerability: CVE-2023-5678

  - CVSS Score: N/A

– Description: Issue summary: Generating excessively long X9.42 DH keys or checkingexcessively long X9.42 DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_generate_key() togenerate an X9.42 DH key may experience long delays. Likewise, applicationsthat use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check()to check an X9.42 DH key or X9.42 DH parameters may experience long delays.Where the key or parameters that are being checked have been obtained froman untrusted source this may lead to a Denial of Service.While DH_check() performs all the necessary checks (as of CVE-2023-3817),DH_check_pub_key() doesn't make any of these checks, and is thereforevulnerable for excessively large P and Q parameters.Likewise, while DH_generate_key() performs a check for an excessively largeP, it doesn't check for an excessively large Q.An application that calls DH_generate_key() or DH_check_pub_key() andsupplies a key or parameters obtained from an untrusted source could bevulnerable to a Denial of Service attack.DH_generate_key() and DH_check_pub_key() are also called by a number ofother OpenSSL functions. An application calling any of those otherfunctions may similarly be affected. The other functions affected by thisare DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate().Also vulnerable are the OpenSSL pkey command line application when using the"-pubcheck" option, as well as the OpenSSL genpkey command line application.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2017-3736

    – CVSS Score: 4

    – Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

- Vulnerability: CVE-2017-3737

    – CVSS Score: 4.3

– Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

- Vulnerability: CVE-2019-1547

  – CVSS Score: 1.9

  – Description: Normally in OpenSSL EC groups always have a co-factor present and this is used in side channel resistant code paths. However, in some cases, it is possible to construct a group using explicit parameters (instead of using a named curve). In those cases it is possible that such a group does not have the cofactor present. This can occur even where all the parameters match a known named curve. If such a curve is used then OpenSSL falls back to non-side channel resistant code paths which may result in full key recovery during an ECDSA signature operation. In order to be vulnerable an attacker would have to have the ability to time the creation of a large number of signatures where explicit parameters with no co-factor present are in use by an application using libcrypto. For the avoidance of doubt libssl is not vulnerable because explicit parameters are never used. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).

- Vulnerability: CVE-2017-3735

  – CVSS Score: 5

  – Description: While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL before 1.0.2m and 1.1.0g.

- Vulnerability: CVE-2009-2299

  – CVSS Score: 5

  – Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2022-1292

  – CVSS Score: 10

- Description: The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n). Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).

- Vulnerability: CVE-2017-3738

  - CVSS Score: 4.3
  - Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

- Vulnerability: CVE-2012-4001

  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2022-37436

  - CVSS Score: N/A
  - Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2021-23840

  - CVSS Score: 5

- Description: Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissable length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2018-0737

  - CVSS Score: 4.3
  - Description: The OpenSSL RSA Key generation algorithm has been shown to be vulnerable to a cache timing side channel attack. An attacker with sufficient access to mount cache timing attacks during the RSA key generation process could recover the private key. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2b-1.0.2o).

- Vulnerability: CVE-2018-0734

  - CVSS Score: 4.3
  - Description: The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.1a (Affected 1.1.1). Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.0.2q (Affected 1.0.2-1.0.2p).

- Vulnerability: CVE-2018-0732

  - CVSS Score: 5
  - Description: During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime value to the client. This will cause the client to spend an unreasonably long period of time generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2-1.0.2o).

- Vulnerability: CVE-2017-9788

  - CVSS Score: 6.4
  - Description: In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.

- Vulnerability: CVE-2018-0739

  - CVSS Score: 4.3

- Description: Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o (Affected 1.0.2b-1.0.2n).

- Vulnerability: CVE-2014-8109

  - CVSS Score: 4.3
  - Description: mod_lua.c in the mod_lua module in the Apache HTTP Server 2.3.x and 2.4.x through 2.4.10 does not support an httpd configuration in which the same Lua authorization provider is used with different arguments within different contexts, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives, as demonstrated by a configuration that specifies authorization for one group to access a certain directory, and authorization for a second group to access a second directory.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2016-2161

  - CVSS Score: 5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.23, malicious input to mod_auth_digest can cause the server to crash, and each instance continues to crash even for subsequently valid requests.

- Vulnerability: CVE-2016-8612

  - CVSS Score: 3.3
  - Description: Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.

- Vulnerability: CVE-2019-1552

  - CVSS Score: 1.9

- Description: OpenSSL has internal defaults for a directory tree where it
  can find a configuration file as well as certificates used for
  verification in TLS. This directory is most commonly referred to
  as OPENSSLDIR, and is configurable with the --prefix / --openssldir
  configuration options. For OpenSSL versions 1.1.0 and 1.1.1, the
  mingw configuration targets assume that resulting programs and
  libraries are installed in a Unix-like environment and the default
  prefix for program installation as well as for OPENSSLDIR should be
  '/usr/local'. However, mingw programs are Windows programs, and as
  such, find themselves looking at sub-directories of 'C:/usr/local',
  which may be world writable, which enables untrusted users to modify
  OpenSSL's default configuration, insert CA certificates, modify (or
  even replace) existing engine modules, etc. For OpenSSL 1.0.2,
  '/usr/local/ssl' is used as default for OPENSSLDIR on all Unix and
  Windows targets, including Visual C builds. However, some build
  instructions for the diverse Windows targets on 1.0.2 encourage
  you to specify your own --prefix. OpenSSL versions 1.1.1, 1.1.0
  and 1.0.2 are affected by this issue. Due to the limited scope
  of affected deployments this has been assessed as low severity and
  therefore we are not creating new releases at this time. Fixed
  in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL
  1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected
  1.0.2-1.0.2s).

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5
    for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM
    Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows
    use an improper encryption algorithm and a weak key for maintaining
    the stored data of the node secret for the SecurID Authentication
    API, which allows local users to obtain sensitive information via
    cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication
    Agent 7.1 before 7.1.1 for Web for Internet Information Services,
    and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to
    inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2019-1551

  - CVSS Score: 5
  - Description: There is an overflow bug in the x64_64 Montgomery squaring procedure
    used in exponentiation with 512-bit moduli. No EC algorithms are
    affected. Analysis suggests that attacks against 2-prime RSA1024,
    3-prime RSA1536, and DSA1024 as a result of this defect would be
    very difficult to perform and are not believed likely. Attacks
    against DH512 are considered just feasible. However, for an attack
    the target would have to re-use the DH512 private key, which is not
    recommended anyway. Also applications directly using the low level
    API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME. Fixed
    in OpenSSL 1.1.1e (Affected 1.1.1-1.1.1d). Fixed in OpenSSL 1.0.2u
    (Affected 1.0.2-1.0.2t).

- Vulnerability: CVE-2019-1559

  - CVSS Score: 4.3

- Description: If an application encounters a fatal protocol error and then calls
  SSL_shutdown() twice (once to send a close_notify, and once to
  receive one) then OpenSSL can respond differently to the calling
  application if a 0 byte record is received with invalid padding
  compared to if a 0 byte record is received with an invalid MAC. If
  the application then behaves differently based on that in a way that
  is detectable to the remote peer, then this amounts to a padding
  oracle that could be used to decrypt data. In order for this to be
  exploitable "non-stitched" ciphersuites must be in use. Stitched
  ciphersuites are optimised implementations of certain commonly
  used ciphersuites. Also the application must call SSL_shutdown()
  twice even if a protocol error has occurred (applications should
  not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected
  1.0.2-1.0.2q).

- **Vulnerability:** CVE-2023-45802

  - CVSS Score: N/A

  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a
    time window were the request's memory resources were not reclaimed
    immediately. Instead, de-allocation was deferred to connection
    close. A client could send new requests and resets, keeping the
    connection busy and open and causing the memory footprint to keep
    on growing. On connection close, all resources were reclaimed, but
    the process might run out of memory before that.This was found by
    the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset
    Exploit) with their own test client. During "normal" HTTP/2 use, the
    probability to hit this bug is very low. The kept memory would not
    become noticeable before the connection closes or times out.Users are
    recommended to upgrade to version 2.4.58, which fixes the issue.

- **Vulnerability:** CVE-2018-1283

  - CVSS Score: 3.5

  - Description: In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to
    forward its session data to CGI applications (SessionEnv on, not
    the default), a remote user may influence their content by using a
    "Session" header. This comes from the "HTTP_SESSION" variable name
    used by mod_session to forward its data to CGIs, since the prefix
    "HTTP_" is also used by the Apache HTTP Server to pass HTTP header
    fields, per CGI specifications.

- **Vulnerability:** CVE-2020-1968

  - CVSS Score: 4.3

  - Description: The Raccoon attack exploits a flaw in the TLS specification which
    can lead to an attacker being able to compute the pre-master
    secret in connections which have used a Diffie-Hellman (DH) based
    ciphersuite. In such a case this would result in the attacker being
    able to eavesdrop on all encrypted communications sent over that TLS
    connection. The attack can only be exploited if an implementation
    re-uses a DH secret across multiple TLS connections. Note that this
    issue only impacts DH ciphersuites and not ECDH ciphersuites. This
    issue affects OpenSSL 1.0.2 which is out of support and no longer
    receiving public updates. OpenSSL 1.1.1 is not vulnerable to this
    issue. Fixed in OpenSSL 1.0.2w (Affected 1.0.2-1.0.2v).

- **Vulnerability:** CVE-2019-0217

  - CVSS Score: 6

– Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition
in mod_auth_digest when running in a threaded server could allow a
user with valid credentials to authenticate using another username,
bypassing configured access control restrictions.

- **Vulnerability: CVE-2022-28615**

  – CVSS Score: 6.4
  – Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose
  information due to a read beyond bounds in ap_strcmp_match() when
  provided with an extremely large input buffer. While no code
  distributed with the server can be coerced into such a call,
  third-party modules or lua scripts that use ap_strcmp_match() may
  hypothetically be affected.

- **Vulnerability: CVE-2022-28614**

  – CVSS Score: 5
  – Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier
  may read unintended memory if an attacker can cause the server to
  reflect very large input using ap_rwrite() or ap_rputs(), such as
  with mod_luas r:puts() function. Modules compiled and distributed
  separately from Apache HTTP Server that use the 'ap_rputs' function
  and may pass it a very large (INT_MAX or larger) string must be
  compiled against current headers to resolve the issue.

- **Vulnerability: CVE-2014-0117**

  – CVSS Score: 4.3
  – Description: The mod_proxy module in the Apache HTTP Server 2.4.x before 2.4.10,
  when a reverse proxy is enabled, allows remote attackers to cause a
  denial of service (child-process crash) via a crafted HTTP Connection
  header.

- **Vulnerability: CVE-2017-7679**

  – CVSS Score: 7.5
  – Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime
  can read one byte past the end of a buffer when sending a malicious
  Content-Type response header.

- **Vulnerability: CVE-2017-9798**

  – CVSS Score: 5
  – Description: Apache httpd allows remote attackers to read secret data from process
  memory if the Limit directive can be set in a user's .htaccess file,
  or if httpd.conf has certain misconfigurations, aka Optionsbleed.
  This affects the Apache HTTP Server through 2.2.34 and 2.4.x through
  2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request
  when attempting to read secret data. This is a use-after-free
  issue and thus secret data is not always sent, and the specific data
  depends on many factors including configuration. Exploitation with
  .htaccess can be blocked with a patch to the ap_limit_section function
  in server/core.c.

- **Vulnerability: CVE-2015-3185**

  – CVSS Score: 4.3
  – Description: The ap_some_auth_required function in server/request.c in the Apache
  HTTP Server 2.4.x before 2.4.14 does not consider that a Require
  directive may be associated with an authorization setting rather
  than an authentication setting, which allows remote attackers to
  bypass intended access restrictions in opportunistic circumstances
  by leveraging the presence of a module that relies on the 2.2 API
  behavior.

- Vulnerability: CVE-2015-3184

  – CVSS Score: 5
  – Description: mod_authz_svn in Apache Subversion 1.7.x before 1.7.21 and 1.8.x
                 before 1.8.14, when using Apache httpd 2.4.x, does not properly
                 restrict anonymous access, which allows remote anonymous users to
                 read hidden files via the path name.

- Vulnerability: CVE-2015-3183

  – CVSS Score: 5
  – Description: The chunked transfer coding implementation in the Apache HTTP
                 Server before 2.4.14 does not properly parse chunk headers,
                 which allows remote attackers to conduct HTTP request smuggling
                 attacks via a crafted request, related to mishandling of large
                 chunk-size values and invalid chunk-extension characters in
                 modules/http/http_filters.c.

- Vulnerability: CVE-2013-4365

  – CVSS Score: 7.5
  – Description: Heap-based buffer overflow in the fcgid_header_bucket_read function
                 in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache
                 HTTP Server allows remote attackers to have an unspecified impact via
                 unknown vectors.

- Vulnerability: CVE-2018-5407

  – CVSS Score: 1.9
  – Description: Simultaneous Multi-threading (SMT) in processors can enable local
                 users to exploit software vulnerable to timing attacks via a
                 side-channel timing attack on 'port contention'.

- Vulnerability: CVE-2022-28330

  – CVSS Score: 5
  – Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond
                 bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2021-32791

  – CVSS Score: 4.3
  – Description: mod_auth_openidc is an authentication/authorization module for the
                 Apache 2.x HTTP server that functions as an OpenID Connect Relying
                 Party, authenticating users against an OpenID Connect Provider.
                 In mod_auth_openidc before version 2.4.9, the AES GCM encryption in
                 mod_auth_openidc uses a static IV and AAD. It is important to fix
                 because this creates a static nonce and since aes-gcm is a stream
                 cipher, this can lead to known cryptographic issues, since the same
                 key is being reused. From 2.4.9 onwards this has been patched to use
                 dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2021-32792

  – CVSS Score: 4.3
  – Description: mod_auth_openidc is an authentication/authorization module for the
                 Apache 2.x HTTP server that functions as an OpenID Connect Relying
                 Party, authenticating users against an OpenID Connect Provider. In
                 mod_auth_openidc before version 2.4.9, there is an XSS vulnerability
                 in when using 'OIDCPreservePost On'.

- Vulnerability: CVE-2024-38476

- CVSS Score: N/A
- Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

• Vulnerability: CVE-2024-38477

- CVSS Score: N/A
- Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

• Vulnerability: CVE-2023-31122

- CVSS Score: N/A
- Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

• Vulnerability: CVE-2009-0796

- CVSS Score: 2.6
- Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

• Vulnerability: CVE-2022-2068

- CVSS Score: 10
- Description: In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze).

• Vulnerability: CVE-2014-0118

- CVSS Score: 4.3
- Description: The deflate_in_filter function in mod_deflate.c in the mod_deflate module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.

• Vulnerability: CVE-2013-6438

- CVSS Score: 5

- Description: The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.

- Vulnerability: CVE-2020-1927

  - CVSS Score: 5.8
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.

- Vulnerability: CVE-2023-0286

  - CVSS Score: N/A
  - Description: There is a type confusion vulnerability relating to X.400 address processinginside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING butthe public structure definition for GENERAL_NAME incorrectly specified the typeof the x400Address field as ASN1_TYPE. This field is subsequently interpreted bythe OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than anASN1_STRING.When CRL checking is enabled (i.e. the application sets theX509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to passarbitrary pointers to a memcmp call, enabling them to read memory contents orenact a denial of service. In most cases, the attack requires the attacker toprovide both the certificate chain and CRL, neither of which need to have avalid signature. If the attacker only controls one of these inputs, the otherinput must already contain an X.400 address as a CRL distribution point, whichis uncommon. As such, this vulnerability is most likely to only affectapplications which have implemented their own functionality for retrieving CRLsover a network.

- Vulnerability: CVE-2023-3817

  - CVSS Score: N/A
  - Description: Issue summary: Checking excessively long DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH key or DH parameters may experience longdelays. Where the key or parameters that are being checked have been obtainedfrom an untrusted source this may lead to a Denial of Service.The function DH_check() performs various checks on DH parameters. After fixingCVE-2023-3446 it was discovered that a large q parameter value can also triggeran overly long computation during some of these checks. A correct q value,if present, cannot be larger than the modulus p parameter, thus it isunnecessary to perform these checks if q is larger than p.An application that calls DH_check() and supplies a key or parameters obtainedfrom an untrusted source could be vulnerable to a Denial of Service attack.The function DH_check() is itself called by a number of other OpenSSL functions.An application calling any of those other functions may similarly be affected.The other functions affected by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable are the OpenSSL dhparam and pkeyparam command line applicationswhen using the "-check" option.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2017-3167

- CVSS Score: 7.5
- Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.

- Vulnerability: CVE-2021-32786

  - CVSS Score: 5.8
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, `oidc_validate_redirect_url()` does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring `mod_auth_openidc` to only allow redirection whose destination matches a given regular expression.

- Vulnerability: CVE-2021-32785

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache (`OIDCCacheEncrypt off`, `OIDCSessionType server-cache`, `OIDCCacheType redis`), `mod_auth_openidc` wrongly performed argument interpolation before passing Redis requests to `hiredis`, which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the `hiredis` API. As a workaround, this vulnerability can be mitigated by setting `OIDCCacheEncrypt` to `on`, as cache keys are cryptographically hashed before use when this option is enabled.

- Vulnerability: CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2021-44790

  - CVSS Score: 7.5
  - Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

- Vulnerability: CVE-2016-4975

  – CVSS Score: 4.3
  – Description: Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).

- Vulnerability: CVE-2020-13938

  – CVSS Score: 2.1
  – Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

- Vulnerability: CVE-2023-2650

  – CVSS Score: N/A
  – Description: Issue summary: Processing some specially crafted ASN.1 object identifiers ordata containing them may be very slow.Impact summary: Applications that use OBJ_obj2txt() directly, or use any ofthe OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no messagesize limit may experience notable to very long delays when processing thosemessages, which may lead to a Denial of Service.An OBJECT IDENTIFIER is composed of a series of numbers – sub-identifiers -most of which have no size limit. OBJ_obj2txt() may be used to translatean ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSLtype ASN1_OBJECT) to its canonical numeric text form, which are thesub-identifiers of the OBJECT IDENTIFIER in decimal form, separated byperiods.When one of the sub-identifiers in the OBJECT IDENTIFIER is very large(these are sizes that are seen as absurdly large, taking up tens or hundredsof KiBs), the translation to a decimal number in text may take a very longtime. The time complexity is O(n$\hat{2}$) with 'n' being the size of thesub-identifiers in bytes (*).With OpenSSL 3.0, support to fetch cryptographic algorithms using names /identifiers in string form was introduced. This includes using OBJECTIDENTIFIERs in canonical numeric text form as identifiers for fetchingalgorithms.Such OBJECT IDENTIFIERs may be received through the ASN.1 structureAlgorithmIdentifier, which is commonly used in multiple protocols to specifywhat cryptographic algorithm should be used to sign or verify, encrypt ordecrypt, or digest passed data.Applications that call OBJ_obj2txt() directly with untrusted data areaffected, with any version of OpenSSL. If the use is for the mere purposeof display, the severity is considered low.In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME,CMS, CMP/CRMF or TS. It also impacts anything that processes X.509certificates, including simple things like verifying its signature.The impact on TLS is relatively low, because all versions of OpenSSL have a100KiB limit on the peer's certificate chain. Additionally, this onlyimpacts clients, or servers that have explicitly enabled clientauthentication.In OpenSSL 1.1.1 and 1.0.2, this only affects displaying diverse objects,such as X.509 certificates. This is assumed to not happen in such a waythat it would cause a Denial of Service, so these versions are considerednot affected by this issue in such a way that it would be cause for concern,and the severity is therefore considered low.

- Vulnerability: CVE-2023-0215

  – CVSS Score: N/A

– Description: The public API function BIO_new_NDEF is a helper function used for streamingASN.1 data via a BIO. It is primarily used internally to OpenSSL to support theSMIME, CMS and PKCS7 streaming capabilities, but may also be called directly byend user applications.The function receives a BIO from the caller, prepends a new BIO_f_asn1 filterBIO onto the front of it to form a BIO chain, and then returns the new head ofthe BIO chain to the caller. Under certain conditions, for example if a CMSrecipient public key is invalid, the new filter BIO is freed and the functionreturns a NULL result indicating a failure. However, in this case, the BIO chainis not properly cleaned up and the BIO passed by the caller still retainsinternal pointers to the previously freed filter BIO. If the caller then goes onto call BIO_pop() on the BIO then a use-after-free will occur. This will mostlikely result in a crash.This scenario occurs directly in the internal function B64_write_ASN1() whichmay cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() onthe BIO. This internal function is in turn called by the public API functionsPEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream,SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7.Other public API functions that may be impacted by this includei2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream andi2d_PKCS7_bio_stream.The OpenSSL cms and smime command line applications are similarly affected.

- Vulnerability: CVE-2020-35452

  – CVSS Score: 6.8
  – Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

- Vulnerability: CVE-2022-22719

  – CVSS Score: 5
  – Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2020-1934

  – CVSS Score: 5
  – Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

- Vulnerability: CVE-2022-36760

  – CVSS Score: N/A
  – Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-4304

  – CVSS Score: N/A

- Description: A timing based side channel exists in the OpenSSL RSA Decryption implementationwhich could be sufficient to recover a plaintext across a network in aBleichenbacher style attack. To achieve a successful decryption an attackerwould have to be able to send a very large number of trial messages fordecryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5,RSA-OEAP and RSASVE.For example, in a TLS connection, RSA is commonly used by a client to send anencrypted pre-master secret to the server. An attacker that had observed agenuine connection between a client and a server could use this flaw to sendtrial messages to the server and record the time taken to process them. After asufficiently large number of messages the attacker could recover the pre-mastersecret used for the original connection and thus be able to decrypt theapplication data sent over that connection.

- Vulnerability: CVE-2019-1563

  - CVSS Score: 4.3
  - Description: In situations where an attacker receives automated notification of the success or failure of a decryption attempt an attacker, after sending a very large number of messages to be decrypted, can recover a CMS/PKCS7 transported encryption key or decrypt any RSA encrypted message that was encrypted with the public RSA key, using a Bleichenbacher padding oracle attack. Applications are not affected if they use a certificate together with the private RSA key to the CMS_decrypt or PKCS7_decrypt functions to select the correct recipient info to decrypt. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).

- Vulnerability: CVE-2014-3523

  - CVSS Score: 5
  - Description: Memory leak in the winnt_accept function in server/mpm/winnt/child.c in the WinNT MPM in the Apache HTTP Server 2.4.x before 2.4.10 on Windows, when the default AcceptFilter is enabled, allows remote attackers to cause a denial of service (memory consumption) via crafted requests.

- Vulnerability: CVE-2013-5704

  - CVSS Score: 5
  - Description: The mod_headers module in the Apache HTTP Server 2.2.22 allows remote attackers to bypass "RequestHeader unset" directives by placing a header in the trailer portion of data sent with chunked transfer coding. NOTE: the vendor states "this is not a security issue in httpd as such."

- Vulnerability: CVE-2019-17567

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

- Vulnerability: CVE-2022-31813

  - CVSS Score: 7.5

- Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-*
                 headers to the origin server based on client side Connection
                 header hop-by-hop mechanism. This may be used to bypass IP based
                 authentication on the origin server/application.

- Vulnerability: CVE-2012-4360

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module
                  0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote
                  attackers to inject arbitrary web script or HTML via unspecified
                  vectors.

- Vulnerability: CVE-2014-0231

  - CVSS Score: 5
  - Description: The mod_cgid module in the Apache HTTP Server before 2.4.10 does not
                  have a timeout mechanism, which allows remote attackers to cause a
                  denial of service (process hang) via a request to a CGI script that
                  does not read from its stdin file descriptor.

- Vulnerability: CVE-2021-26690

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted
                  Cookie header handled by mod_session can cause a NULL pointer
                  dereference and crash, leading to a possible Denial Of Service

- Vulnerability: CVE-2021-26691

  - CVSS Score: 7.5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted
                  SessionHeader sent by an origin server could cause a heap overflow

- Vulnerability: CVE-2019-0220

  - CVSS Score: 5
  - Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38.
                  When the path component of a request URL contains multiple
                  consecutive slashes ('/'), directives such as LocationMatch and
                  RewriteRule must account for duplicates in regular expressions while
                  other aspects of the servers processing will implicitly collapse
                  them.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to
                  applications calling r:wsread() that point past the end of the
                  storage allocated for the buffer.

- Vulnerability: CVE-2021-39275

  - CVSS Score: 7.5
  - Description: ap_escape_quotes() may write beyond the end of a buffer when given
                  malicious input. No included modules pass untrusted data to these
                  functions, but third-party / external modules may. This issue
                  affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2014-3581

  - CVSS Score: 5

– Description: The cache_merge_headers_out function in modules/cache/cache_util.c in the mod_cache module in the Apache HTTP Server before 2.4.11 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty HTTP Content-Type header.

- Vulnerability: CVE-2016-0736

  – CVSS Score: 5
  – Description: In Apache HTTP Server versions 2.4.0 to 2.4.23, mod_session_crypto was encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This made it vulnerable to padding oracle attacks, particularly with CBC.

- Vulnerability: CVE-2022-29404

  – CVSS Score: 5
  – Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2018-1312

  – CVSS Score: 6.8
  – Description: In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

- Vulnerability: CVE-2006-20001

  – CVSS Score: N/A
  – Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2017-15710

  – CVSS Score: 5
  – Description: In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.

- Vulnerability: CVE-2014-0226

  – CVSS Score: 6.8

- Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

- Vulnerability: CVE-2024-0727

  - CVSS Score: N/A

  - Description: Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSLto crash leading to a potential Denial of Service attackImpact summary: Applications loading files in the PKCS12 format from untrustedsources might terminate abruptly.A file in PKCS12 format can contain certificates and keys and may come from anuntrusted source. The PKCS12 specification allows certain fields to be NULL, butOpenSSL does not correctly check for this case. This can lead to a NULL pointerdereference that results in OpenSSL crashing. If an application processes PKCS12files from an untrusted source using the OpenSSL APIs then that application willbe vulnerable to this issue.OpenSSL APIs that are vulnerable to this are: PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a similar issue in SMIME_write_PKCS7(). However since thisfunction is related to writing data we do not consider it security significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.

- Vulnerability: CVE-2009-3766

  - CVSS Score: 6.8

  - Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when OpenSSL is used, does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

- Vulnerability: CVE-2009-3767

  - CVSS Score: 4.3

  - Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other versions, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2009-3765

  - CVSS Score: 6.8

  - Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2022-22721

  - CVSS Score: 5.8

– Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2022-22720

  – CVSS Score: 7.5
  – Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2019-10092

  – CVSS Score: 4.3
  – Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

- Vulnerability: CVE-2021-3712

  – CVSS Score: 5.8
  – Description: ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own "d2i" functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the "data" and "length" fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the "data" field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). It can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y).

- Vulnerability: CVE-2023-0464

- CVSS Score: N/A
- Description: A security vulnerability has been identified in all supported versionsof OpenSSL related to the verification of X.509 certificate chainsthat include policy constraints. Attackers may be able to exploit thisvulnerability by creating a malicious certificate chain that triggersexponential use of computational resources, leading to a denial-of-service(DoS) attack on affected systems.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0465

  - CVSS Score: N/A
  - Description: Applications that use a non-default option when verifying certificates may bevulnerable to an attack from a malicious CA to circumvent certain checks.Invalid certificate policies in leaf certificates are silently ignored byOpenSSL and other certificate policy checks are skipped for that certificate.A malicious CA could use this to deliberately assert invalid certificate policiesin order to circumvent policy checking on the certificate altogether.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0466

  - CVSS Score: N/A
  - Description: The function X509_VERIFY_PARAM_add0_policy() is documented toimplicitly enable the certificate policy check when doing certificateverification. However the implementation of the function does notenable the check which allows certificates with invalid or incorrectpolicies to pass the certificate verification.As suddenly enabling the policy check could break existing deployments it wasdecided to keep the existing behavior of the X509_VERIFY_PARAM_add0_policy()function.Instead the applications that require OpenSSL to perform certificatepolicy check need to use X509_VERIFY_PARAM_set1_policies() or explicitlyenable the policy check by calling X509_VERIFY_PARAM_set_flags() withthe X509_V_FLAG_POLICY_CHECK flag argument.Certificate policy checks are disabled by default in OpenSSL and are notcommonly used by applications.

- Vulnerability: CVE-2019-10098

  - CVSS Score: 5.8
  - Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.

- Vulnerability: CVE-2015-0228

  - CVSS Score: 5
  - Description: The lua_websocket_read function in lua_request.c in the mod_lua module in the Apache HTTP Server through 2.4.12 allows remote attackers to cause a denial of service (child-process crash) by sending a crafted WebSocket Ping frame after a Lua script has called the wsupgrade function.

- Vulnerability: CVE-2016-5387

– CVSS Score: 6.8

– Description: The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18
and therefore does not protect applications from the presence of
untrusted client data in the HTTP_PROXY environment variable, which
might allow remote attackers to redirect an application's outbound
HTTP traffic to an arbitrary proxy server via a crafted Proxy header
in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states
"This mitigation has been assigned the identifier CVE-2016-5387"; in
other words, this is not a CVE ID for a vulnerability.

• Vulnerability: CVE-2017-15715

– CVSS Score: 6.8

– Description: In Apache httpd 2.4.0 to 2.4.29, the expression specified in
<FilesMatch> could match '$' to a newline character in a malicious
filename, rather than matching only the end of the filename. This
could be exploited in environments where uploads of some files are
are externally blocked, but only by matching the trailing portion of
the filename.

• Vulnerability: CVE-2021-40438

– CVSS Score: 6.8

– Description: A crafted request uri-path can cause mod_proxy to forward the request
to an origin server choosen by the remote user. This issue affects
Apache HTTP Server 2.4.48 and earlier.

• Vulnerability: CVE-2011-1176

– CVSS Score: 4.3

– Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk
Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP
Server does not properly handle certain configuration sections that
specify NiceValue but not AssignUserID, which might allow remote
attackers to gain privileges by leveraging the root uid and root gid
of an mpm-itk process.

• Vulnerability: CVE-2022-23943

– CVSS Score: 7.5

– Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server
allows an attacker to overwrite heap memory with possibly attacker
provided data. This issue affects Apache HTTP Server 2.4 version
2.4.52 and prior versions.

• Vulnerability: CVE-2018-17199

– CVSS Score: 5

– Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session
checks the session expiry time before decoding the session. This
causes session expiry time to be ignored for mod_session_cookie
sessions since the expiry time is loaded when the session is decoded.

• Vulnerability: CVE-2021-23841

– CVSS Score: 4.3

– Description: The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack. The function X509_issuer_and_serial_hash() is never directly called by OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on certificates that may have been obtained from untrusted sources. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

• Vulnerability: CVE-2018-1301

  – CVSS Score: 4.3
  – Description: A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.

• Vulnerability: CVE-2018-1302

  – CVSS Score: 4.3
  – Description: When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.

• Vulnerability: CVE-2018-1303

  – CVSS Score: 5
  – Description: A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache. The vulnerability is considered as low risk since mod_cache_socache is not widely used, mod_cache_disk is not concerned by this vulnerability.

• Vulnerability: CVE-2021-34798

  – CVSS Score: 5
  – Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

• Vulnerability: CVE-2023-25690

  – CVSS Score: N/A

- Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2020-11985

  - CVSS Score: 4.3
  - Description: IP address spoofing when proxying using mod_remoteip and mod_rewrite For configurations using proxying with mod_remoteip and certain mod_rewrite rules, an attacker could spoof their IP address for logging and PHP scripts. Note this issue was fixed in Apache HTTP Server 2.4.24 but was retrospectively allocated a low severity CVE in 2020.

- Vulnerability: CVE-2021-4160

  - CVSS Score: 4.3
  - Description: There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that is available to premium support customers only. It will be made available in 1.0.2zc when it is released. The issue only affects OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0). Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL 1.0.2zc-dev (Affected 1.0.2-1.0.2zb).

- Vulnerability: CVE-2013-4352

  - CVSS Score: 4.3
  - Description: The cache_invalidate function in modules/cache/cache_storage.c in the mod_cache module in the Apache HTTP Server 2.4.6, when a caching forward proxy is enabled, allows remote HTTP servers to cause a denial of service (NULL pointer dereference and daemon crash) via vectors that trigger a missing hostname value.

- Vulnerability: CVE-2022-26377

  - CVSS Score: 5

   – Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request
               Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server
               allows an attacker to smuggle requests to the AJP server it forwards
               requests to. This issue affects Apache HTTP Server Apache HTTP
               Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2014-0098

   – CVSS Score: 5

   – Description: The log_cookie function in mod_log_config.c in the mod_log_config
               module in the Apache HTTP Server before 2.4.8 allows remote attackers
               to cause a denial of service (segmentation fault and daemon crash)
               via a crafted cookie that is not properly handled during truncation.

- Vulnerability: CVE-2016-8743

   – CVSS Score: 5

   – Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was
               liberal in the whitespace accepted from requests and sent in response
               lines and headers. Accepting these different behaviors represented a
               security concern when httpd participates in any chain of proxies or
               interacts with back-end application servers, either through mod_proxy
               or using conventional CGI mechanisms, and may result in request
               smuggling, response splitting and cache pollution.

- Vulnerability: CVE-2024-40898

   – CVSS Score: N/A

   – Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in
               server/vhost context, allows to potentially leak NTML hashes to
               a malicious server via SSRF and malicious requests.Users are
               recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2024-38474

   – CVSS Score: N/A

   – Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server
               2.4.59 and earlier allows attacker to execute scripts indirectories
               permitted by the configuration but not directly reachable by anyURL
               or source disclosure of scripts meant to only to be executed as
               CGI.Users are recommended to upgrade to version 2.4.60, which fixes
               this issue.Some RewriteRules that capture and substitute unsafely
               will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2022-0778

   – CVSS Score: 5

- Description: The BN_mod_sqrt() function, which computes a modular square root,
  contains a bug that can cause it to loop forever for non-prime
  moduli. Internally this function is used when parsing certificates
  that contain elliptic curve public keys in compressed form or
  explicit elliptic curve parameters with a base point encoded in
  compressed form. It is possible to trigger the infinite loop by
  crafting a certificate that has invalid explicit curve parameters.
  Since certificate parsing happens prior to verification of the
  certificate signature, any process that parses an externally supplied
  certificate may thus be subject to a denial of service attack. The
  infinite loop can also be reached when parsing crafted private
  keys as they can contain explicit elliptic curve parameters. Thus
  vulnerable situations include: - TLS clients consuming server
  certificates - TLS servers consuming client certificates - Hosting
  providers taking certificates or private keys from customers
  - Certificate authorities parsing certification requests from
  subscribers - Anything else which parses ASN.1 elliptic curve
  parameters Also any other applications that use the BN_mod_sqrt()
  where the attacker can control the parameter values are vulnerable
  to this DoS issue. In the OpenSSL 1.0.2 version the public key is
  not parsed during initial parsing of the certificate which makes
  it slightly harder to trigger the infinite loop. However any
  operation which requires the public key from the certificate will
  trigger the infinite loop. In particular the attacker can use a
  self-signed certificate to trigger the loop during verification
  of the certificate signature. This issue affects OpenSSL versions
  1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n
  and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected
  3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m).
  Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

- Vulnerability: CVE-2020-1971

  - CVSS Score: 4.3

– Description: The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s_server, s_client and verify tools have support for the "-crl_download" option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue. Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w).

- **Vulnerability:** CVE-2009-1390

  – CVSS Score: 6.8
  – Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2) GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS certificate in the chain is accepted instead of verifying the entire chain, which allows remote attackers to spoof trusted servers via a man-in-the-middle attack.

- **Vulnerability:** CVE-2012-3526

  – CVSS Score: 5
  – Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- **Vulnerability:** CVE-2023-5678

  – CVSS Score: N/A

- Description: Issue summary: Generating excessively long X9.42 DH keys or checkingexcessively long X9.42 DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_generate_key() togenerate an X9.42 DH key may experience long delays. Likewise, applicationsthat use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check()to check an X9.42 DH key or X9.42 DH parameters may experience long delays.Where the key or parameters that are being checked have been obtained froman untrusted source this may lead to a Denial of Service.While DH_check() performs all the necessary checks (as of CVE-2023-3817),DH_check_pub_key() doesn't make any of these checks, and is thereforevulnerable for excessively large P and Q parameters.Likewise, while DH_generate_key() performs a check for an excessively largeP, it doesn't check for an excessively large Q.An application that calls DH_generate_key() or DH_check_pub_key() andsupplies a key or parameters obtained from an untrusted source could bevulnerable to a Denial of Service attack.DH_generate_key() and DH_check_pub_key() are also called by a number ofother OpenSSL functions. An application calling any of those otherfunctions may similarly be affected. The other functions affected by thisare DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate().Also vulnerable are the OpenSSL pkey command line application when using the"-pubcheck" option, as well as the OpenSSL genpkey command line application.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2017-3736

  - CVSS Score: 4

  - Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

- Vulnerability: CVE-2017-3737

  - CVSS Score: 4.3

– Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

- Vulnerability: CVE-2019-1547

  – CVSS Score: 1.9

  – Description: Normally in OpenSSL EC groups always have a co-factor present and this is used in side channel resistant code paths. However, in some cases, it is possible to construct a group using explicit parameters (instead of using a named curve). In those cases it is possible that such a group does not have the cofactor present. This can occur even where all the parameters match a known named curve. If such a curve is used then OpenSSL falls back to non-side channel resistant code paths which may result in full key recovery during an ECDSA signature operation. In order to be vulnerable an attacker would have to have the ability to time the creation of a large number of signatures where explicit parameters with no co-factor present are in use by an application using libcrypto. For the avoidance of doubt libssl is not vulnerable because explicit parameters are never used. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).

- Vulnerability: CVE-2017-3735

  – CVSS Score: 5

  – Description: While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL before 1.0.2m and 1.1.0g.

- Vulnerability: CVE-2009-2299

  – CVSS Score: 5

  – Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2022-1292

  – CVSS Score: 10

– Description: The c_rehash script does not properly sanitise shell metacharacters
                to prevent command injection. This script is distributed by
                some operating systems in a manner where it is automatically
                executed. On such operating systems, an attacker could execute
                arbitrary commands with the privileges of the script. Use of the
                c_rehash script is considered obsolete and should be replaced by the
                OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected
                3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n).
                Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).

• Vulnerability: CVE-2017-3738

   – CVSS Score: 4.3

   – Description: There is an overflow bug in the AVX2 Montgomery multiplication
                procedure used in exponentiation with 1024-bit moduli. No EC
                algorithms are affected. Analysis suggests that attacks against
                RSA and DSA as a result of this defect would be very difficult to
                perform and are not believed likely. Attacks against DH1024 are
                considered just feasible, because most of the work necessary to
                deduce information about a private key may be performed offline. The
                amount of resources required for such an attack would be significant.
                However, for an attack on TLS to be meaningful, the server would have
                to share the DH1024 private key among multiple clients, which is no
                longer an option since CVE-2016-0701. This only affects processors
                that support the AVX2 but not ADX extensions like Intel Haswell
                (4th generation). Note: The impact from this issue is similar to
                CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version
                1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n.
                Due to the low severity of this issue we are not issuing a new
                release of OpenSSL 1.1.0 at this time. The fix will be included in
                OpenSSL 1.1.0h when it becomes available. The fix is also available
                in commit e502cc86d in the OpenSSL git repository.

• Vulnerability: CVE-2012-4001

   – CVSS Score: 5

   – Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server
                does not properly verify its host name, which allows remote attackers
                to trigger HTTP requests to arbitrary hosts via unspecified vectors,
                as demonstrated by requests to intranet servers.

• Vulnerability: CVE-2022-37436

   – CVSS Score: N/A

   – Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause
                the response headers to be truncated early, resulting in some headers
                being incorporated into the response body. If the later headers have
                any security purpose, they will not be interpreted by the client.

• Vulnerability: CVE-2021-23840

   – CVSS Score: 5

- Description: Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissable length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2018-0737

  - CVSS Score: 4.3
  - Description: The OpenSSL RSA Key generation algorithm has been shown to be vulnerable to a cache timing side channel attack. An attacker with sufficient access to mount cache timing attacks during the RSA key generation process could recover the private key. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2b-1.0.2o).

- Vulnerability: CVE-2018-0734

  - CVSS Score: 4.3
  - Description: The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.1a (Affected 1.1.1). Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.0.2q (Affected 1.0.2-1.0.2p).

- Vulnerability: CVE-2018-0732

  - CVSS Score: 5
  - Description: During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime value to the client. This will cause the client to spend an unreasonably long period of time generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2-1.0.2o).

- Vulnerability: CVE-2017-9788

  - CVSS Score: 6.4
  - Description: In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.

- Vulnerability: CVE-2018-0739

  - CVSS Score: 4.3

- Description: Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o (Affected 1.0.2b-1.0.2n).

- Vulnerability: CVE-2014-8109

  - CVSS Score: 4.3
  - Description: mod_lua.c in the mod_lua module in the Apache HTTP Server 2.3.x and 2.4.x through 2.4.10 does not support an httpd configuration in which the same Lua authorization provider is used with different arguments within different contexts, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives, as demonstrated by a configuration that specifies authorization for one group to access a certain directory, and authorization for a second group to access a second directory.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2016-2161

  - CVSS Score: 5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.23, malicious input to mod_auth_digest can cause the server to crash, and each instance continues to crash even for subsequently valid requests.

- Vulnerability: CVE-2016-8612

  - CVSS Score: 3.3
  - Description: Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.

- Vulnerability: CVE-2019-1552

  - CVSS Score: 1.9

- Description: OpenSSL has internal defaults for a directory tree where it
  can find a configuration file as well as certificates used for
  verification in TLS. This directory is most commonly referred to
  as OPENSSLDIR, and is configurable with the --prefix / --openssldir
  configuration options. For OpenSSL versions 1.1.0 and 1.1.1, the
  mingw configuration targets assume that resulting programs and
  libraries are installed in a Unix-like environment and the default
  prefix for program installation as well as for OPENSSLDIR should be
  '/usr/local'. However, mingw programs are Windows programs, and as
  such, find themselves looking at sub-directories of 'C:/usr/local',
  which may be world writable, which enables untrusted users to modify
  OpenSSL's default configuration, insert CA certificates, modify (or
  even replace) existing engine modules, etc. For OpenSSL 1.0.2,
  '/usr/local/ssl' is used as default for OPENSSLDIR on all Unix and
  Windows targets, including Visual C builds. However, some build
  instructions for the diverse Windows targets on 1.0.2 encourage
  you to specify your own --prefix. OpenSSL versions 1.1.1, 1.1.0
  and 1.0.2 are affected by this issue. Due to the limited scope
  of affected deployments this has been assessed as low severity and
  therefore we are not creating new releases at this time. Fixed
  in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL
  1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected
  1.0.2-1.0.2s).

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5
    for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM
    Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows
    use an improper encryption algorithm and a weak key for maintaining
    the stored data of the node secret for the SecurID Authentication
    API, which allows local users to obtain sensitive information via
    cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication
    Agent 7.1 before 7.1.1 for Web for Internet Information Services,
    and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to
    inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2019-1551

  - CVSS Score: 5
  - Description: There is an overflow bug in the x64_64 Montgomery squaring procedure
    used in exponentiation with 512-bit moduli. No EC algorithms are
    affected. Analysis suggests that attacks against 2-prime RSA1024,
    3-prime RSA1536, and DSA1024 as a result of this defect would be
    very difficult to perform and are not believed likely. Attacks
    against DH512 are considered just feasible. However, for an attack
    the target would have to re-use the DH512 private key, which is not
    recommended anyway. Also applications directly using the low level
    API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME. Fixed
    in OpenSSL 1.1.1e (Affected 1.1.1-1.1.1d). Fixed in OpenSSL 1.0.2u
    (Affected 1.0.2-1.0.2t).

- Vulnerability: CVE-2019-1559

  - CVSS Score: 4.3

- Description: If an application encounters a fatal protocol error and then calls
  SSL_shutdown() twice (once to send a close_notify, and once to
  receive one) then OpenSSL can respond differently to the calling
  application if a 0 byte record is received with invalid padding
  compared to if a 0 byte record is received with an invalid MAC. If
  the application then behaves differently based on that in a way that
  is detectable to the remote peer, then this amounts to a padding
  oracle that could be used to decrypt data. In order for this to be
  exploitable "non-stitched" ciphersuites must be in use. Stitched
  ciphersuites are optimised implementations of certain commonly
  used ciphersuites. Also the application must call SSL_shutdown()
  twice even if a protocol error has occurred (applications should
  not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected
  1.0.2-1.0.2q).

- Vulnerability: CVE-2023-45802

  - CVSS Score: N/A

  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a
    time window were the request's memory resources were not reclaimed
    immediately. Instead, de-allocation was deferred to connection
    close. A client could send new requests and resets, keeping the
    connection busy and open and causing the memory footprint to keep
    on growing. On connection close, all resources were reclaimed, but
    the process might run out of memory before that.This was found by
    the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset
    Exploit) with their own test client. During "normal" HTTP/2 use, the
    probability to hit this bug is very low. The kept memory would not
    become noticeable before the connection closes or times out.Users are
    recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2018-1283

  - CVSS Score: 3.5

  - Description: In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to
    forward its session data to CGI applications (SessionEnv on, not
    the default), a remote user may influence their content by using a
    "Session" header. This comes from the "HTTP_SESSION" variable name
    used by mod_session to forward its data to CGIs, since the prefix
    "HTTP_" is also used by the Apache HTTP Server to pass HTTP header
    fields, per CGI specifications.

- Vulnerability: CVE-2020-1968

  - CVSS Score: 4.3

  - Description: The Raccoon attack exploits a flaw in the TLS specification which
    can lead to an attacker being able to compute the pre-master
    secret in connections which have used a Diffie-Hellman (DH) based
    ciphersuite. In such a case this would result in the attacker being
    able to eavesdrop on all encrypted communications sent over that TLS
    connection. The attack can only be exploited if an implementation
    re-uses a DH secret across multiple TLS connections. Note that this
    issue only impacts DH ciphersuites and not ECDH ciphersuites. This
    issue affects OpenSSL 1.0.2 which is out of support and no longer
    receiving public updates. OpenSSL 1.1.1 is not vulnerable to this
    issue. Fixed in OpenSSL 1.0.2w (Affected 1.0.2-1.0.2v).

- Vulnerability: CVE-2019-0217

  - CVSS Score: 6

- Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.

- **Vulnerability:** CVE-2022-28615

  - CVSS Score: 6.4
  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- **Vulnerability:** CVE-2022-28614

  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

11.12   IP Address: 159.149.53.27

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 4

- High Vulnerabilities: 14

- Medium Vulnerabilities: 94

- Low Vulnerabilities: 12

- Total Vulnerabilities: 124

Services Running on IP Address

- Service: Apache httpd

  – Port: 80
  – Version: 2.2.34
  – Location: /

- Service: Apache httpd

  – Port: 443
  – Version: 2.2.34
  – Location: /

Vulnerabilities Found

- Vulnerability: CVE-2009-2299

  – CVSS Score: 5
  – Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module
                  before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before
                  3.1.1-11637, a module for the Apache HTTP Server, allows remote
                  attackers to cause a denial of service (memory consumption) via an
                  HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2011-2688

  – CVSS Score: 7.5
  – Description: SQL injection vulnerability in mysql/mysql-auth.pl in the
                  mod_authnz_external module 3.2.5 and earlier for the Apache HTTP
                  Server allows remote attackers to execute arbitrary SQL commands
                  via the user field.

- Vulnerability: CVE-2022-0778

  – CVSS Score: 5

- Description: The BN_mod_sqrt() function, which computes a modular square root,
  contains a bug that can cause it to loop forever for non-prime
  moduli. Internally this function is used when parsing certificates
  that contain elliptic curve public keys in compressed form or
  explicit elliptic curve parameters with a base point encoded in
  compressed form. It is possible to trigger the infinite loop by
  crafting a certificate that has invalid explicit curve parameters.
  Since certificate parsing happens prior to verification of the
  certificate signature, any process that parses an externally supplied
  certificate may thus be subject to a denial of service attack. The
  infinite loop can also be reached when parsing crafted private
  keys as they can contain explicit elliptic curve parameters. Thus
  vulnerable situations include: - TLS clients consuming server
  certificates - TLS servers consuming client certificates - Hosting
  providers taking certificates or private keys from customers
  - Certificate authorities parsing certification requests from
  subscribers - Anything else which parses ASN.1 elliptic curve
  parameters Also any other applications that use the BN_mod_sqrt()
  where the attacker can control the parameter values are vulnerable
  to this DoS issue. In the OpenSSL 1.0.2 version the public key is
  not parsed during initial parsing of the certificate which makes
  it slightly harder to trigger the infinite loop. However any
  operation which requires the public key from the certificate will
  trigger the infinite loop. In particular the attacker can use a
  self-signed certificate to trigger the loop during verification
  of the certificate signature. This issue affects OpenSSL versions
  1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n
  and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected
  3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m).
  Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

- Vulnerability: CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk
    Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP
    Server does not properly handle certain configuration sections that
    specify NiceValue but not AssignUserID, which might allow remote
    attackers to gain privileges by leveraging the root uid and root gid
    of an mpm-itk process.

- Vulnerability: CVE-2018-5407

  - CVSS Score: 1.9
  - Description: Simultaneous Multi-threading (SMT) in processors can enable local
    users to exploit software vulnerable to timing attacks via a
    side-channel timing attack on 'port contention'.

- Vulnerability: CVE-2022-31813

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-*
    headers to the origin server based on client side Connection
    header hop-by-hop mechanism. This may be used to bypass IP based
    authentication on the origin server/application.

- Vulnerability: CVE-2022-29404

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a
    lua script that calls r:parsebody(0) may cause a denial of service
    due to no default limit on possible input size.

- Vulnerability: CVE-2020-1971

  – CVSS Score: 4.3
  – Description: The X.509 GeneralName type is a generic type for representing
    different types of names. One of those name types is known as
    EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which
    compares different instances of a GENERAL_NAME to see if they
    are equal or not. This function behaves incorrectly when both
    GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference
    and a crash may occur leading to a possible denial of service
    attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two
    purposes: 1) Comparing CRL distribution point names between an
    available CRL and a CRL distribution point embedded in an X509
    certificate 2) When verifying that a timestamp response token signer
    matches the timestamp authority name (exposed via the API functions
    TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can
    control both items being compared then that attacker could trigger
    a crash. For example if the attacker can trick a client or server
    into checking a malicious certificate against a malicious CRL then
    this may occur. Note that some applications automatically download
    CRLs based on a URL embedded in a certificate. This checking happens
    prior to the signatures on the certificate and CRL being verified.
    OpenSSL's s_server, s_client and verify tools have support for the
    "-crl_download" option which implements automatic CRL downloading and
    this attack has been demonstrated to work against those tools. Note
    that an unrelated bug means that affected versions of OpenSSL cannot
    parse or construct correct encodings of EDIPARTYNAME. However it is
    possible to construct a malformed EDIPARTYNAME that OpenSSL's parser
    will accept and hence trigger this attack. All OpenSSL 1.1.1 and
    1.0.2 versions are affected by this issue. Other OpenSSL releases
    are out of support and have not been checked. Fixed in OpenSSL
    1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected
    1.0.2-1.0.2w).

- Vulnerability: CVE-2022-4304

  – CVSS Score: N/A
  – Description: A timing based side channel exists in the OpenSSL RSA Decryption
    implementationwhich could be sufficient to recover a plaintext
    across a network in aBleichenbacher style attack. To achieve a
    successful decryption an attackerwould have to be able to send a
    very large number of trial messages fordecryption. The vulnerability
    affects all RSA padding modes: PKCS#1 v1.5,RSA-OEAP and RSASVE.For
    example, in a TLS connection, RSA is commonly used by a client to
    send anencrypted pre-master secret to the server. An attacker that
    had observed agenuine connection between a client and a server could
    use this flaw to sendtrial messages to the server and record the time
    taken to process them. After asufficiently large number of messages
    the attacker could recover the pre-mastersecret used for the original
    connection and thus be able to decrypt theapplication data sent over
    that connection.

- Vulnerability: CVE-2013-4365

  – CVSS Score: 7.5
  – Description: Heap-based buffer overflow in the fcgid_header_bucket_read function
    in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache
    HTTP Server allows remote attackers to have an unspecified impact via
    unknown vectors.

- Vulnerability: CVE-2009-1390

- CVSS Score: 6.8
- Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2) GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS certificate in the chain is accepted instead of verifying the entire chain, which allows remote attackers to spoof trusted servers via a man-in-the-middle attack.

- Vulnerability: CVE-2017-9798

  - CVSS Score: 5
  - Description: Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.

- Vulnerability: CVE-2022-22720

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2019-1563

  - CVSS Score: 4.3
  - Description: In situations where an attacker receives automated notification of the success or failure of a decryption attempt an attacker, after sending a very large number of messages to be decrypted, can recover a CMS/PKCS7 transported encryption key or decrypt any RSA encrypted message that was encrypted with the public RSA key, using a Bleichenbacher padding oracle attack. Applications are not affected if they use a certificate together with the private RSA key to the CMS_decrypt or PKCS7_decrypt functions to select the correct recipient info to decrypt. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).

- Vulnerability: CVE-2022-28330

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2021-32791

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2023-5678

  - CVSS Score: N/A

  - Description: Issue summary: Generating excessively long X9.42 DH keys or checkingexcessively long X9.42 DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_generate_key() togenerate an X9.42 DH key may experience long delays. Likewise, applicationsthat use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check()to check an X9.42 DH key or X9.42 DH parameters may experience long delays.Where the key or parameters that are being checked have been obtained froman untrusted source this may lead to a Denial of Service.While DH_check() performs all the necessary checks (as of CVE-2023-3817),DH_check_pub_key() doesn't make any of these checks, and is thereforevulnerable for excessively large P and Q parameters.Likewise, while DH_generate_key() performs a check for an excessively largeP, it doesn't check for an excessively large Q.An application that calls DH_generate_key() or DH_check_pub_key() andsupplies a key or parameters obtained from an untrusted source could bevulnerable to a Denial of Service attack.DH_generate_key() and DH_check_pub_key() are also called by a number ofother OpenSSL functions. An application calling any of those otherfunctions may similarly be affected. The other functions affected by thisare DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate().Also vulnerable are the OpenSSL pkey command line application when using the"-pubcheck" option, as well as the OpenSSL genpkey command line application.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2024-40898

  - CVSS Score: N/A

  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2017-3736

  - CVSS Score: 4

  - Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

- Vulnerability: CVE-2017-3737

  - CVSS Score: 4.3

- Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error
  state" mechanism. The intent was that if a fatal error occurred
  during a handshake then OpenSSL would move into the error state and
  would immediately fail if you attempted to continue the handshake.
  This works as designed for the explicit handshake functions
  (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due
  to a bug it does not work correctly if SSL_read() or SSL_write()
  is called directly. In that scenario, if the handshake fails then
  a fatal error will be returned in the initial function call. If
  SSL_read()/SSL_write() is subsequently called by the application
  for the same SSL object then it will succeed and the data is passed
  without being decrypted/encrypted directly from the SSL/TLS record
  layer. In order to exploit this issue an application bug would have
  to be present that resulted in a call to SSL_read()/SSL_write() being
  issued after having already received a fatal error. OpenSSL version
  1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0
  is not affected.

- Vulnerability: CVE-2019-1547

  - CVSS Score: 1.9

  - Description: Normally in OpenSSL EC groups always have a co-factor present and
    this is used in side channel resistant code paths. However, in some
    cases, it is possible to construct a group using explicit parameters
    (instead of using a named curve). In those cases it is possible
    that such a group does not have the cofactor present. This can occur
    even where all the parameters match a known named curve. If such a
    curve is used then OpenSSL falls back to non-side channel resistant
    code paths which may result in full key recovery during an ECDSA
    signature operation. In order to be vulnerable an attacker would
    have to have the ability to time the creation of a large number of
    signatures where explicit parameters with no co-factor present are
    in use by an application using libcrypto. For the avoidance of doubt
    libssl is not vulnerable because explicit parameters are never used.
    Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL
    1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected
    1.0.2-1.0.2s).

- Vulnerability: CVE-2022-2068

  - CVSS Score: 10

  - Description: In addition to the c_rehash shell command injection identified in
    CVE-2022-1292, further circumstances where the c_rehash script
    does not properly sanitise shell metacharacters to prevent command
    injection were found by code review. When the CVE-2022-1292 was
    fixed it was not discovered that there are other places in the
    script where the file names of certificates being hashed were
    possibly passed to a command executed through the shell. This
    script is distributed by some operating systems in a manner where
    it is automatically executed. On such operating systems, an
    attacker could execute arbitrary commands with the privileges of
    the script. Use of the c_rehash script is considered obsolete and
    should be replaced by the OpenSSL rehash command line tool. Fixed in
    OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL
    1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected
    1.0.2-1.0.2ze).

- Vulnerability: CVE-2009-3766

  - CVSS Score: 6.8

- Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when OpenSSL is used, does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

- Vulnerability: CVE-2022-1292

  - CVSS Score: 10
  - Description: The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n). Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).

- Vulnerability: CVE-2017-3738

  - CVSS Score: 4.3
  - Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

- Vulnerability: CVE-2009-3765

  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- Vulnerability: CVE-2006-20001

  - CVSS Score: N/A

- Description: A carefully crafted If: request header can cause a memory read, or
  write of a single zero byte, in a pool (heap) memory location beyond
  the header value sent. This could cause the process to crash.This
  issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2009-0796

  – CVSS Score: 2.6
  – Description: Cross-site scripting (XSS) vulnerability in Status.pm in
    Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the
    Apache HTTP Server, when /perl-status is accessible, allows remote
    attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2024-0727

  – CVSS Score: N/A
  – Description: Issue summary: Processing a maliciously formatted PKCS12 file
    may lead OpenSSLto crash leading to a potential Denial of Service
    attackImpact summary: Applications loading files in the PKCS12
    format from untrustedsources might terminate abruptly.A file in
    PKCS12 format can contain certificates and keys and may come from
    anuntrusted source. The PKCS12 specification allows certain fields
    to be NULL, butOpenSSL does not correctly check for this case.
    This can lead to a NULL pointerdereference that results in OpenSSL
    crashing. If an application processes PKCS12files from an untrusted
    source using the OpenSSL APIs then that application willbe vulnerable
    to this issue.OpenSSL APIs that are vulnerable to this are:
    PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(),
    PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a
    similar issue in SMIME_write_PKCS7(). However since thisfunction
    is related to writing data we do not consider it security
    significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected
    by this issue.

- Vulnerability: CVE-2021-3712

  – CVSS Score: 5.8

- Description: ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own "d2i" functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the "data" and "length" fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the "data" field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). It can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y).

- Vulnerability: CVE-2023-0464

  - CVSS Score: N/A

  - Description: A security vulnerability has been identified in all supported versionsof OpenSSL related to the verification of X.509 certificate chainsthat include policy constraints. Attackers may be able to exploit thisvulnerability by creating a malicious certificate chain that triggersexponential use of computational resources, leading to a denial-of-service(DoS) attack on affected systems.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0465

  - CVSS Score: N/A

– Description: Applications that use a non-default option when verifying
certificates may bevulnerable to an attack from a malicious CA
to circumvent certain checks.Invalid certificate policies in leaf
certificates are silently ignored byOpenSSL and other certificate
policy checks are skipped for that certificate.A malicious CA could
use this to deliberately assert invalid certificate policiesin order
to circumvent policy checking on the certificate altogether.Policy
processing is disabled by default but can be enabled by passingthe
'-policy' argument to the command line utilities or by calling
the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0466

  – CVSS Score: N/A

  – Description: The function X509_VERIFY_PARAM_add0_policy() is documented
toimplicitly enable the certificate policy check when doing
certificateverification. However the implementation of the
function does notenable the check which allows certificates
with invalid or incorrectpolicies to pass the certificate
verification.As suddenly enabling the policy check could break
existing deployments it wasdecided to keep the existing behavior of
the X509_VERIFY_PARAM_add0_policy()function.Instead the applications
that require OpenSSL to perform certificatepolicy check need
to use X509_VERIFY_PARAM_set1_policies() or explicitlyenable the
policy check by calling X509_VERIFY_PARAM_set_flags() withthe
X509_V_FLAG_POLICY_CHECK flag argument.Certificate policy checks
are disabled by default in OpenSSL and are notcommonly used by
applications.

- Vulnerability: CVE-2012-4001

  – CVSS Score: 5

  – Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server
does not properly verify its host name, which allows remote attackers
to trigger HTTP requests to arbitrary hosts via unspecified vectors,
as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2022-37436

  – CVSS Score: N/A

  – Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause
the response headers to be truncated early, resulting in some headers
being incorporated into the response body. If the later headers have
any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2022-22721

  – CVSS Score: 5.8

  – Description: If LimitXMLRequestBody is set to allow request bodies larger than
350MB (defaults to 1M) on 32 bit systems an integer overflow happens
which later causes out of bounds writes. This issue affects Apache
HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2012-4360

  – CVSS Score: 4.3

  – Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module
0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote
attackers to inject arbitrary web script or HTML via unspecified
vectors.

- Vulnerability: CVE-2021-40438

- CVSS Score: 6.8
- Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2018-0737

  - CVSS Score: 4.3
  - Description: The OpenSSL RSA Key generation algorithm has been shown to be vulnerable to a cache timing side channel attack. An attacker with sufficient access to mount cache timing attacks during the RSA key generation process could recover the private key. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2b-1.0.2o).

- Vulnerability: CVE-2018-0734

  - CVSS Score: 4.3
  - Description: The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.1a (Affected 1.1.1). Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.0.2q (Affected 1.0.2-1.0.2p).

- Vulnerability: CVE-2018-0732

  - CVSS Score: 5
  - Description: During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime value to the client. This will cause the client to spend an unreasonably long period of time generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2-1.0.2o).

- Vulnerability: CVE-2017-3735

  - CVSS Score: 5
  - Description: While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL before 1.0.2m and 1.1.0g.

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2021-23840

  - CVSS Score: 5

- Description: Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissable length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2021-23841

  - CVSS Score: 4.3

  - Description: The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack. The function X509_issuer_and_serial_hash() is never directly called by OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on certificates that may have been obtained from untrusted sources. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2021-32792

  - CVSS Score: 4.3

  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.

- Vulnerability: CVE-2023-0286

  - CVSS Score: N/A

- Description: There is a type confusion vulnerability relating to X.400 address processinginside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING butthe public structure definition for GENERAL_NAME incorrectly specified the typeof the x400Address field as ASN1_TYPE. This field is subsequently interpreted bythe OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than anASN1_STRING.When CRL checking is enabled (i.e. the application sets theX509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to passarbitrary pointers to a memcmp call, enabling them to read memory contents orenact a denial of service. In most cases, the attack requires the attacker toprovide both the certificate chain and CRL, neither of which need to have avalid signature. If the attacker only controls one of these inputs, the otherinput must already contain an X.400 address as a CRL distribution point, whichis uncommon. As such, this vulnerability is most likely to only affectapplications which have implemented their own functionality for retrieving CRLsover a network.

- Vulnerability: CVE-2023-3817

  - CVSS Score: N/A

  - Description: Issue summary: Checking excessively long DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH key or DH parameters may experience longdelays. Where the key or parameters that are being checked have been obtainedfrom an untrusted source this may lead to a Denial of Service.The function DH_check() performs various checks on DH parameters. After fixingCVE-2023-3446 it was discovered that a large q parameter value can also triggeran overly long computation during some of these checks. A correct q value,if present, cannot be larger than the modulus p parameter, thus it isunnecessary to perform these checks if q is larger than p.An application that calls DH_check() and supplies a key or parameters obtainedfrom an untrusted source could be vulnerable to a Denial of Service attack.The function DH_check() is itself called by a number of other OpenSSL functions.An application calling any of those other functions may similarly be affected.The other functions affected by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable are the OpenSSL dhparam and pkeyparam command line applicationswhen using the "-check" option.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2018-1301

  - CVSS Score: 4.3

  - Description: A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.

- Vulnerability: CVE-2018-1302

  - CVSS Score: 4.3

- Description: When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.

- Vulnerability: CVE-2019-1551

  - CVSS Score: 5
  - Description: There is an overflow bug in the x64_64 Montgomery squaring procedure used in exponentiation with 512-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against 2-prime RSA1024, 3-prime RSA1536, and DSA1024 as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH512 are considered just feasible. However, for an attack the target would have to re-use the DH512 private key, which is not recommended anyway. Also applications directly using the low level API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME. Fixed in OpenSSL 1.1.1e (Affected 1.1.1-1.1.1d). Fixed in OpenSSL 1.0.2u (Affected 1.0.2-1.0.2t).

- Vulnerability: CVE-2021-34798

  - CVSS Score: 5
  - Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2015-0228

  - CVSS Score: 5
  - Description: The lua_websocket_read function in lua_request.c in the mod_lua module in the Apache HTTP Server through 2.4.12 allows remote attackers to cause a denial of service (child-process crash) by sending a crafted WebSocket Ping frame after a Lua script has called the wsupgrade function.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2018-1303

  - CVSS Score: 5
  - Description: A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache. The vulnerability is considered as low risk since mod_cache_socache is not widely used, mod_cache_disk is not concerned by this vulnerability.

- Vulnerability: CVE-2021-32786

  - CVSS Score: 5.8

- Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, `oidc_validate_redirect_url()` does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring `mod_auth_openidc` to only allow redirection whose destination matches a given regular expression.

- Vulnerability: CVE-2021-32785

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache (`OIDCCacheEncrypt off`, `OIDCSessionType server-cache`, `OIDCCacheType redis`), `mod_auth_openidc` wrongly performed argument interpolation before passing Redis requests to `hiredis`, which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the `hiredis` API. As a workaround, this vulnerability can be mitigated by setting `OIDCCacheEncrypt` to `on`, as cache keys are cryptographically hashed before use when this option is enabled.

- Vulnerability: CVE-2018-0739

  - CVSS Score: 4.3
  - Description: Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o (Affected 1.0.2b-1.0.2n).

- Vulnerability: CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2016-8612

  - CVSS Score: 3.3
  - Description: Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.

- Vulnerability: CVE-2019-1552

  – CVSS Score: 1.9
  – Description: OpenSSL has internal defaults for a directory tree where it can find a configuration file as well as certificates used for verification in TLS. This directory is most commonly referred to as OPENSSLDIR, and is configurable with the --prefix / --openssldir configuration options. For OpenSSL versions 1.1.0 and 1.1.1, the mingw configuration targets assume that resulting programs and libraries are installed in a Unix-like environment and the default prefix for program installation as well as for OPENSSLDIR should be '/usr/local'. However, mingw programs are Windows programs, and as such, find themselves looking at sub-directories of 'C:/usr/local', which may be world writable, which enables untrusted users to modify OpenSSL's default configuration, insert CA certificates, modify (or even replace) existing engine modules, etc. For OpenSSL 1.0.2, '/usr/local/ssl' is used as default for OPENSSLDIR on all Unix and Windows targets, including Visual C builds. However, some build instructions for the diverse Windows targets on 1.0.2 encourage you to specify your own --prefix. OpenSSL versions 1.1.1, 1.1.0 and 1.0.2 are affected by this issue. Due to the limited scope of affected deployments this has been assessed as low severity and therefore we are not creating new releases at this time. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).

- Vulnerability: CVE-2021-44790

  – CVSS Score: 7.5
  – Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

- Vulnerability: CVE-2013-0942

  – CVSS Score: 4.3
  – Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2021-4160

  – CVSS Score: 4.3

- Description: There is a carry propagation bug in the MIPS32 and MIPS64 squaring
procedure. Many EC algorithms are affected, including some of the
TLS 1.3 default curves. Impact was not analyzed in detail, because
the pre-requisites for attack are considered unlikely and include
reusing private keys. Analysis suggests that attacks against RSA and
DSA as a result of this defect would be very difficult to perform
and are not believed likely. Attacks against DH are considered
just feasible (although very difficult) because most of the work
necessary to deduce information about a private key may be performed
offline. The amount of resources required for such an attack would
be significant. However, for an attack on TLS to be meaningful, the
server would have to share the DH private key among multiple clients,
which is no longer an option since CVE-2016-0701. This issue affects
OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the
releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For
the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that
is available to premium support customers only. It will be made
available in 1.0.2zc when it is released. The issue only affects
OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0).
Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL
1.0.2zc-dev (Affected 1.0.2-1.0.2zb).

- Vulnerability: CVE-2019-1559

  - CVSS Score: 4.3

  - Description: If an application encounters a fatal protocol error and then calls
SSL_shutdown() twice (once to send a close_notify, and once to
receive one) then OpenSSL can respond differently to the calling
application if a 0 byte record is received with invalid padding
compared to if a 0 byte record is received with an invalid MAC. If
the application then behaves differently based on that in a way that
is detectable to the remote peer, then this amounts to a padding
oracle that could be used to decrypt data. In order for this to be
exploitable "non-stitched" ciphersuites must be in use. Stitched
ciphersuites are optimised implementations of certain commonly
used ciphersuites. Also the application must call SSL_shutdown()
twice even if a protocol error has occurred (applications should
not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected
1.0.2-1.0.2q).

- Vulnerability: CVE-2023-45802

  - CVSS Score: N/A

  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a
time window were the request's memory resources were not reclaimed
immediately. Instead, de-allocation was deferred to connection
close. A client could send new requests and resets, keeping the
connection busy and open and causing the memory footprint to keep
on growing. On connection close, all resources were reclaimed, but
the process might run out of memory before that.This was found by
the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset
Exploit) with their own test client. During "normal" HTTP/2 use, the
probability to hit this bug is very low. The kept memory would not
become noticeable before the connection closes or times out.Users are
recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-28614

  - CVSS Score: 5

– Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier
  may read unintended memory if an attacker can cause the server to
  reflect very large input using ap_rwrite() or ap_rputs(), such as
  with mod_luas r:puts() function. Modules compiled and distributed
  separately from Apache HTTP Server that use the 'ap_rputs' function
  and may pass it a very large (INT_MAX or larger) string must be
  compiled against current headers to resolve the issue.

- Vulnerability: CVE-2023-2650

  – CVSS Score: N/A

  – Description: Issue summary: Processing some specially crafted ASN.1 object
    identifiers ordata containing them may be very slow.Impact summary:
    Applications that use OBJ_obj2txt() directly, or use any ofthe
    OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with
    no messagesize limit may experience notable to very long delays
    when processing thosemessages, which may lead to a Denial of
    Service.An OBJECT IDENTIFIER is composed of a series of numbers –
    sub-identifiers –most of which have no size limit. OBJ_obj2txt() may
    be used to translatean ASN.1 OBJECT IDENTIFIER given in DER encoding
    form (using the OpenSSLtype ASN1_OBJECT) to its canonical numeric
    text form, which are thesub-identifiers of the OBJECT IDENTIFIER in
    decimal form, separated byperiods.When one of the sub-identifiers in
    the OBJECT IDENTIFIER is very large(these are sizes that are seen as
    absurdly large, taking up tens or hundredsof KiBs), the translation
    to a decimal number in text may take a very longtime. The time
    complexity is $O(n^2)$ with 'n' being the size of thesub-identifiers
    in bytes (*).With OpenSSL 3.0, support to fetch cryptographic
    algorithms using names /identifiers in string form was introduced.
    This includes using OBJECTIDENTIFIERs in canonical numeric text form
    as identifiers for fetchingalgorithms.Such OBJECT IDENTIFIERs may
    be received through the ASN.1 structureAlgorithmIdentifier, which
    is commonly used in multiple protocols to specifywhat cryptographic
    algorithm should be used to sign or verify, encrypt ordecrypt, or
    digest passed data.Applications that call OBJ_obj2txt() directly
    with untrusted data areaffected, with any version of OpenSSL. If the
    use is for the mere purposeof display, the severity is considered
    low.In OpenSSL 3.0 and newer, this affects the subsystems OCSP,
    PKCS7/SMIME,CMS, CMP/CRMF or TS. It also impacts anything that
    processes X.509certificates, including simple things like verifying
    its signature.The impact on TLS is relatively low, because all
    versions of OpenSSL have a100KiB limit on the peer's certificate
    chain. Additionally, this onlyimpacts clients, or servers that
    have explicitly enabled clientauthentication.In OpenSSL 1.1.1 and
    1.0.2, this only affects displaying diverse objects,such as X.509
    certificates. This is assumed to not happen in such a waythat it
    would cause a Denial of Service, so these versions are considerednot
    affected by this issue in such a way that it would be cause for
    concern,and the severity is therefore considered low.

- Vulnerability: CVE-2023-0215

  – CVSS Score: N/A

- Description: The public API function BIO_new_NDEF is a helper function used for streamingASN.1 data via a BIO. It is primarily used internally to OpenSSL to support theSMIME, CMS and PKCS7 streaming capabilities, but may also be called directly byend user applications.The function receives a BIO from the caller, prepends a new BIO_f_asn1 filterBIO onto the front of it to form a BIO chain, and then returns the new head ofthe BIO chain to the caller. Under certain conditions, for example if a CMSrecipient public key is invalid, the new filter BIO is freed and the functionreturns a NULL result indicating a failure. However, in this case, the BIO chainis not properly cleaned up and the BIO passed by the caller still retainsinternal pointers to the previously freed filter BIO. If the caller then goes onto call BIO_pop() on the BIO then a use-after-free will occur. This will mostlikely result in a crash.This scenario occurs directly in the internal function B64_write_ASN1() whichmay cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() onthe BIO. This internal function is in turn called by the public API functionsPEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream,SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7.Other public API functions that may be impacted by this includei2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream andi2d_PKCS7_bio_stream.The OpenSSL cms and smime command line applications are similarly affected.

- Vulnerability: CVE-2020-1968

  - CVSS Score: 4.3

  - Description: The Raccoon attack exploits a flaw in the TLS specification which can lead to an attacker being able to compute the pre-master secret in connections which have used a Diffie-Hellman (DH) based ciphersuite. In such a case this would result in the attacker being able to eavesdrop on all encrypted communications sent over that TLS connection. The attack can only be exploited if an implementation re-uses a DH secret across multiple TLS connections. Note that this issue only impacts DH ciphersuites and not ECDH ciphersuites. This issue affects OpenSSL 1.0.2 which is out of support and no longer receiving public updates. OpenSSL 1.1.1 is not vulnerable to this issue. Fixed in OpenSSL 1.0.2w (Affected 1.0.2-1.0.2v).

- Vulnerability: CVE-2012-3526

  - CVSS Score: 5

  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2009-3767

  - CVSS Score: 4.3

  - Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other versions, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2021-39275

  - CVSS Score: 7.5

- Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2022-28615

  - CVSS Score: 6.4
  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- Vulnerability: CVE-2023-31122

  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2022-0778

  - CVSS Score: 5

- Description: The BN_mod_sqrt() function, which computes a modular square root,
  contains a bug that can cause it to loop forever for non-prime
  moduli. Internally this function is used when parsing certificates
  that contain elliptic curve public keys in compressed form or
  explicit elliptic curve parameters with a base point encoded in
  compressed form. It is possible to trigger the infinite loop by
  crafting a certificate that has invalid explicit curve parameters.
  Since certificate parsing happens prior to verification of the
  certificate signature, any process that parses an externally supplied
  certificate may thus be subject to a denial of service attack. The
  infinite loop can also be reached when parsing crafted private
  keys as they can contain explicit elliptic curve parameters. Thus
  vulnerable situations include: - TLS clients consuming server
  certificates - TLS servers consuming client certificates - Hosting
  providers taking certificates or private keys from customers
  - Certificate authorities parsing certification requests from
  subscribers - Anything else which parses ASN.1 elliptic curve
  parameters Also any other applications that use the BN_mod_sqrt()
  where the attacker can control the parameter values are vulnerable
  to this DoS issue. In the OpenSSL 1.0.2 version the public key is
  not parsed during initial parsing of the certificate which makes
  it slightly harder to trigger the infinite loop. However any
  operation which requires the public key from the certificate will
  trigger the infinite loop. In particular the attacker can use a
  self-signed certificate to trigger the loop during verification
  of the certificate signature. This issue affects OpenSSL versions
  1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n
  and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected
  3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m).
  Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

- Vulnerability: CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk
    Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP
    Server does not properly handle certain configuration sections that
    specify NiceValue but not AssignUserID, which might allow remote
    attackers to gain privileges by leveraging the root uid and root gid
    of an mpm-itk process.

- Vulnerability: CVE-2018-5407

  - CVSS Score: 1.9
  - Description: Simultaneous Multi-threading (SMT) in processors can enable local
    users to exploit software vulnerable to timing attacks via a
    side-channel timing attack on 'port contention'.

- Vulnerability: CVE-2022-31813

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-*
    headers to the origin server based on client side Connection
    header hop-by-hop mechanism. This may be used to bypass IP based
    authentication on the origin server/application.

- Vulnerability: CVE-2022-29404

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a
    lua script that calls r:parsebody(0) may cause a denial of service
    due to no default limit on possible input size.

- Vulnerability: CVE-2020-1971

  – CVSS Score: 4.3
  – Description: The X.509 GeneralName type is a generic type for representing
    different types of names. One of those name types is known as
    EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which
    compares different instances of a GENERAL_NAME to see if they
    are equal or not. This function behaves incorrectly when both
    GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference
    and a crash may occur leading to a possible denial of service
    attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two
    purposes: 1) Comparing CRL distribution point names between an
    available CRL and a CRL distribution point embedded in an X509
    certificate 2) When verifying that a timestamp response token signer
    matches the timestamp authority name (exposed via the API functions
    TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can
    control both items being compared then that attacker could trigger
    a crash. For example if the attacker can trick a client or server
    into checking a malicious certificate against a malicious CRL then
    this may occur. Note that some applications automatically download
    CRLs based on a URL embedded in a certificate. This checking happens
    prior to the signatures on the certificate and CRL being verified.
    OpenSSL's s_server, s_client and verify tools have support for the
    "-crl_download" option which implements automatic CRL downloading and
    this attack has been demonstrated to work against those tools. Note
    that an unrelated bug means that affected versions of OpenSSL cannot
    parse or construct correct encodings of EDIPARTYNAME. However it is
    possible to construct a malformed EDIPARTYNAME that OpenSSL's parser
    will accept and hence trigger this attack. All OpenSSL 1.1.1 and
    1.0.2 versions are affected by this issue. Other OpenSSL releases
    are out of support and have not been checked. Fixed in OpenSSL
    1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected
    1.0.2-1.0.2w).

- Vulnerability: CVE-2022-4304

  – CVSS Score: N/A
  – Description: A timing based side channel exists in the OpenSSL RSA Decryption
    implementationwhich could be sufficient to recover a plaintext
    across a network in aBleichenbacher style attack. To achieve a
    successful decryption an attackerwould have to be able to send a
    very large number of trial messages fordecryption. The vulnerability
    affects all RSA padding modes: PKCS#1 v1.5,RSA-OEAP and RSASVE.For
    example, in a TLS connection, RSA is commonly used by a client to
    send anencrypted pre-master secret to the server. An attacker that
    had observed agenuine connection between a client and a server could
    use this flaw to sendtrial messages to the server and record the time
    taken to process them. After asufficiently large number of messages
    the attacker could recover the pre-mastersecret used for the original
    connection and thus be able to decrypt theapplication data sent over
    that connection.

- Vulnerability: CVE-2013-4365

  – CVSS Score: 7.5
  – Description: Heap-based buffer overflow in the fcgid_header_bucket_read function
    in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache
    HTTP Server allows remote attackers to have an unspecified impact via
    unknown vectors.

- Vulnerability: CVE-2009-1390

– CVSS Score: 6.8

– Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2) GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS certificate in the chain is accepted instead of verifying the entire chain, which allows remote attackers to spoof trusted servers via a man-in-the-middle attack.

- Vulnerability: CVE-2017-9798

– CVSS Score: 5

– Description: Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.

- Vulnerability: CVE-2022-22720

– CVSS Score: 7.5

– Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2019-1563

– CVSS Score: 4.3

– Description: In situations where an attacker receives automated notification of the success or failure of a decryption attempt an attacker, after sending a very large number of messages to be decrypted, can recover a CMS/PKCS7 transported encryption key or decrypt any RSA encrypted message that was encrypted with the public RSA key, using a Bleichenbacher padding oracle attack. Applications are not affected if they use a certificate together with the private RSA key to the CMS_decrypt or PKCS7_decrypt functions to select the correct recipient info to decrypt. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).

- Vulnerability: CVE-2022-28330

– CVSS Score: 5

– Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2021-32791

– CVSS Score: 4.3

– Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2023-5678
  - CVSS Score: N/A
  - Description: Issue summary: Generating excessively long X9.42 DH keys or checkingexcessively long X9.42 DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_generate_key() togenerate an X9.42 DH key may experience long delays. Likewise, applicationsthat use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check()to check an X9.42 DH key or X9.42 DH parameters may experience long delays.Where the key or parameters that are being checked have been obtained froman untrusted source this may lead to a Denial of Service.While DH_check() performs all the necessary checks (as of CVE-2023-3817),DH_check_pub_key() doesn't make any of these checks, and is thereforevulnerable for excessively large P and Q parameters.Likewise, while DH_generate_key() performs a check for an excessively largeP, it doesn't check for an excessively large Q.An application that calls DH_generate_key() or DH_check_pub_key() andsupplies a key or parameters obtained from an untrusted source could bevulnerable to a Denial of Service attack.DH_generate_key() and DH_check_pub_key() are also called by a number ofother OpenSSL functions. An application calling any of those otherfunctions may similarly be affected. The other functions affected by thisare DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate().Also vulnerable are the OpenSSL pkey command line application when using the"-pubcheck" option, as well as the OpenSSL genpkey command line application.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2024-40898
  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2017-3736
  - CVSS Score: 4
  - Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

- Vulnerability: CVE-2017-3737
  - CVSS Score: 4.3

- Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error
  state" mechanism. The intent was that if a fatal error occurred
  during a handshake then OpenSSL would move into the error state and
  would immediately fail if you attempted to continue the handshake.
  This works as designed for the explicit handshake functions
  (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due
  to a bug it does not work correctly if SSL_read() or SSL_write()
  is called directly. In that scenario, if the handshake fails then
  a fatal error will be returned in the initial function call. If
  SSL_read()/SSL_write() is subsequently called by the application
  for the same SSL object then it will succeed and the data is passed
  without being decrypted/encrypted directly from the SSL/TLS record
  layer. In order to exploit this issue an application bug would have
  to be present that resulted in a call to SSL_read()/SSL_write() being
  issued after having already received a fatal error. OpenSSL version
  1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0
  is not affected.

- Vulnerability: CVE-2019-1547

  - CVSS Score: 1.9

  - Description: Normally in OpenSSL EC groups always have a co-factor present and
    this is used in side channel resistant code paths. However, in some
    cases, it is possible to construct a group using explicit parameters
    (instead of using a named curve). In those cases it is possible
    that such a group does not have the cofactor present. This can occur
    even where all the parameters match a known named curve. If such a
    curve is used then OpenSSL falls back to non-side channel resistant
    code paths which may result in full key recovery during an ECDSA
    signature operation. In order to be vulnerable an attacker would
    have to have the ability to time the creation of a large number of
    signatures where explicit parameters with no co-factor present are
    in use by an application using libcrypto. For the avoidance of doubt
    libssl is not vulnerable because explicit parameters are never used.
    Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL
    1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected
    1.0.2-1.0.2s).

- Vulnerability: CVE-2022-2068

  - CVSS Score: 10

  - Description: In addition to the c_rehash shell command injection identified in
    CVE-2022-1292, further circumstances where the c_rehash script
    does not properly sanitise shell metacharacters to prevent command
    injection were found by code review. When the CVE-2022-1292 was
    fixed it was not discovered that there are other places in the
    script where the file names of certificates being hashed were
    possibly passed to a command executed through the shell. This
    script is distributed by some operating systems in a manner where
    it is automatically executed. On such operating systems, an
    attacker could execute arbitrary commands with the privileges of
    the script. Use of the c_rehash script is considered obsolete and
    should be replaced by the OpenSSL rehash command line tool. Fixed in
    OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL
    1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected
    1.0.2-1.0.2ze).

- Vulnerability: CVE-2009-3766

  - CVSS Score: 6.8

- Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when OpenSSL is used, does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

- Vulnerability: CVE-2022-1292

  - CVSS Score: 10
  - Description: The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n). Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).

- Vulnerability: CVE-2017-3738

  - CVSS Score: 4.3
  - Description: There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.

- Vulnerability: CVE-2009-3765

  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- Vulnerability: CVE-2006-20001

  - CVSS Score: N/A

– Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2009-0796

    – CVSS Score: 2.6
    – Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2024-0727

    – CVSS Score: N/A
    – Description: Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSLto crash leading to a potential Denial of Service attackImpact summary: Applications loading files in the PKCS12 format from untrustedsources might terminate abruptly.A file in PKCS12 format can contain certificates and keys and may come from anuntrusted source. The PKCS12 specification allows certain fields to be NULL, butOpenSSL does not correctly check for this case. This can lead to a NULL pointerdereference that results in OpenSSL crashing. If an application processes PKCS12files from an untrusted source using the OpenSSL APIs then that application willbe vulnerable to this issue.OpenSSL APIs that are vulnerable to this are: PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a similar issue in SMIME_write_PKCS7(). However since thisfunction is related to writing data we do not consider it security significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.

- Vulnerability: CVE-2021-3712

    – CVSS Score: 5.8

- Description: ASN.1 strings are represented internally within OpenSSL as an
                ASN1␣STRING structure which contains a buffer holding the string
                data and a field holding the buffer length. This contrasts with
                normal C strings which are repesented as a buffer for the string
                data which is terminated with a NUL (0) byte. Although not a
                strict requirement, ASN.1 strings that are parsed using OpenSSL's
                own "d2i" functions (and other similar parsing functions) as well
                as any string whose value has been set with the ASN1␣STRING␣set()
                function will additionally NUL terminate the byte array in the
                ASN1␣STRING structure. However, it is possible for applications
                to directly construct valid ASN1␣STRING structures which do not NUL
                terminate the byte array by directly setting the "data" and "length"
                fields in the ASN1␣STRING array. This can also happen by using
                the ASN1␣STRING␣set0() function. Numerous OpenSSL functions that
                print ASN.1 data have been found to assume that the ASN1␣STRING byte
                array will be NUL terminated, even though this is not guaranteed for
                strings that have been directly constructed. Where an application
                requests an ASN.1 structure to be printed, and where that ASN.1
                structure contains ASN1␣STRINGs that have been directly constructed
                by the application without NUL terminating the "data" field, then
                a read buffer overrun can occur. The same thing can also occur
                during name constraints processing of certificates (for example
                if a certificate has been directly constructed by the application
                instead of loading it via the OpenSSL parsing functions, and the
                certificate contains non NUL terminated ASN1␣STRING structures).
                It can also occur in the X509␣get1␣email(), X509␣REQ␣get1␣email()
                and X509␣get1␣ocsp() functions. If a malicious actor can cause an
                application to directly construct an ASN1␣STRING and then process it
                through one of the affected OpenSSL functions then this issue could
                be hit. This might result in a crash (causing a Denial of Service
                attack). It could also result in the disclosure of private memory
                contents (such as private keys, or sensitive plaintext). Fixed in
                OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za
                (Affected 1.0.2-1.0.2y).

- Vulnerability: CVE-2023-0464

  - CVSS Score: N/A

  - Description: A security vulnerability has been identified in all supported
                versionsof OpenSSL related to the verification of X.509 certificate
                chainsthat include policy constraints. Attackers may be able to
                exploit thisvulnerability by creating a malicious certificate chain
                that triggersexponential use of computational resources, leading
                to a denial-of-service(DoS) attack on affected systems.Policy
                processing is disabled by default but can be enabled by passingthe
                '-policy' argument to the command line utilities or by calling
                the'X509␣VERIFY␣PARAM␣set1␣policies()' function.

- Vulnerability: CVE-2023-0465

  - CVSS Score: N/A

- Description: Applications that use a non-default option when verifying certificates may bevulnerable to an attack from a malicious CA to circumvent certain checks.Invalid certificate policies in leaf certificates are silently ignored byOpenSSL and other certificate policy checks are skipped for that certificate.A malicious CA could use this to deliberately assert invalid certificate policiesin order to circumvent policy checking on the certificate altogether.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509 VERIFY PARAM set1 policies()' function.

- Vulnerability: CVE-2023-0466

  - CVSS Score: N/A
  - Description: The function X509 VERIFY PARAM add0 policy() is documented toimplicitly enable the certificate policy check when doing certificateverification. However the implementation of the function does notenable the check which allows certificates with invalid or incorrectpolicies to pass the certificate verification.As suddenly enabling the policy check could break existing deployments it wasdecided to keep the existing behavior of the X509 VERIFY PARAM add0 policy()function.Instead the applications that require OpenSSL to perform certificatepolicy check need to use X509 VERIFY PARAM set1 policies() or explicitlyenable the policy check by calling X509 VERIFY PARAM set flags() withthe X509 V FLAG POLICY CHECK flag argument.Certificate policy checks are disabled by default in OpenSSL and are notcommonly used by applications.

- Vulnerability: CVE-2012-4001

  - CVSS Score: 5
  - Description: The mod pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2022-37436

  - CVSS Score: N/A
  - Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2022-22721

  - CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2012-4360

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2021-40438

- CVSS Score: 6.8
- Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2018-0737

  - CVSS Score: 4.3
  - Description: The OpenSSL RSA Key generation algorithm has been shown to be vulnerable to a cache timing side channel attack. An attacker with sufficient access to mount cache timing attacks during the RSA key generation process could recover the private key. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2b-1.0.2o).

- Vulnerability: CVE-2018-0734

  - CVSS Score: 4.3
  - Description: The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.1a (Affected 1.1.1). Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.0.2q (Affected 1.0.2-1.0.2p).

- Vulnerability: CVE-2018-0732

  - CVSS Score: 5
  - Description: During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime value to the client. This will cause the client to spend an unreasonably long period of time generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2-1.0.2o).

- Vulnerability: CVE-2017-3735

  - CVSS Score: 5
  - Description: While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL before 1.0.2m and 1.1.0g.

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2021-23840

  - CVSS Score: 5

- Description: Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissable length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2021-23841

  - CVSS Score: 4.3
  - Description: The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack. The function X509_issuer_and_serial_hash() is never directly called by OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on certificates that may have been obtained from untrusted sources. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2021-32792

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.

- Vulnerability: CVE-2023-0286

  - CVSS Score: N/A

– Description: There is a type confusion vulnerability relating to X.400 address processinginside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING butthe public structure definition for GENERAL_NAME incorrectly specified the typeof the x400Address field as ASN1_TYPE. This field is subsequently interpreted bythe OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than anASN1_STRING.When CRL checking is enabled (i.e. the application sets theX509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to passarbitrary pointers to a memcmp call, enabling them to read memory contents orenact a denial of service. In most cases, the attack requires the attacker toprovide both the certificate chain and CRL, neither of which need to have avalid signature. If the attacker only controls one of these inputs, the otherinput must already contain an X.400 address as a CRL distribution point, whichis uncommon. As such, this vulnerability is most likely to only affectapplications which have implemented their own functionality for retrieving CRLsover a network.

- Vulnerability: CVE-2023-3817

  – CVSS Score: N/A

  – Description: Issue summary: Checking excessively long DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH key or DH parameters may experience longdelays. Where the key or parameters that are being checked have been obtainedfrom an untrusted source this may lead to a Denial of Service.The function DH_check() performs various checks on DH parameters. After fixingCVE-2023-3446 it was discovered that a large q parameter value can also triggeran overly long computation during some of these checks. A correct q value,if present, cannot be larger than the modulus p parameter, thus it isunnecessary to perform these checks if q is larger than p.An application that calls DH_check() and supplies a key or parameters obtainedfrom an untrusted source could be vulnerable to a Denial of Service attack.The function DH_check() is itself called by a number of other OpenSSL functions.An application calling any of those other functions may similarly be affected.The other functions affected by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable are the OpenSSL dhparam and pkeyparam command line applicationswhen using the "-check" option.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2018-1301

  – CVSS Score: 4.3

  – Description: A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.

- Vulnerability: CVE-2018-1302

  – CVSS Score: 4.3

- Description: When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.

- Vulnerability: CVE-2019-1551

  - CVSS Score: 5

  - Description: There is an overflow bug in the x64_64 Montgomery squaring procedure used in exponentiation with 512-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against 2-prime RSA1024, 3-prime RSA1536, and DSA1024 as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH512 are considered just feasible. However, for an attack the target would have to re-use the DH512 private key, which is not recommended anyway. Also applications directly using the low level API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME. Fixed in OpenSSL 1.1.1e (Affected 1.1.1-1.1.1d). Fixed in OpenSSL 1.0.2u (Affected 1.0.2-1.0.2t).

- Vulnerability: CVE-2021-34798

  - CVSS Score: 5

  - Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2015-0228

  - CVSS Score: 5

  - Description: The lua_websocket_read function in lua_request.c in the mod_lua module in the Apache HTTP Server through 2.4.12 allows remote attackers to cause a denial of service (child-process crash) by sending a crafted WebSocket Ping frame after a Lua script has called the wsupgrade function.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5

  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2018-1303

  - CVSS Score: 5

  - Description: A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache. The vulnerability is considered as low risk since mod_cache_socache is not widely used, mod_cache_disk is not concerned by this vulnerability.

- Vulnerability: CVE-2021-32786

  - CVSS Score: 5.8

- Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, `oidc_validate_redirect_url()` does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring `mod_auth_openidc` to only allow redirection whose destination matches a given regular expression.

- Vulnerability: CVE-2021-32785

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache (`OIDCCacheEncrypt off`, `OIDCSessionType server-cache`, `OIDCCacheType redis`), `mod_auth_openidc` wrongly performed argument interpolation before passing Redis requests to `hiredis`, which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the `hiredis` API. As a workaround, this vulnerability can be mitigated by setting `OIDCCacheEncrypt` to `on`, as cache keys are cryptographically hashed before use when this option is enabled.

- Vulnerability: CVE-2018-0739

  - CVSS Score: 4.3
  - Description: Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o (Affected 1.0.2b-1.0.2n).

- Vulnerability: CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2016-8612

  - CVSS Score: 3.3
  - Description: Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.

- **Vulnerability:** CVE-2019-1552

  - CVSS Score: 1.9
  - Description: OpenSSL has internal defaults for a directory tree where it
    can find a configuration file as well as certificates used for
    verification in TLS. This directory is most commonly referred to
    as OPENSSLDIR, and is configurable with the --prefix / --openssldir
    configuration options. For OpenSSL versions 1.1.0 and 1.1.1, the
    mingw configuration targets assume that resulting programs and
    libraries are installed in a Unix-like environment and the default
    prefix for program installation as well as for OPENSSLDIR should be
    '/usr/local'. However, mingw programs are Windows programs, and as
    such, find themselves looking at sub-directories of 'C:/usr/local',
    which may be world writable, which enables untrusted users to modify
    OpenSSL's default configuration, insert CA certificates, modify (or
    even replace) existing engine modules, etc. For OpenSSL 1.0.2,
    '/usr/local/ssl' is used as default for OPENSSLDIR on all Unix and
    Windows targets, including Visual C builds. However, some build
    instructions for the diverse Windows targets on 1.0.2 encourage
    you to specify your own --prefix. OpenSSL versions 1.1.1, 1.1.0
    and 1.0.2 are affected by this issue. Due to the limited scope
    of affected deployments this has been assessed as low severity and
    therefore we are not creating new releases at this time. Fixed
    in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL
    1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected
    1.0.2-1.0.2s).

- **Vulnerability:** CVE-2021-44790

  - CVSS Score: 7.5
  - Description: A carefully crafted request body can cause a buffer overflow in the
    mod_lua multipart parser (r:parsebody() called from Lua scripts).
    The Apache httpd team is not aware of an exploit for the vulnerabilty
    though it might be possible to craft one. This issue affects Apache
    HTTP Server 2.4.51 and earlier.

- **Vulnerability:** CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication
    Agent 7.1 before 7.1.1 for Web for Internet Information Services,
    and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to
    inject arbitrary web script or HTML via unspecified vectors.

- **Vulnerability:** CVE-2021-4160

  - CVSS Score: 4.3

- Description: There is a carry propagation bug in the MIPS32 and MIPS64 squaring
procedure. Many EC algorithms are affected, including some of the
TLS 1.3 default curves. Impact was not analyzed in detail, because
the pre-requisites for attack are considered unlikely and include
reusing private keys. Analysis suggests that attacks against RSA and
DSA as a result of this defect would be very difficult to perform
and are not believed likely. Attacks against DH are considered
just feasible (although very difficult) because most of the work
necessary to deduce information about a private key may be performed
offline. The amount of resources required for such an attack would
be significant. However, for an attack on TLS to be meaningful, the
server would have to share the DH private key among multiple clients,
which is no longer an option since CVE-2016-0701. This issue affects
OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the
releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For
the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that
is available to premium support customers only. It will be made
available in 1.0.2zc when it is released. The issue only affects
OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0).
Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL
1.0.2zc-dev (Affected 1.0.2-1.0.2zb).

- Vulnerability: CVE-2019-1559

  - CVSS Score: 4.3

  - Description: If an application encounters a fatal protocol error and then calls
SSL_shutdown() twice (once to send a close_notify, and once to
receive one) then OpenSSL can respond differently to the calling
application if a 0 byte record is received with invalid padding
compared to if a 0 byte record is received with an invalid MAC. If
the application then behaves differently based on that in a way that
is detectable to the remote peer, then this amounts to a padding
oracle that could be used to decrypt data. In order for this to be
exploitable "non-stitched" ciphersuites must be in use. Stitched
ciphersuites are optimised implementations of certain commonly
used ciphersuites. Also the application must call SSL_shutdown()
twice even if a protocol error has occurred (applications should
not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected
1.0.2-1.0.2q).

- Vulnerability: CVE-2023-45802

  - CVSS Score: N/A

  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a
time window were the request's memory resources were not reclaimed
immediately. Instead, de-allocation was deferred to connection
close. A client could send new requests and resets, keeping the
connection busy and open and causing the memory footprint to keep
on growing. On connection close, all resources were reclaimed, but
the process might run out of memory before that.This was found by
the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset
Exploit) with their own test client. During "normal" HTTP/2 use, the
probability to hit this bug is very low. The kept memory would not
become noticeable before the connection closes or times out.Users are
recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-28614

  - CVSS Score: 5

- Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier
  may read unintended memory if an attacker can cause the server to
  reflect very large input using ap_rwrite() or ap_rputs(), such as
  with mod_luas r:puts() function. Modules compiled and distributed
  separately from Apache HTTP Server that use the 'ap_rputs' function
  and may pass it a very large (INT_MAX or larger) string must be
  compiled against current headers to resolve the issue.

- Vulnerability: CVE-2023-2650

  - CVSS Score: N/A

  - Description: Issue summary: Processing some specially crafted ASN.1 object
    identifiers ordata containing them may be very slow.Impact summary:
    Applications that use OBJ_obj2txt() directly, or use any ofthe
    OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with
    no messagesize limit may experience notable to very long delays
    when processing thosemessages, which may lead to a Denial of
    Service.An OBJECT IDENTIFIER is composed of a series of numbers -
    sub-identifiers -most of which have no size limit. OBJ_obj2txt() may
    be used to translatean ASN.1 OBJECT IDENTIFIER given in DER encoding
    form (using the OpenSSLtype ASN1_OBJECT) to its canonical numeric
    text form, which are thesub-identifiers of the OBJECT IDENTIFIER in
    decimal form, separated byperiods.When one of the sub-identifiers in
    the OBJECT IDENTIFIER is very large(these are sizes that are seen as
    absurdly large, taking up tens or hundredsof KiBs), the translation
    to a decimal number in text may take a very longtime. The time
    complexity is $O(n^2)$ with 'n' being the size of thesub-identifiers
    in bytes (*).With OpenSSL 3.0, support to fetch cryptographic
    algorithms using names /identifiers in string form was introduced.
    This includes using OBJECTIDENTIFIERs in canonical numeric text form
    as identifiers for fetchingalgorithms.Such OBJECT IDENTIFIERs may
    be received through the ASN.1 structureAlgorithmIdentifier, which
    is commonly used in multiple protocols to specifywhat cryptographic
    algorithm should be used to sign or verify, encrypt ordecrypt, or
    digest passed data.Applications that call OBJ_obj2txt() directly
    with untrusted data areaffected, with any version of OpenSSL. If the
    use is for the mere purposeof display, the severity is considered
    low.In OpenSSL 3.0 and newer, this affects the subsystems OCSP,
    PKCS7/SMIME,CMS, CMP/CRMF or TS. It also impacts anything that
    processes X.509certificates, including simple things like verifying
    its signature.The impact on TLS is relatively low, because all
    versions of OpenSSL have a100KiB limit on the peer's certificate
    chain. Additionally, this onlyimpacts clients, or servers that
    have explicitly enabled clientauthentication.In OpenSSL 1.1.1 and
    1.0.2, this only affects displaying diverse objects,such as X.509
    certificates. This is assumed to not happen in such a waythat it
    would cause a Denial of Service, so these versions are considerednot
    affected by this issue in such a way that it would be cause for
    concern,and the severity is therefore considered low.

- Vulnerability: CVE-2023-0215

  - CVSS Score: N/A

- Description: The public API function BIO_new_NDEF is a helper function used for streamingASN.1 data via a BIO. It is primarily used internally to OpenSSL to support theSMIME, CMS and PKCS7 streaming capabilities, but may also be called directly byend user applications.The function receives a BIO from the caller, prepends a new BIO_f_asn1 filterBIO onto the front of it to form a BIO chain, and then returns the new head ofthe BIO chain to the caller. Under certain conditions, for example if a CMSrecipient public key is invalid, the new filter BIO is freed and the functionreturns a NULL result indicating a failure. However, in this case, the BIO chainis not properly cleaned up and the BIO passed by the caller still retainsinternal pointers to the previously freed filter BIO. If the caller then goes onto call BIO_pop() on the BIO then a use-after-free will occur. This will mostlikely result in a crash.This scenario occurs directly in the internal function B64_write_ASN1() whichmay cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() onthe BIO. This internal function is in turn called by the public API functionsPEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream,SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7.Other public API functions that may be impacted by this includei2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream andi2d_PKCS7_bio_stream.The OpenSSL cms and smime command line applications are similarly affected.

- Vulnerability: CVE-2020-1968

  - CVSS Score: 4.3
  - Description: The Raccoon attack exploits a flaw in the TLS specification which can lead to an attacker being able to compute the pre-master secret in connections which have used a Diffie-Hellman (DH) based ciphersuite. In such a case this would result in the attacker being able to eavesdrop on all encrypted communications sent over that TLS connection. The attack can only be exploited if an implementation re-uses a DH secret across multiple TLS connections. Note that this issue only impacts DH ciphersuites and not ECDH ciphersuites. This issue affects OpenSSL 1.0.2 which is out of support and no longer receiving public updates. OpenSSL 1.1.1 is not vulnerable to this issue. Fixed in OpenSSL 1.0.2w (Affected 1.0.2-1.0.2v).

- Vulnerability: CVE-2012-3526

  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2009-3767

  - CVSS Score: 4.3
  - Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other versions, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2021-39275

  - CVSS Score: 7.5

– Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2022-28615

  – CVSS Score: 6.4
  – Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- Vulnerability: CVE-2023-31122

  – CVSS Score: N/A
  – Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2022-22719

  – CVSS Score: 5
  – Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

11.13   IP Address: 159.149.130.178

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 3

- High Vulnerabilities: 8

- Medium Vulnerabilities: 35

- Low Vulnerabilities: 2

- Total Vulnerabilities: 48

Services Running on IP Address

- Service: OpenSSH

  - Port: 22
  - Version: 9.6
  - Location:

- Service: Apache httpd

  - Port: 443
  - Version: 2.4.52
  - Location: /

- Service: MariaDB

  - Port: 3306
  - Version: 10.5.10-MariaDB-1:10.5.10+maria~focal
  - Location:

Vulnerabilities Found

- Vulnerability: CVE-2007-2768

  - CVSS Score: 4.3
  - Description: OpenSSH, when using OPIE (One-Time Passwords in Everything) for PAM, allows remote attackers to determine the existence of certain user accounts, which displays a different response if the user account exists and is configured to use one-time passwords (OTP), a similar issue to CVE-2007-2243.

- Vulnerability: CVE-2008-3844

  - CVSS Score: 9.3
  - Description: Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, as signed in August 2008 using a legitimate Red Hat GPG key, contain an externally introduced modification (Trojan Horse) that allows the package authors to have an unknown impact. NOTE: since the malicious packages were not distributed from any official Red Hat sources, the scope of this issue is restricted to users who may have obtained these packages through unofficial distribution points. As of 20080827, no unofficial distributions of this software are known.

- Vulnerability: CVE-2024-6387

  - CVSS Score: N/A

- Description: A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period.

- Vulnerability: CVE-2023-51767

  - CVSS Score: N/A
  - Description: OpenSSH through 9.6, when common types of DRAM are used, might allow row hammer attacks (for authentication bypass) because the integer value of authenticated in mm_answer_authpassword does not resist flips of a single bit. NOTE: this is applicable to a certain threat model of attacker-victim co-location in which the attacker has user privileges.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2024-27316

  - CVSS Score: N/A
  - Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

- Vulnerability: CVE-2022-31628

  - CVSS Score: N/A
  - Description: In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the phar uncompressor code would recursively uncompress "quines" gzip files, resulting in an infinite loop.

- Vulnerability: CVE-2022-31629

  - CVSS Score: N/A
  - Description: In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the vulnerability enables network and same-site attackers to set a standard insecure cookie in the victim's browser which is treated as a '__Host-' or '__Secure-' cookie by PHP applications.

- Vulnerability: CVE-2022-31626

  - CVSS Score: 6
  - Description: In PHP versions 7.4.x below 7.4.30, 8.0.x below 8.0.20, and 8.1.x below 8.1.7, when pdo_mysql extension with mysqlnd driver, if the third party is allowed to supply host to connect to and the password for the connection, password of excessive length can trigger a buffer overflow in PHP, which can lead to a remote code execution vulnerability.

- Vulnerability: CVE-2022-31625

  - CVSS Score: 6.8

– Description: In PHP versions 7.4.x below 7.4.30, 8.0.x below 8.0.20, and 8.1.x below 8.1.7, when using Postgres database extension, supplying invalid parameters to the parametrized query may lead to PHP attempting to free memory using uninitialized data as pointers. This could lead to RCE vulnerability or denial of service.

- Vulnerability: CVE-2022-36760

    – CVSS Score: N/A
    – Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-4450

    – CVSS Score: N/A
    – Description: The function PEM_read_bio_ex() reads a PEM file from a BIO and parses anddecodes the "name" (e.g. "CERTIFICATE"), any header data and the payload data.If the function succeeds then the "name_out", "header" and "data" arguments arepopulated with pointers to buffers containing the relevant decoded data. Thecaller is responsible for freeing those buffers. It is possible to construct aPEM file that results in 0 bytes of payload data. In this case PEM_read_bio_ex()will return a failure code but will populate the header argument with a pointerto a buffer that has already been freed. If the caller also frees this bufferthen a double free will occur. This will most likely lead to a crash. Thiscould be exploited by an attacker who has the ability to supply malicious PEMfiles for parsing to achieve a denial of service attack.The functions PEM_read_bio() and PEM_read() are simple wrappers aroundPEM_read_bio_ex() and therefore these functions are also directly affected.These functions are also called indirectly by a number of other OpenSSLfunctions including PEM_X509_INFO_read_bio_ex() andSSL_CTX_use_serverinfo_file() which are also vulnerable. Some OpenSSL internaluses of these functions are not vulnerable because the caller does not free theheader argument if PEM_read_bio_ex() returns a failure code. These locationsinclude the PEM_read_bio_TYPE() functions as well as the decoders introduced inOpenSSL 3.0.The OpenSSL asn1parse command line application is also impacted by this issue.

- Vulnerability: CVE-2022-23943

    – CVSS Score: 7.5
    – Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

- Vulnerability: CVE-2022-2097

    – CVSS Score: 5
    – Description: AES OCB mode for 32-bit x86 platforms using the AES-NI assembly optimised implementation will not encrypt the entirety of the data under some circumstances. This could reveal sixteen bytes of data that was preexisting in the memory that wasn't written. In the special case of "in place" encryption, sixteen bytes of the plaintext would be revealed. Since OpenSSL does not support OCB based cipher suites for TLS and DTLS, they are both unaffected. Fixed in OpenSSL 3.0.5 (Affected 3.0.0-3.0.4). Fixed in OpenSSL 1.1.1q (Affected 1.1.1-1.1.1p).

- Vulnerability: CVE-2024-4577

  – CVSS Score: N/A

  – Description: In PHP versions8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in command line given toWin32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc.

- Vulnerability: CVE-2020-1971

  – CVSS Score: 4.3

  – Description: The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s_server, s_client and verify tools have support for the "-crl_download" option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue. Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w).

- Vulnerability: CVE-2022-4304

  – CVSS Score: N/A

- Description: A timing based side channel exists in the OpenSSL RSA Decryption implementationwhich could be sufficient to recover a plaintext across a network in aBleichenbacher style attack. To achieve a successful decryption an attackerwould have to be able to send a very large number of trial messages fordecryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5,RSA-OEAP and RSASVE.For example, in a TLS connection, RSA is commonly used by a client to send anencrypted pre-master secret to the server. An attacker that had observed agenuine connection between a client and a server could use this flaw to sendtrial messages to the server and record the time taken to process them. After asufficiently large number of messages the attacker could recover the pre-mastersecret used for the original connection and thus be able to decrypt theapplication data sent over that connection.

- Vulnerability: CVE-2013-4365

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2009-1390

  - CVSS Score: 6.8
  - Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2) GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS certificate in the chain is accepted instead of verifying the entire chain, which allows remote attackers to spoof trusted servers via a man-in-the-middle attack.

- Vulnerability: CVE-2006-20001

  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2007-3205

  - CVSS Score: 5
  - Description: The parse_str function in (1) PHP, (2) Hardened-PHP, and (3) Suhosin, when called without a second parameter, might allow remote attackers to overwrite arbitrary variables by specifying variable names and values in the string to be parsed. NOTE: it is not clear whether this is a design limitation of the function or a bug in PHP, although it is likely to be regarded as a bug in Hardened-PHP and Suhosin.

- Vulnerability: CVE-2024-5458

  - CVSS Score: N/A
  - Description: In PHP versions8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, due to a code logic error, filtering functions such as filter_var when validating URLs(FILTER_VALIDATE_URL) for certain types of URLs the function will result in invalid user information (username + password part of URLs) being treated as valid user information. This may lead to the downstream code accepting invalid URLs as valid and parsing them incorrectly.

- Vulnerability: CVE-2009-0796

- CVSS Score: 2.6
- Description: Cross-site scripting (XSS) vulnerability in Status.pm in
  Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the
  Apache HTTP Server, when /perl-status is accessible, allows remote
  attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2023-5678

  - CVSS Score: N/A
  - Description: Issue summary: Generating excessively long X9.42 DH keys or
    checkingexcessively long X9.42 DH keys or parameters may be
    very slow.Impact summary: Applications that use the functions
    DH_generate_key() togenerate an X9.42 DH key may experience
    long delays. Likewise, applicationsthat use DH_check_pub_key(),
    DH_check_pub_key_ex() or EVP_PKEY_public_check()to check an
    X9.42 DH key or X9.42 DH parameters may experience long
    delays.Where the key or parameters that are being checked have
    been obtained froman untrusted source this may lead to a Denial
    of Service.While DH_check() performs all the necessary checks
    (as of CVE-2023-3817),DH_check_pub_key() doesn't make any of
    these checks, and is thereforevulnerable for excessively large
    P and Q parameters.Likewise, while DH_generate_key() performs
    a check for an excessively largeP, it doesn't check for an
    excessively large Q.An application that calls DH_generate_key() or
    DH_check_pub_key() andsupplies a key or parameters obtained from
    an untrusted source could bevulnerable to a Denial of Service
    attack.DH_generate_key() and DH_check_pub_key() are also called by
    a number ofother OpenSSL functions. An application calling any of
    those otherfunctions may similarly be affected. The other functions
    affected by thisare DH_check_pub_key_ex(), EVP_PKEY_public_check(), and
    EVP_PKEY_generate().Also vulnerable are the OpenSSL pkey command line
    application when using the"-pubcheck" option, as well as the OpenSSL
    genpkey command line application.The OpenSSL SSL/TLS implementation
    is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers
    are not affected by this issue.

- Vulnerability: CVE-2024-40898

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in
    server/vhost context, allows to potentially leak NTML hashes to
    a malicious server via SSRF and malicious requests.Users are
    recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2012-4001

  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server
    does not properly verify its host name, which allows remote attackers
    to trigger HTTP requests to arbitrary hosts via unspecified vectors,
    as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2022-2068

  - CVSS Score: 10

- Description: In addition to the c_rehash shell command injection identified in
  CVE-2022-1292, further circumstances where the c_rehash script
  does not properly sanitise shell metacharacters to prevent command
  injection were found by code review. When the CVE-2022-1292 was
  fixed it was not discovered that there are other places in the
  script where the file names of certificates being hashed were
  possibly passed to a command executed through the shell. This
  script is distributed by some operating systems in a manner where
  it is automatically executed. On such operating systems, an
  attacker could execute arbitrary commands with the privileges of
  the script. Use of the c_rehash script is considered obsolete and
  should be replaced by the OpenSSL rehash command line tool. Fixed in
  OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL
  1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected
  1.0.2-1.0.2ze).

- Vulnerability: CVE-2009-3766

  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when
    OpenSSL is used, does not verify the domain name in the subject's
    Common Name (CN) field of an X.509 certificate, which allows
    man-in-the-middle attackers to spoof SSL servers via an arbitrary
    valid certificate.

- Vulnerability: CVE-2022-1292

  - CVSS Score: 10
  - Description: The c_rehash script does not properly sanitise shell metacharacters
    to prevent command injection. This script is distributed by
    some operating systems in a manner where it is automatically
    executed. On such operating systems, an attacker could execute
    arbitrary commands with the privileges of the script. Use of the
    c_rehash script is considered obsolete and should be replaced by the
    OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected
    3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n).
    Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).

- Vulnerability: CVE-2024-38474

  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server
    2.4.59 and earlier allows attacker to execute scripts indirectories
    permitted by the configuration but not directly reachable by anyURL
    or source disclosure of scripts meant to only to be executed as
    CGI.Users are recommended to upgrade to version 2.4.60, which fixes
    this issue.Some RewriteRules that capture and substitute unsafely
    will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2009-3765

  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does
    not properly handle a '\{}0' character in a domain name in the
    subject's Common Name (CN) field of an X.509 certificate, which
    allows man-in-the-middle attackers to spoof arbitrary SSL servers via
    a crafted certificate issued by a legitimate Certification Authority,
    a related issue to CVE-2009-2408.

- Vulnerability: CVE-2019-0190

  - CVSS Score: 5

- Description: A bug exists in the way mod_ssl handled client renegotiations. A remote attacker could send a carefully crafted request that would cause mod_ssl to enter a loop leading to a denial of service. This bug can be only triggered with Apache HTTP Server version 2.4.37 when using OpenSSL version 1.1.1 or later, due to an interaction in changes to handling of renegotiation attempts.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- Vulnerability: CVE-2022-37454

  - CVSS Score: N/A
  - Description: The Keccak XKCP SHA-3 reference implementation before fdc6fef has an integer overflow and resultant buffer overflow that allows attackers to execute arbitrary code or eliminate expected cryptographic properties. This occurs in the sponge function interface.

- Vulnerability: CVE-2021-3711

  - CVSS Score: 7.5
  - Description: In order to decrypt SM2 encrypted data an application is expected to call the API function EVP_PKEY_decrypt(). Typically an application will call this function twice. The first time, on entry, the "out" parameter can be NULL and, on exit, the "outlen" parameter is populated with the buffer size required to hold the decrypted plaintext. The application can then allocate a sufficiently sized buffer and call EVP_PKEY_decrypt() again, but this time passing a non-NULL value for the "out" parameter. A bug in the implementation of the SM2 decryption code means that the calculation of the buffer size required to hold the plaintext returned by the first call to EVP_PKEY_decrypt() can be smaller than the actual size required by the second call. This can lead to a buffer overflow when EVP_PKEY_decrypt() is called by the application a second time with a buffer that is too small. A malicious attacker who is able present SM2 content for decryption to an application could cause attacker chosen data to overflow the buffer by up to a maximum of 62 bytes altering the contents of other data held after the buffer, possibly changing application behaviour or causing the application to crash. The location of the buffer is application dependent but is typically heap allocated. Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k).

- Vulnerability: CVE-2024-0727

  - CVSS Score: N/A

– Description: Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSLto crash leading to a potential Denial of Service attackImpact summary: Applications loading files in the PKCS12 format from untrustedsources might terminate abruptly.A file in PKCS12 format can contain certificates and keys and may come from anuntrusted source. The PKCS12 specification allows certain fields to be NULL, butOpenSSL does not correctly check for this case. This can lead to a NULL pointerdereference that results in OpenSSL crashing. If an application processes PKCS12files from an untrusted source using the OpenSSL APIs then that application willbe vulnerable to this issue.OpenSSL APIs that are vulnerable to this are: PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a similar issue in SMIME_write_PKCS7(). However since thisfunction is related to writing data we do not consider it security significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.

- Vulnerability: CVE-2021-3712

  – CVSS Score: 5.8

  – Description: ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own "d2i" functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the "data" and "length" fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the "data" field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). It can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y).

- Vulnerability: CVE-2023-0464

  – CVSS Score: N/A

- Description: A security vulnerability has been identified in all supported versionsof OpenSSL related to the verification of X.509 certificate chainsthat include policy constraints. Attackers may be able to exploit thisvulnerability by creating a malicious certificate chain that triggersexponential use of computational resources, leading to a denial-of-service(DoS) attack on affected systems.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0465

  - CVSS Score: N/A

  - Description: Applications that use a non-default option when verifying certificates may bevulnerable to an attack from a malicious CA to circumvent certain checks.Invalid certificate policies in leaf certificates are silently ignored byOpenSSL and other certificate policy checks are skipped for that certificate.A malicious CA could use this to deliberately assert invalid certificate policiesin order to circumvent policy checking on the certificate altogether.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0466

  - CVSS Score: N/A

  - Description: The function X509_VERIFY_PARAM_add0_policy() is documented toimplicitly enable the certificate policy check when doing certificateverification. However the implementation of the function does notenable the check which allows certificates with invalid or incorrectpolicies to pass the certificate verification.As suddenly enabling the policy check could break existing deployments it wasdecided to keep the existing behavior of the X509_VERIFY_PARAM_add0_policy()function.Instead the applications that require OpenSSL to perform certificatepolicy check need to use X509_VERIFY_PARAM_set1_policies() or explicitlyenable the policy check by calling X509_VERIFY_PARAM_set_flags() withthe X509_V_FLAG_POLICY_CHECK flag argument.Certificate policy checks are disabled by default in OpenSSL and are notcommonly used by applications.

- Vulnerability: CVE-2013-2220

  - CVSS Score: 7.5

  - Description: Buffer overflow in the radius_get_vendor_attr function in the Radius extension before 1.2.7 for PHP allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a large Vendor Specific Attributes (VSA) length value.

- Vulnerability: CVE-2022-37436

  - CVSS Score: N/A

  - Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2021-3449

  - CVSS Score: 4.3

- Description: An OpenSSL TLS server may crash if sent a maliciously crafted
renegotiation ClientHello message from a client. If a TLSv1.2
renegotiation ClientHello omits the signature_algorithms extension
(where it was present in the initial ClientHello), but includes a
signature_algorithms_cert extension then a NULL pointer dereference
will result, leading to a crash and a denial of service attack. A
server is only vulnerable if it has TLSv1.2 and renegotiation enabled
(which is the default configuration). OpenSSL TLS clients are not
impacted by this issue. All OpenSSL 1.1.1 versions are affected
by this issue. Users of these versions should upgrade to OpenSSL
1.1.1k. OpenSSL 1.0.2 is not impacted by this issue. Fixed in
OpenSSL 1.1.1k (Affected 1.1.1-1.1.1j).

- Vulnerability: CVE-2012-4360

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module
0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote
attackers to inject arbitrary web script or HTML via unspecified
vectors.

- Vulnerability: CVE-2022-22721

  - CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than
350MB (defaults to 1M) on 32 bit systems an integer overflow happens
which later causes out of bounds writes. This issue affects Apache
HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2021-21708

  - CVSS Score: 6.8
  - Description: In PHP versions 7.4.x below 7.4.28, 8.0.x below 8.0.16, and 8.1.x
below 8.1.3, when using filter functions with FILTER_VALIDATE_FLOAT
filter and min/max limits, if the filter fails, there is a
possibility to trigger use of allocated memory after free,
which can result it crashes, and potentially in overwrite of
other memory chunks and RCE. This issue affects: code that uses
FILTER_VALIDATE_FLOAT with min/max limits.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server
allows remote attackers to cause a denial of service (NULL pointer
dereference, process crash, and disk consumption) via a POST request
with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk
Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP
Server does not properly handle certain configuration sections that
specify NiceValue but not AssignUserID, which might allow remote
attackers to gain privileges by leveraging the root uid and root gid
of an mpm-itk process.

- Vulnerability: CVE-2022-0778

  - CVSS Score: 5

- Description: The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - TLS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

- Vulnerability: CVE-2022-31813

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

- Vulnerability: CVE-2024-38476

  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2021-23840

  - CVSS Score: 5

- Description: Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissable length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2021-23841

  - CVSS Score: 4.3
  - Description: The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack. The function X509_issuer_and_serial_hash() is never directly called by OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on certificates that may have been obtained from untrusted sources. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2022-31630

  - CVSS Score: N/A
  - Description: In PHP versions prior to 7.4.33, 8.0.25 and 8.1.12, when using imageloadfont() function in gd extension, it is possible to supply a specially crafted font file, such as if the loaded font is used with imagechar() function, the read outside allocated buffer will be used. This can lead to crashes or disclosure of confidential information.

- Vulnerability: CVE-2023-0286

  - CVSS Score: N/A

- Description: There is a type confusion vulnerability relating to X.400 address processinginside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING butthe public structure definition for GENERAL_NAME incorrectly specified the typeof the x400Address field as ASN1_TYPE. This field is subsequently interpreted bythe OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than anASN1_STRING.When CRL checking is enabled (i.e. the application sets theX509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to passarbitrary pointers to a memcmp call, enabling them to read memory contents orenact a denial of service. In most cases, the attack requires the attacker toprovide both the certificate chain and CRL, neither of which need to have avalid signature. If the attacker only controls one of these inputs, the otherinput must already contain an X.400 address as a CRL distribution point, whichis uncommon. As such, this vulnerability is most likely to only affectapplications which have implemented their own functionality for retrieving CRLsover a network.

- Vulnerability: CVE-2023-3817

  - CVSS Score: N/A

  - Description: Issue summary: Checking excessively long DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH key or DH parameters may experience longdelays. Where the key or parameters that are being checked have been obtainedfrom an untrusted source this may lead to a Denial of Service.The function DH_check() performs various checks on DH parameters. After fixingCVE-2023-3446 it was discovered that a large q parameter value can also triggeran overly long computation during some of these checks. A correct q value,if present, cannot be larger than the modulus p parameter, thus it isunnecessary to perform these checks if q is larger than p.An application that calls DH_check() and supplies a key or parameters obtainedfrom an untrusted source could be vulnerable to a Denial of Service attack.The function DH_check() is itself called by a number of other OpenSSL functions.An application calling any of those other functions may similarly be affected.The other functions affected by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable are the OpenSSL dhparam and pkeyparam command line applicationswhen using the "-check" option.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2023-4807

  - CVSS Score: N/A

- Description: Issue summary: The POLY1305 MAC (message authentication code)
  implementationcontains a bug that might corrupt the internal state
  of applications on theWindows 64 platform when running on newer
  X86_64 processors supporting theAVX512-IFMA instructions.Impact
  summary: If in an application that uses the OpenSSL library an
  attackercan influence whether the POLY1305 MAC algorithm is used,
  the applicationstate might be corrupted with various application
  dependent consequences.The POLY1305 MAC (message authentication
  code) implementation in OpenSSL doesnot save the contents of
  non-volatile XMM registers on Windows 64 platformwhen calculating
  the MAC of data larger than 64 bytes. Before returning tothe
  caller all the XMM registers are set to zero rather than restoring
  theirprevious content. The vulnerable code is used only on newer
  x86_64 processorssupporting the AVX512-IFMA instructions.The
  consequences of this kind of internal application state corruption
  canbe various – from no consequences, if the calling application
  does notdepend on the contents of non-volatile XMM registers at
  all, to the worstconsequences, where the attacker could get complete
  control of the applicationprocess. However given the contents of
  the registers are just zeroized sothe attacker cannot put arbitrary
  values inside, the most likely consequence,if any, would be an
  incorrect result of some application dependentcalculations or a crash
  leading to a denial of service.The POLY1305 MAC algorithm is most
  frequently used as part of theCHACHA20-POLY1305 AEAD (authenticated
  encryption with associated data)algorithm. The most common usage
  of this AEAD cipher is with TLS protocolversions 1.2 and 1.3 and
  a malicious client can influence whether this AEADcipher is used
  by the server. This implies that server applications usingOpenSSL
  can be potentially impacted. However we are currently not aware
  ofany concrete application that would be affected by this issue
  therefore weconsider this a Low severity security issue.As a
  workaround the AVX512-IFMA instructions support can be disabled
  atruntime by setting the environment variable OPENSSL_ia32cap:
  OPENSSL_ia32cap=:~0x200000The FIPS provider is not affected by this
  issue.

- Vulnerability: CVE-2019-1551

  - CVSS Score: 5

  - Description: There is an overflow bug in the x64_64 Montgomery squaring procedure
    used in exponentiation with 512-bit moduli. No EC algorithms are
    affected. Analysis suggests that attacks against 2-prime RSA1024,
    3-prime RSA1536, and DSA1024 as a result of this defect would be
    very difficult to perform and are not believed likely. Attacks
    against DH512 are considered just feasible. However, for an attack
    the target would have to re-use the DH512 private key, which is not
    recommended anyway. Also applications directly using the low level
    API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME. Fixed
    in OpenSSL 1.1.1e (Affected 1.1.1-1.1.1d). Fixed in OpenSSL 1.0.2u
    (Affected 1.0.2-1.0.2t).

- Vulnerability: CVE-2022-22720

  - CVSS Score: 7.5

  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound
    connection when errors are encountered discarding the request body,
    exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2023-25690

  - CVSS Score: N/A

- Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2022-28330

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2020-1967

  - CVSS Score: 5
  - Description: Server or client applications that call the SSL_check_chain() function during or after a TLS 1.3 handshake may crash due to a NULL pointer dereference as a result of incorrect handling of the "signature_algorithms_cert" TLS extension. The crash occurs if an invalid or unrecognised signature algorithm is received from the peer. This could be exploited by a malicious peer in a Denial of Service attack. OpenSSL version 1.1.1d, 1.1.1e, and 1.1.1f are affected by this issue. This issue did not affect OpenSSL versions prior to 1.1.1d. Fixed in OpenSSL 1.1.1g (Affected 1.1.1d-1.1.1f).

- Vulnerability: CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  – CVSS Score: 4.3
  – Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication
    Agent 7.1 before 7.1.1 for Web for Internet Information Services,
    and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to
    inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2021-4160

  – CVSS Score: 4.3
  – Description: There is a carry propagation bug in the MIPS32 and MIPS64 squaring
    procedure. Many EC algorithms are affected, including some of the
    TLS 1.3 default curves. Impact was not analyzed in detail, because
    the pre-requisites for attack are considered unlikely and include
    reusing private keys. Analysis suggests that attacks against RSA and
    DSA as a result of this defect would be very difficult to perform
    and are not believed likely. Attacks against DH are considered
    just feasible (although very difficult) because most of the work
    necessary to deduce information about a private key may be performed
    offline. The amount of resources required for such an attack would
    be significant. However, for an attack on TLS to be meaningful, the
    server would have to share the DH private key among multiple clients,
    which is no longer an option since CVE-2016-0701. This issue affects
    OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the
    releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For
    the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that
    is available to premium support customers only. It will be made
    available in 1.0.2zc when it is released. The issue only affects
    OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0).
    Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL
    1.0.2zc-dev (Affected 1.0.2-1.0.2zb).

- Vulnerability: CVE-2024-38477

  – CVSS Score: N/A
  – Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59
    and earlier allows an attacker to crash the server via a malicious
    request.Users are recommended to upgrade to version 2.4.60, which
    fixes this issue.

- Vulnerability: CVE-2022-26377

  – CVSS Score: 5
  – Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request
    Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server
    allows an attacker to smuggle requests to the AJP server it forwards
    requests to. This issue affects Apache HTTP Server Apache HTTP
    Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2023-45802

  – CVSS Score: N/A

- Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-28614

  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

- Vulnerability: CVE-2023-2650

  - CVSS Score: N/A

- Description: Issue summary: Processing some specially crafted ASN.1 object identifiers ordata containing them may be very slow.Impact summary: Applications that use OBJ_obj2txt() directly, or use any ofthe OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no messagesize limit may experience notable to very long delays when processing thosemessages, which may lead to a Denial of Service.An OBJECT IDENTIFIER is composed of a series of numbers – sub-identifiers –most of which have no size limit. OBJ_obj2txt() may be used to translatean ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSLtype ASN1_OBJECT) to its canonical numeric text form, which are thesub-identifiers of the OBJECT IDENTIFIER in decimal form, separated byperiods.When one of the sub-identifiers in the OBJECT IDENTIFIER is very large(these are sizes that are seen as absurdly large, taking up tens or hundredsof KiBs), the translation to a decimal number in text may take a very longtime. The time complexity is $O(n^2)$ with 'n' being the size of thesub-identifiers in bytes (*).With OpenSSL 3.0, support to fetch cryptographic algorithms using names /identifiers in string form was introduced. This includes using OBJECTIDENTIFIERs in canonical numeric text form as identifiers for fetchingalgorithms.Such OBJECT IDENTIFIERs may be received through the ASN.1 structureAlgorithmIdentifier, which is commonly used in multiple protocols to specifywhat cryptographic algorithm should be used to sign or verify, encrypt ordecrypt, or digest passed data.Applications that call OBJ_obj2txt() directly with untrusted data areaffected, with any version of OpenSSL. If the use is for the mere purposeof display, the severity is considered low.In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME,CMS, CMP/CRMF or TS. It also impacts anything that processes X.509certificates, including simple things like verifying its signature.The impact on TLS is relatively low, because all versions of OpenSSL have a100KiB limit on the peer's certificate chain. Additionally, this onlyimpacts clients, or servers that have explicitly enabled clientauthentication.In OpenSSL 1.1.1 and 1.0.2, this only affects displaying diverse objects,such as X.509 certificates. This is assumed to not happen in such a waythat it would cause a Denial of Service, so these versions are considerednot affected by this issue in such a way that it would be cause for concern,and the severity is therefore considered low.

- Vulnerability: CVE-2023-0215

  - CVSS Score: N/A

- Description: The public API function BIO_new_NDEF is a helper function used for streamingASN.1 data via a BIO. It is primarily used internally to OpenSSL to support theSMIME, CMS and PKCS7 streaming capabilities, but may also be called byend user applications.The function receives a BIO from the caller, prepends a new BIO_f_asn1 filterBIO onto the front of it to form a BIO chain, and then returns the new head ofthe BIO chain to the caller. Under certain conditions, for example if a CMSrecipient public key is invalid, the new filter BIO is freed and the functionreturns a NULL result indicating a failure. However, in this case, the BIO chainis not properly cleaned up and the BIO passed by the caller still retainsinternal pointers to the previously freed filter BIO. If the caller then goes onto call BIO_pop() on the BIO then a use-after-free will occur. This will mostlikely result in a crash.This scenario occurs directly in the internal function B64_write_ASN1() whichmay cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() onthe BIO. This internal function is in turn called by the public API functionsPEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream,SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7.Other public API functions that may be impacted by this includei2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream andi2d_PKCS7_bio_stream.The OpenSSL cms and smime command line applications are similarly affected.

- Vulnerability: CVE-2022-29404

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2012-3526

  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2009-3767

  - CVSS Score: 4.3
  - Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other versions, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2022-28615

  - CVSS Score: 6.4

- Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- Vulnerability: CVE-2023-31122

  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2023-27522

  - CVSS Score: N/A
  - Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.Special characters in the origin response header can truncate/split the response forwarded to the client.

11.14   IP Address: 159.149.15.22

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 2

- High Vulnerabilities: 66

- Medium Vulnerabilities: 211

- Low Vulnerabilities: 23

- Total Vulnerabilities: 302

Services Running on IP Address

- Service: Apache httpd

  – Port: 80
  – Version: 2.4.18
  – Location: https://159.149.15.22/

- Service: Apache httpd

  – Port: 443
  – Version: 2.4.18
  – Location: /

Vulnerabilities Found

- Vulnerability: CVE-2019-0220

  – CVSS Score: 5
  – Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.

- Vulnerability: CVE-2017-3169

  – CVSS Score: 7.5
  – Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.

- Vulnerability: CVE-2024-27316

  – CVSS Score: N/A
  – Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

- Vulnerability: CVE-2017-7679

  – CVSS Score: 7.5
  – Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

- Vulnerability: CVE-2013-2765

  – CVSS Score: 5

  – Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2020-1934

  – CVSS Score: 5

  – Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

- Vulnerability: CVE-2018-17189

  – CVSS Score: 5

  – Description: In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 (mod_http2) connections.

- Vulnerability: CVE-2022-36760

  – CVSS Score: N/A

  – Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2020-35452

  – CVSS Score: 6.8

  – Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

- Vulnerability: CVE-2017-9798

  – CVSS Score: 5

  – Description: Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.

- Vulnerability: CVE-2016-1546

  – CVSS Score: 4.3

  – Description: The Apache HTTP Server 2.4.17 and 2.4.18, when mod_http2 is enabled, does not limit the number of simultaneous stream workers for a single HTTP/2 connection, which allows remote attackers to cause a denial of service (stream-processing outage) via modified flow-control windows.

- Vulnerability: CVE-2022-29404
  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2021-33193
  - CVSS Score: 5
  - Description: A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.

- Vulnerability: CVE-2009-0796
  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2013-4365
  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2018-1333
  - CVSS Score: 5
  - Description: By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.18-2.4.30,2.4.33).

- Vulnerability: CVE-2022-22720
  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2018-11763
  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.17 to 2.4.34, by sending continuous, large SETTINGS frames a client can occupy a connection, server thread and CPU time without any connection timeout coming to effect. This affects only HTTP/2 connections. A possible mitigation is to not enable the h2 protocol.

- Vulnerability: CVE-2022-28330
  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2021-32791
  - CVSS Score: 4.3

- Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2021-32792

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.

- Vulnerability: CVE-2023-31122

  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2016-8612

  - CVSS Score: 3.3
  - Description: Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.

- Vulnerability: CVE-2024-38476

  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-38477

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-38474

  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2019-0196

- CVSS Score: 5
- Description: A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.

- **Vulnerability:** CVE-2019-0211

  - CVSS Score: 7.2
  - Description: In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.

- **Vulnerability:** CVE-2022-22721

  - CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- **Vulnerability:** CVE-2006-20001

  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- **Vulnerability:** CVE-2019-10092

  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

- **Vulnerability:** CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- **Vulnerability:** CVE-2019-17567

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

- Vulnerability: CVE-2017-15715

  – CVSS Score: 6.8
  – Description: In Apache httpd 2.4.0 to 2.4.29, the expression specified in
    <FilesMatch> could match '$' to a newline character in a malicious
    filename, rather than matching only the end of the filename. This
    could be exploited in environments where uploads of some files are
    are externally blocked, but only by matching the trailing portion of
    the filename.

- Vulnerability: CVE-2022-31813

  – CVSS Score: 7.5
  – Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-*
    headers to the origin server based on client side Connection
    header hop-by-hop mechanism. This may be used to bypass IP based
    authentication on the origin server/application.

- Vulnerability: CVE-2012-4001

  – CVSS Score: 5
  – Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server
    does not properly verify its host name, which allows remote attackers
    to trigger HTTP requests to arbitrary hosts via unspecified vectors,
    as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2019-10098

  – CVSS Score: 5.8
  – Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with
    mod_rewrite that were intended to be self-referential might be fooled
    by encoded newlines and redirect instead to an unexpected URL within
    the request URL.

- Vulnerability: CVE-2022-37436

  – CVSS Score: N/A
  – Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause
    the response headers to be truncated early, resulting in some headers
    being incorporated into the response body. If the later headers have
    any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2016-5387

  – CVSS Score: 6.8
  – Description: The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18
    and therefore does not protect applications from the presence of
    untrusted client data in the HTTP_PROXY environment variable, which
    might allow remote attackers to redirect an application's outbound
    HTTP traffic to an arbitrary proxy server via a crafted Proxy header
    in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states
    "This mitigation has been assigned the identifier CVE-2016-5387"; in
    other words, this is not a CVE ID for a vulnerability.

- Vulnerability: CVE-2012-4360

  – CVSS Score: 4.3
  – Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module
    0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote
    attackers to inject arbitrary web script or HTML via unspecified
    vectors.

- Vulnerability: CVE-2021-40438

- CVSS Score: 6.8
- Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2022-23943

  - CVSS Score: 7.5
  - Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

- Vulnerability: CVE-2020-1927

  - CVSS Score: 5.8
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.

- Vulnerability: CVE-2018-17199

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

- Vulnerability: CVE-2017-9788

  - CVSS Score: 6.4
  - Description: In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.

- Vulnerability: CVE-2017-15710

  - CVSS Score: 5

- Description: In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.

- Vulnerability: CVE-2016-4975

  - CVSS Score: 4.3
  - Description: Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).

- Vulnerability: CVE-2018-1302

  - CVSS Score: 4.3
  - Description: When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.

- Vulnerability: CVE-2018-1303

  - CVSS Score: 5
  - Description: A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache. The vulnerability is considered as low risk since mod_cache_socache is not widely used, mod_cache_disk is not concerned by this vulnerability.

- Vulnerability: CVE-2017-3167

  - CVSS Score: 7.5
  - Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.

- Vulnerability: CVE-2021-34798

  - CVSS Score: 5
  - Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2023-25690

  - CVSS Score: N/A

- Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2021-32786

  - CVSS Score: 5.8
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, 'oidc_validate_redirect_url()' does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring 'mod_auth_openidc' to only allow redirection whose destination matches a given regular expression.

- Vulnerability: CVE-2021-32785

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache ('OIDCCacheEncrypt off', 'OIDCSessionType server-cache', 'OIDCCacheType redis'), 'mod_auth_openidc' wrongly performed argument interpolation before passing Redis requests to 'hiredis', which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the 'hiredis' API. As a workaround, this vulnerability can be mitigated by setting 'OIDCCacheEncrypt' to 'on', as cache keys are cryptographically hashed before use when this option is enabled.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2021-44224

- CVSS Score: 6.4
- Description: A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).

- Vulnerability: CVE-2020-11985

  - CVSS Score: 4.3
  - Description: IP address spoofing when proxying using mod_remoteip and mod_rewrite For configurations using proxying with mod_remoteip and certain mod_rewrite rules, an attacker could spoof their IP address for logging and PHP scripts. Note this issue was fixed in Apache HTTP Server 2.4.24 but was retrospectively allocated a low severity CVE in 2020.

- Vulnerability: CVE-2021-44790

  - CVSS Score: 7.5
  - Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2016-4979

  - CVSS Score: 5
  - Description: The Apache HTTP Server 2.4.18 through 2.4.20, when mod_http2 and mod_ssl are enabled, does not properly recognize the "SSLVerifyClient require" directive for HTTP/2 request authorization, which allows remote attackers to bypass intended access restrictions by leveraging the ability to send multiple requests over a single connection and aborting a renegotiation.

- Vulnerability: CVE-2012-3526

  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2018-1301

  - CVSS Score: 4.3
  - Description: A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.

- Vulnerability: CVE-2021-26690

  – CVSS Score: 5
  – Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted
                 Cookie header handled by mod_session can cause a NULL pointer
                 dereference and crash, leading to a possible Denial Of Service

- Vulnerability: CVE-2021-26691

  – CVSS Score: 7.5
  – Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted
                 SessionHeader sent by an origin server could cause a heap overflow

- Vulnerability: CVE-2022-26377

  – CVSS Score: 5
  – Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request
                 Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server
                 allows an attacker to smuggle requests to the AJP server it forwards
                 requests to. This issue affects Apache HTTP Server Apache HTTP
                 Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2007-4723

  – CVSS Score: 7.5
  – Description: Directory traversal vulnerability in Ragnarok Online Control Panel
                 4.3.4a, when the Apache HTTP Server is used, allows remote attackers
                 to bypass authentication via directory traversal sequences in a URI
                 that ends with the name of a publicly available page, as demonstrated
                 by a "/...../" sequence and an account_manage.php/login.php final
                 component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2023-45802

  – CVSS Score: N/A
  – Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a
                 time window were the request's memory resources were not reclaimed
                 immediately. Instead, de-allocation was deferred to connection
                 close. A client could send new requests and resets, keeping the
                 connection busy and open and causing the memory footprint to keep
                 on growing. On connection close, all resources were reclaimed, but
                 the process might run out of memory before that.This was found by
                 the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset
                 Exploit) with their own test client. During "normal" HTTP/2 use, the
                 probability to hit this bug is very low. The kept memory would not
                 become noticeable before the connection closes or times out.Users are
                 recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-28614

  – CVSS Score: 5
  – Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier
                 may read unintended memory if an attacker can cause the server to
                 reflect very large input using ap_rwrite() or ap_rputs(), such as
                 with mod_luas r:puts() function. Modules compiled and distributed
                 separately from Apache HTTP Server that use the 'ap_rputs' function
                 and may pass it a very large (INT_MAX or larger) string must be
                 compiled against current headers to resolve the issue.

- Vulnerability: CVE-2020-13938

  – CVSS Score: 2.1

- Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

- **Vulnerability:** CVE-2009-2299

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- **Vulnerability:** CVE-2018-1283

  - CVSS Score: 3.5
  - Description: In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to forward its session data to CGI applications (SessionEnv on, not the default), a remote user may influence their content by using a "Session" header. This comes from the "HTTP_SESSION" variable name used by mod_session to forward its data to CGIs, since the prefix "HTTP_" is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications.

- **Vulnerability:** CVE-2019-10082

  - CVSS Score: 6.4
  - Description: In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.

- **Vulnerability:** CVE-2018-1312

  - CVSS Score: 6.8
  - Description: In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

- **Vulnerability:** CVE-2016-8740

  - CVSS Score: 5
  - Description: The mod_http2 module in the Apache HTTP Server 2.4.17 through 2.4.23, when the Protocols configuration includes h2 or h2c, does not restrict request-header length, which allows remote attackers to cause a denial of service (memory consumption) via crafted CONTINUATION frames in an HTTP/2 request.

- **Vulnerability:** CVE-2016-8743

  - CVSS Score: 5
  - Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

- **Vulnerability:** CVE-2024-40898

  - CVSS Score: N/A

- Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2019-0217

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.

- Vulnerability: CVE-2021-39275

  - CVSS Score: 7.5
  - Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2022-28615

  - CVSS Score: 6.4
  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- Vulnerability: CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2011-1047

  - CVSS Score: 7.5
  - Description: Multiple SQL injection vulnerabilities in VastHTML Forum Server (aka ForumPress) plugin 1.6.1 and 1.6.5 for WordPress allow remote attackers to execute arbitrary SQL commands via the (1) search_max parameter in a search action to index.php, which is not properly handled by wpf.class.php, (2) id parameter in an editpost action to index.php, which is not properly handled by wpf-post.php, or (3) topic parameter to feed.php.

- Vulnerability: CVE-2020-36326

  - CVSS Score: 7.5

- Description: PHPMailer 6.1.8 through 6.4.0 allows object injection through Phar Deserialization via addAttachment with a UNC pathname. NOTE: this is similar to CVE-2018-19296, but arose because 6.1.8 fixed a functionality problem in which UNC pathnames were always considered unreadable by PHPMailer, even in safe contexts. As an unintended side effect, this fix eliminated the code that blocked addAttachment exploitation.

- Vulnerability: CVE-2019-17673

  - CVSS Score: 5
  - Description: WordPress before 5.2.4 is vulnerable to poisoning of the cache of JSON GET requests because certain requests lack a Vary: Origin header.

- Vulnerability: CVE-2019-17672

  - CVSS Score: 4.3
  - Description: WordPress before 5.2.4 is vulnerable to a stored XSS attack to inject JavaScript into STYLE elements.

- Vulnerability: CVE-2019-17671

  - CVSS Score: 5
  - Description: In WordPress before 5.2.4, unauthenticated viewing of certain content is possible because the static query property is mishandled.

- Vulnerability: CVE-2019-17670

  - CVSS Score: 7.5
  - Description: WordPress before 5.2.4 has a Server Side Request Forgery (SSRF) vulnerability because Windows paths are mishandled during certain validation of relative URLs.

- Vulnerability: CVE-2019-17675

  - CVSS Score: 6.8
  - Description: WordPress before 5.2.4 does not properly consider type confusion during validation of the referer in the admin pages, possibly leading to CSRF.

- Vulnerability: CVE-2019-17674

  - CVSS Score: 3.5
  - Description: WordPress before 5.2.4 is vulnerable to stored XSS (cross-site scripting) via the Customizer.

- Vulnerability: CVE-2012-0898

  - CVSS Score: 5
  - Description: Directory traversal vulnerability in meb_download.php in the myEASYbackup plugin 1.0.8.1 for WordPress allows remote attackers to read arbitrary files via a .. (dot dot) in the dwn_file parameter.

- Vulnerability: CVE-2008-4625

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in stnl_iframe.php in the ShiftThis Newsletter (st_newsletter) plugin for WordPress allows remote attackers to execute arbitrary SQL commands via the newsletter parameter, a different vector than CVE-2008-0683.

- Vulnerability: CVE-2019-17567

  - CVSS Score: 5

- Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

- Vulnerability: CVE-2013-4365

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2012-0895

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in map/map.php in the Count Per Day module before 3.1.1 for WordPress allows remote attackers to inject arbitrary web script or HTML via the map parameter.

- Vulnerability: CVE-2017-3169

  - CVSS Score: 7.5
  - Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.

- Vulnerability: CVE-2022-28330

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2012-0896

  - CVSS Score: 5
  - Description: Absolute path traversal vulnerability in download.php in the Count Per Day module before 3.1.1 for WordPress allows remote attackers to read arbitrary files via the f parameter.

- Vulnerability: CVE-2021-32791

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2021-32792

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.

- Vulnerability: CVE-2023-31122

  – CVSS Score: N/A
  – Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2009-2852

  – CVSS Score: 6.8
  – Description: WP-Syntax plugin 0.9.1 and earlier for Wordpress, with register_globals enabled, allows remote attackers to execute arbitrary PHP code via the test_filter[wp_head] array parameter to test/index.php, which is used in a call to the call_user_func_array function.

- Vulnerability: CVE-2024-38476

  – CVSS Score: N/A
  – Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2010-3977

  – CVSS Score: 4.3
  – Description: Multiple cross-site scripting (XSS) vulnerabilities in wp-content/plugins/cforms/lib_ajax.php in cforms WordPress plugin 11.5 allow remote attackers to inject arbitrary web script or HTML via the (1) rs and (2) rsargs[] parameters.

- Vulnerability: CVE-2024-38474

  – CVSS Score: N/A
  – Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2010-4825

  – CVSS Score: 4.3
  – Description: Cross-site scripting (XSS) vulnerability in magpie_debug.php in the Twitter Feed plugin (wp-twitter-feed) 0.3.1 for WordPress allows remote attackers to inject arbitrary web script or HTML via the url parameter.

- Vulnerability: CVE-2009-0796

  – CVSS Score: 2.6
  – Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2020-11028

  – CVSS Score: 4.3

- Description: In affected versions of WordPress, some private posts, which were previously public, can result in unauthenticated disclosure under a specific set of conditions. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).

- Vulnerability: CVE-2020-11029

  - CVSS Score: 4.3

  - Description: In affected versions of WordPress, a vulnerability in the stats() method of class-wp-object-cache.php can be exploited to execute cross-site scripting (XSS) attacks. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).

- Vulnerability: CVE-2016-1546

  - CVSS Score: 4.3

  - Description: The Apache HTTP Server 2.4.17 and 2.4.18, when mod_http2 is enabled, does not limit the number of simultaneous stream workers for a single HTTP/2 connection, which allows remote attackers to cause a denial of service (stream-processing outage) via modified flow-control windows.

- Vulnerability: CVE-2020-11025

  - CVSS Score: 3.5

  - Description: In affected versions of WordPress, a cross-site scripting (XSS) vulnerability in the navigation section of Customizer allows JavaScript code to be executed. Exploitation requires an authenticated user. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).

- Vulnerability: CVE-2020-11026

  - CVSS Score: 3.5

  - Description: In affected versions of WordPress, files with a specially crafted name when uploaded to the Media section can lead to script execution upon accessing the file. This requires an authenticated user with privileges to upload files. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).

- Vulnerability: CVE-2020-11027

  - CVSS Score: 5.5

  - Description: In affected versions of WordPress, a password reset link emailed to a user does not expire upon changing the user password. Access would be needed to the email account of the user by a malicious party for successful execution. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).

- Vulnerability: CVE-2011-3981

  - CVSS Score: 7.5

- Description: PHP remote file inclusion vulnerability in actions.php in the Allwebmenus plugin 1.1.3 for WordPress allows remote attackers to execute arbitrary PHP code via a URL in the abspath parameter.

- Vulnerability: CVE-2020-11022

  - CVSS Score: 4.3
  - Description: In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

- Vulnerability: CVE-2020-7656

  - CVSS Score: 4.3
  - Description: jquery prior to 1.9.0 allows Cross-site Scripting attacks via the load method. The load method fails to recognize and remove "<script>" HTML tags that contain a whitespace character, i.e: "</script >", which results in the enclosed script logic to be executed.

- Vulnerability: CVE-2008-4733

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in wpcommentremix.php in WP Comment Remix plugin before 1.4.4 for WordPress allows remote attackers to inject arbitrary web script or HTML via the (1) replytotext, (2) quotetext, (3) originallypostedby, (4) sep, (5) maxtags, (6) tagsep, (7) tagheadersep, (8) taglabel, and (9) tagheaderlabel parameters.

- Vulnerability: CVE-2009-0968

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in fmoblog.php in the fMoblog plugin 2.1 for WordPress allows remote attackers to execute arbitrary SQL commands via the id parameter to index.php. NOTE: some of these details are obtained from third party information.

- Vulnerability: CVE-2018-1000773

  - CVSS Score: 6.5
  - Description: WordPress version 4.9.8 and earlier contains a CWE-20 Input Validation vulnerability in thumbnail processing that can result in remote code execution due to an incomplete fix for CVE-2017-1000600. This attack appears to be exploitable via thumbnail upload by an authenticated user and may require additional plugins in order to be exploited however this has not been confirmed at this time.

- Vulnerability: CVE-2011-3853

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the Hybrid theme before 0.10 for WordPress allows remote attackers to inject arbitrary web script or HTML via the cpage parameter.

- Vulnerability: CVE-2008-4734

  - CVSS Score: 7.5

- Description: Cross-site request forgery (CSRF) vulnerability in the
  wpcr_do_options_page function in WP Comment Remix plugin before 1.4.4
  for WordPress allows remote attackers to perform unauthorized actions
  as administrators via a request that sets the wpcr_hidden_form_input
  parameter.

- Vulnerability: CVE-2020-1927

  - CVSS Score: 5.8
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with
    mod_rewrite that were intended to be self-referential might be fooled
    by encoded newlines and redirect instead to an an unexpected URL
    within the request URL.

- Vulnerability: CVE-2011-3852

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the EvoLve theme before
    1.2.6 for WordPress allows remote attackers to inject arbitrary web
    script or HTML via the s parameter.

- Vulnerability: CVE-2011-0641

  - CVSS Score: 4.3
  - Description: Multiple cross-site scripting (XSS) vulnerabilities in
    wp-admin/admin.php in the StatPressCN plugin 1.9.0 for WordPress
    allow remote attackers to inject arbitrary web script or HTML via the
    (1) what1, (2) what2, (3) what3, (4) what4, and (5) what5 parameters.
    NOTE: the provenance of this information is unknown; the details are
    obtained solely from third party information.

- Vulnerability: CVE-2018-17189

  - CVSS Score: 5
  - Description: In Apache HTTP server versions 2.4.37 and prior, by sending request
    bodies in a slow loris way to plain resources, the h2 stream for
    that request unnecessarily occupied a server thread cleaning up that
    incoming data. This affects only HTTP/2 (mod_http2) connections.

- Vulnerability: CVE-2020-25286

  - CVSS Score: 5
  - Description: In wp-includes/comment-template.php in WordPress before 5.4.2,
    comments from a post or page could sometimes be seen in the latest
    comments even if the post or page was not public.

- Vulnerability: CVE-2016-4979

  - CVSS Score: 5
  - Description: The Apache HTTP Server 2.4.18 through 2.4.20, when mod_http2 and
    mod_ssl are enabled, does not properly recognize the "SSLVerifyClient
    require" directive for HTTP/2 request authorization, which allows
    remote attackers to bypass intended access restrictions by leveraging
    the ability to send multiple requests over a single connection and
    aborting a renegotiation.

- Vulnerability: CVE-2009-4424

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in results.php in the Pyrmont plugin
    2 for WordPress allows remote attackers to execute arbitrary SQL
    commands via the id parameter.

- Vulnerability: CVE-2011-4669

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in wp-users.php in WordPress Users plugin 1.3 and possibly earlier for WordPress allows remote attackers to execute arbitrary SQL commands via the uid parameter to index.php.

- Vulnerability: CVE-2021-32786

  - CVSS Score: 5.8
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, 'oidc_validate_redirect_url()' does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring 'mod_auth_openidc' to only allow redirection whose destination matches a given regular expression.

- Vulnerability: CVE-2021-32785

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache ('OIDCCacheEncrypt off', 'OIDCSessionType server-cache', 'OIDCCacheType redis'), 'mod_auth_openidc' wrongly performed argument interpolation before passing Redis requests to 'hiredis', which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the 'hiredis' API. As a workaround, this vulnerability can be mitigated by setting 'OIDCCacheEncrypt' to 'on', as cache keys are cryptographically hashed before use when this option is enabled.

- Vulnerability: CVE-2012-2920

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the userphoto_options_page function in user-photo.php in the User Photo plugin before 0.9.5.2 for WordPress allows remote attackers to inject arbitrary web script or HTML via the PATH_INFO to wp-admin/options-general.php. NOTE: some of these details are obtained from third party information.

- Vulnerability: CVE-2021-34798

  - CVSS Score: 5
  - Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2008-7040

  - CVSS Score: 7.5

743

– Description: SQL injection vulnerability in ahah/sf-profile.php in the Yellow
                  Swordfish Simple Forum module for Wordpress allows remote attackers
                  to execute arbitrary SQL commands via the u parameter. NOTE: this
                  issue was disclosed by an unreliable researcher, so the details might
                  be incorrect.
- Vulnerability: CVE-2021-44790

  – CVSS Score: 7.5
  – Description: A carefully crafted request body can cause a buffer overflow in the
                  mod_lua multipart parser (r:parsebody() called from Lua scripts).
                  The Apache httpd team is not aware of an exploit for the vulnerabilty
                  though it might be possible to craft one. This issue affects Apache
                  HTTP Server 2.4.51 and earlier.
- Vulnerability: CVE-2022-3590

  – CVSS Score: N/A
  – Description: WordPress is affected by an unauthenticated blind SSRF in the
                  pingback feature. Because of a TOCTOU race condition between the
                  validation checks and the HTTP request, attackers can reach internal
                  hosts that are explicitly forbidden.
- Vulnerability: CVE-2012-1068

  – CVSS Score: 4.3
  – Description: Cross-site scripting (XSS) vulnerability in the rc_ajax function in
                  core.php in the WP-RecentComments plugin before 2.0.7 for WordPress
                  allows remote attackers to inject arbitrary web script or HTML via
                  the page parameter, related to AJAX paging.
- Vulnerability: CVE-2020-4049

  – CVSS Score: 3.5
  – Description: In affected versions of WordPress, when uploading themes, the name
                  of the theme folder can be crafted in a way that could lead to
                  JavaScript execution in /wp-admin on the themes page. This does
                  require an admin to upload the theme, and is low severity self-XSS.
                  This has been patched in version 5.4.2, along with all the previously
                  affected versions via a minor release (5.3.4, 5.2.7, 5.1.6, 5.0.10,
                  4.9.15, 4.8.14, 4.7.18, 4.6.19, 4.5.22, 4.4.23, 4.3.24, 4.2.28,
                  4.1.31, 4.0.31, 3.9.32, 3.8.34, 3.7.34).
- Vulnerability: CVE-2020-4048

  – CVSS Score: 4.9
  – Description: In affected versions of WordPress, due to an issue in
                  wp_validate_redirect() and URL sanitization, an arbitrary external
                  link can be crafted leading to unintended/open redirect when clicked.
                  This has been patched in version 5.4.2, along with all the previously
                  affected versions via a minor release (5.3.4, 5.2.7, 5.1.6, 5.0.10,
                  4.9.15, 4.8.14, 4.7.18, 4.6.19, 4.5.22, 4.4.23, 4.3.24, 4.2.28,
                  4.1.31, 4.0.31, 3.9.32, 3.8.34, 3.7.34).
- Vulnerability: CVE-2020-4047

  – CVSS Score: 3.5
  – Description: In affected versions of WordPress, authenticated users with upload
                  permissions (like authors) are able to inject JavaScript into some
                  media file attachment pages in a certain way. This can lead to
                  script execution in the context of a higher privileged user when
                  the file is viewed by them. This has been patched in version 5.4.2,
                  along with all the previously affected versions via a minor release
                  (5.3.4, 5.2.7, 5.1.6, 5.0.10, 4.9.15, 4.8.14, 4.7.18, 4.6.19, 4.5.22,
                  4.4.23, 4.3.24, 4.2.28, 4.1.31, 4.0.31, 3.9.32, 3.8.34, 3.7.34).

- Vulnerability: CVE-2020-4046

    - CVSS Score: 3.5
    - Description: In affected versions of WordPress, users with low privileges (like contributors and authors) can use the embed block in a certain way to inject unfiltered HTML in the block editor. When affected posts are viewed by a higher privileged user, this could lead to script execution in the editor/wp-admin. This has been patched in version 5.4.2, along with all the previously affected versions via a minor release (5.3.4, 5.2.7, 5.1.6, 5.0.10, 4.9.15, 4.8.14, 4.7.18, 4.6.19, 4.5.22, 4.4.23, 4.3.24, 4.2.28, 4.1.31, 4.0.31, 3.9.32, 3.8.34, 3.7.34).

- Vulnerability: CVE-2012-1067

    - CVSS Score: 7.5
    - Description: SQL injection vulnerability in the WP-RecentComments plugin 2.0.7 for WordPress allows remote attackers to execute arbitrary SQL commands via the id parameter in an rc-content action to index.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.

- Vulnerability: CVE-2009-2143

    - CVSS Score: 7.5
    - Description: PHP remote file inclusion vulnerability in firestats-wordpress.php in the FireStats plugin before 1.6.2-stable for WordPress allows remote attackers to execute arbitrary PHP code via a URL in the fs_javascript parameter.

- Vulnerability: CVE-2016-4975

    - CVSS Score: 4.3
    - Description: Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).

- Vulnerability: CVE-2020-13938

    - CVSS Score: 2.1
    - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

- Vulnerability: CVE-2009-2383

    - CVSS Score: 7.5
    - Description: SQL injection vulnerability in BTE_RW_webajax.php in the Related Sites plugin 2.1 for WordPress allows remote attackers to execute arbitrary SQL commands via the guid parameter.

- Vulnerability: CVE-2008-7175

    - CVSS Score: 4.3
    - Description: Cross-site scripting (XSS) vulnerability in wp-admin/admin.php in NextGEN Gallery 0.96 and earlier plugin for Wordpress allows remote attackers to inject arbitrary web script or HTML via the picture description field in a page edit action.

- Vulnerability: CVE-2018-1312

- CVSS Score: 6.8
- Description: In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

- Vulnerability: CVE-2009-4748

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mycategoryorder.php in the My Category Order plugin 2.8 and earlier for WordPress allows remote attackers to execute arbitrary SQL commands via the parentID parameter in an act_OrderCategories action to wp-admin/post-new.php.

- Vulnerability: CVE-2009-2144

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in the FireStats plugin before 1.6.2-stable for WordPress allows remote attackers to execute arbitrary SQL commands via unspecified vectors.

- Vulnerability: CVE-2020-11030

  - CVSS Score: 3.5
  - Description: In affected versions of WordPress, a special payload can be crafted that can lead to scripts getting executed within the search block of the block editor. This requires an authenticated user with the ability to add content. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).

- Vulnerability: CVE-2023-39999

  - CVSS Score: N/A
  - Description: Exposure of Sensitive Information to an Unauthorized Actor in WordPressfrom 6.3 through 6.3.1, from 6.2 through 6.2.2, from 6.1 through 6.13, from 6.0 through 6.0.5, from 5.9 through 5.9.7, from 5.8 through 5.8.7, from 5.7 through 5.7.9, from 5.6 through 5.6.11, from 5.5 through 5.5.12, from 5.4 through 5.4.13, from 5.3 through 5.3.15, from 5.2 through 5.2.18, from 5.1 through 5.1.16, from 5.0 through 5.0.19, from 4.9 through 4.9.23, from 4.8 through 4.8.22, from 4.7 through 4.7.26, from 4.6 through 4.6.26, from 4.5 through 4.5.29, from 4.4 through 4.4.30, from 4.3 through 4.3.31, from 4.2 through 4.2.35, from 4.1 through 4.1.38.

- Vulnerability: CVE-2020-35452

  - CVSS Score: 6.8
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

- Vulnerability: CVE-2021-29450

  - CVSS Score: 4

– Description: Wordpress is an open source CMS. One of the blocks in the WordPress editor can be exploited in a way that exposes password-protected posts and pages. This requires at least contributor privileges. This has been patched in WordPress 5.7.1, along with the older affected versions via minor releases. It's strongly recommended that you keep auto-updates enabled to receive the fix.

• Vulnerability: CVE-2016-5387

  – CVSS Score: 6.8
  – Description: The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.

• Vulnerability: CVE-2020-1934

  – CVSS Score: 5
  – Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

• Vulnerability: CVE-2011-5082

  – CVSS Score: 4.3
  – Description: Cross-site scripting (XSS) vulnerability in the s2Member Pro plugin before 111220 for WordPress allows remote attackers to inject arbitrary web script or HTML via the s2member_pro_authnet_checkout[coupon] parameter (aka Coupon Code field).

• Vulnerability: CVE-2011-4646

  – CVSS Score: 6
  – Description: SQL injection vulnerability in wp-postratings.php in the WP-PostRatings plugin 1.50, 1.61, and probably other versions before 1.62 for WordPress allows remote authenticated users with the Author role to execute arbitrary SQL commands via the id attribute of the ratings shortcode when creating a post. NOTE: some of these details are obtained from third party information.

• Vulnerability: CVE-2022-23943

  – CVSS Score: 7.5
  – Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

• Vulnerability: CVE-2018-1333

  – CVSS Score: 5
  – Description: By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.18-2.4.30,2.4.33).

• Vulnerability: CVE-2009-3703

  – CVSS Score: 7.5

– Description: Multiple SQL injection vulnerabilities in the WP-Forum plugin before
2.4 for WordPress allow remote attackers to execute arbitrary SQL
commands via (1) the search max parameter in a search action to the
default URI, related to wpf.class.php; (2) the forum parameter to
an unspecified component, related to wpf.class.php; (3) the topic
parameter in a viewforum action to the default URI, related to the
remove topic function in wpf.class.php; or the id parameter in a
(4) editpost or (5) viewtopic action to the default URI, related to
wpf-post.php.

- Vulnerability: CVE-2018-11763

    – CVSS Score: 4.3

    – Description: In Apache HTTP Server 2.4.17 to 2.4.34, by sending continuous, large
SETTINGS frames a client can occupy a connection, server thread and
CPU time without any connection timeout coming to effect. This
affects only HTTP/2 connections. A possible mitigation is to not
enable the h2 protocol.

- Vulnerability: CVE-2023-22622

    – CVSS Score: N/A

    – Description: WordPress through 6.1.1 depends on unpredictable client visits to
cause wp-cron.php execution and the resulting security updates,
and the source code describes "the scenario where a site may not
receive enough visits to execute scheduled tasks in a timely manner,"
but neither the installation guide nor the security guide mentions
this default behavior, or alerts the user about security risks on
installations with very few visits.

- Vulnerability: CVE-2009-2396

    – CVSS Score: 9.3

    – Description: PHP remote file inclusion vulnerability in template/album.php in DM
Albums 1.9.2, as used standalone or as a WordPress plugin, allows
remote attackers to execute arbitrary PHP code via a URL in the
SECURITY FILE parameter.

- Vulnerability: CVE-2024-40898

    – CVSS Score: N/A

    – Description: SSRF in Apache HTTP Server on Windows with mod rewrite in
server/vhost context, allows to potentially leak NTML hashes to
a malicious server via SSRF and malicious requests.Users are
recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2020-4050

    – CVSS Score: 6

    – Description: In affected versions of WordPress, misuse of the 'set-screen-option'
filter's return value allows arbitrary user meta fields to be saved.
It does require an admin to install a plugin that would misuse the
filter. Once installed, it can be leveraged by low privileged users.
This has been patched in version 5.4.2, along with all the previously
affected versions via a minor release (5.3.4, 5.2.7, 5.1.6, 5.0.10,
4.9.15, 4.8.14, 4.7.18, 4.6.19, 4.5.22, 4.4.23, 4.3.24, 4.2.28,
4.1.31, 4.0.31, 3.9.32, 3.8.34, 3.7.34).

- Vulnerability: CVE-2019-0217

    – CVSS Score: 6

- Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.

- Vulnerability: CVE-2019-0196

  - CVSS Score: 5
  - Description: A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.

- Vulnerability: CVE-2021-33193

  - CVSS Score: 5
  - Description: A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.

- Vulnerability: CVE-2019-0211

  - CVSS Score: 7.2
  - Description: In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.

- Vulnerability: CVE-2011-3855

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the F8 Lite theme before 4.2.2 for WordPress allows remote attackers to inject arbitrary web script or HTML via the s parameter.

- Vulnerability: CVE-2011-3854

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the ZenLite theme before 4.4 for WordPress allows remote attackers to inject arbitrary web script or HTML via the s parameter.

- Vulnerability: CVE-2011-3857

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the Antisnews theme before 1.10 for WordPress allows remote attackers to inject arbitrary web script or HTML via the s parameter.

- Vulnerability: CVE-2011-3856

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the Elegant Grunge theme before 1.0.4 for WordPress allows remote attackers to inject arbitrary web script or HTML via the s parameter.

- Vulnerability: CVE-2011-3851

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the News theme before 0.2 for WordPress allows remote attackers to inject arbitrary web script or HTML via the cpage parameter.

- Vulnerability: CVE-2011-3850
  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the Atahualpa theme before 3.6.8 for WordPress allows remote attackers to inject arbitrary web script or HTML via the s parameter.

- Vulnerability: CVE-2019-16218
  - CVSS Score: 4.3
  - Description: WordPress before 5.2.3 allows XSS in stored comments.

- Vulnerability: CVE-2019-16219
  - CVSS Score: 4.3
  - Description: WordPress before 5.2.3 allows XSS in shortcode previews.

- Vulnerability: CVE-2019-16217
  - CVSS Score: 4.3
  - Description: WordPress before 5.2.3 allows XSS in media uploads because wp_ajax_upload_attachment is mishandled.

- Vulnerability: CVE-2012-0934
  - CVSS Score: 7.5
  - Description: PHP remote file inclusion vulnerability in ajax/savetag.php in the Theme Tuner plugin for WordPress before 0.8 allows remote attackers to execute arbitrary PHP code via a URL in the tt-abspath parameter.

- Vulnerability: CVE-2011-3859
  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the Trending theme before 0.2 for WordPress allows remote attackers to inject arbitrary web script or HTML via the cpage parameter.

- Vulnerability: CVE-2011-3858
  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the Pixiv Custom theme before 2.1.6 for WordPress allows remote attackers to inject arbitrary web script or HTML via the s parameter.

- Vulnerability: CVE-2010-4402
  - CVSS Score: 4.3
  - Description: Multiple cross-site scripting (XSS) vulnerabilities in wp-login.php in the Register Plus plugin 3.5.1 and earlier for WordPress allow remote attackers to inject arbitrary web script or HTML via the (1) firstname, (2) lastname, (3) website, (4) aim, (5) yahoo, (6) jabber, (7) about, (8) pass1, and (9) pass2 parameters in a register action.

- Vulnerability: CVE-2010-4403
  - CVSS Score: 5
  - Description: The Register Plus plugin 3.5.1 and earlier for WordPress allows remote attackers to obtain sensitive information via a direct request to (1) dash_widget.php and (2) register-plus.php, which reveals the installation path in an error message.

- Vulnerability: CVE-2010-4747
  - CVSS Score: 4.3

- Description: Cross-site scripting (XSS) vulnerability in wordpress-processing-embed/data/p
  in the Processing Embed plugin 0.5 for WordPress allows remote
  attackers to inject arbitrary web script or HTML via the pluginurl
  parameter.

- Vulnerability: CVE-2023-2745

  - CVSS Score: N/A
  - Description: WordPress Core is vulnerable to Directory Traversal in versions up
    to, and including, 6.2, via the wp_lang parameter. This allows
    unauthenticated attackers to access and load arbitrary translation
    files. In cases where an attacker is able to upload a crafted
    translation file onto the site, such as via an upload form, this
    could be also used to perform a Cross-Site Scripting attack.

- Vulnerability: CVE-2022-43497

  - CVSS Score: N/A
  - Description: Cross-site scripting vulnerability in WordPress versions prior to
    6.0.3 allows a remote unauthenticated attacker to inject an arbitrary
    script. The developer also provides new patched releases for all
    versions since 3.7.

- Vulnerability: CVE-2012-2912

  - CVSS Score: 4.3
  - Description: Multiple cross-site scripting (XSS) vulnerabilities in the
    LeagueManager plugin 3.7 for WordPress allow remote attackers to
    inject arbitrary web script or HTML via the (1) group parameter in
    the show-league page or (2) season parameter in the team page to
    wp-admin/admin.php.

- Vulnerability: CVE-2012-2913

  - CVSS Score: 4.3
  - Description: Multiple cross-site scripting (XSS) vulnerabilities in the Leaflet
    plugin 0.0.1 for WordPress allow remote attackers to inject arbitrary
    web script or HTML via the id parameter to (1) leaflet_layer.php or
    (2) leaflet_marker.php, as reachable through wp-admin/admin.php.

- Vulnerability: CVE-2012-2916

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in sabre_class_admin.php in
    the SABRE plugin before 2.1 for WordPress allows remote attackers to
    inject arbitrary web script or HTML via the active_option parameter
    to wp-admin/tools.php.

- Vulnerability: CVE-2012-2917

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the Share and Follow
    plugin 1.80.3 for WordPress allows remote attackers to inject
    arbitrary web script or HTML via the CDN API Key (cnd-key) in a
    share-and-follow-menu page to wp-admin/admin.php.

- Vulnerability: CVE-2016-8743

  - CVSS Score: 5

- Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

- **Vulnerability:** CVE-2010-4875

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in vodpod-video-gallery/vodpod_galler in the Vodpod Video Gallery Plugin 3.1.5 for WordPress allows remote attackers to inject arbitrary web script or HTML via the gid parameter.

- **Vulnerability:** CVE-2011-5051

  - CVSS Score: 7.5
  - Description: Multiple unrestricted file upload vulnerabilities in the WP Symposium plugin before 11.12.24 for WordPress allow remote attackers to execute arbitrary code by uploading a file with an executable extension using (1) uploadify/upload_admin_avatar.php or (2) uploadify/upload_profile_avatar.php, then accessing it via a direct request to the file in an unspecified directory inside the webroot.

- **Vulnerability:** CVE-2021-26690

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service

- **Vulnerability:** CVE-2021-26691

  - CVSS Score: 7.5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow

- **Vulnerability:** CVE-2019-0220

  - CVSS Score: 5
  - Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.

- **Vulnerability:** CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- **Vulnerability:** CVE-2018-20148

  - CVSS Score: 7.5

- Description: In WordPress before 4.9.9 and 5.x before 5.0.1, contributors could conduct PHP object injection attacks via crafted metadata in a wp.getMediaItem XMLRPC call. This is caused by mishandling of serialized data at phar:// URLs in the wp_get_attachment_thumb_file function in wp-includes/post.php.

- Vulnerability: CVE-2018-20149

  - CVSS Score: 3.5
  - Description: In WordPress before 4.9.9 and 5.x before 5.0.1, when the Apache HTTP Server is used, authors could upload crafted files that bypass intended MIME type restrictions, leading to XSS, as demonstrated by a .jpg file without JPEG data.

- Vulnerability: CVE-2024-38477

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2010-1186

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in xml/media-rss.php in the NextGEN Gallery plugin before 1.5.2 for WordPress allows remote attackers to inject arbitrary web script or HTML via the mode parameter.

- Vulnerability: CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2018-20147

  - CVSS Score: 5.5
  - Description: In WordPress before 4.9.9 and 5.x before 5.0.1, authors could modify metadata to bypass intended restrictions on deleting files.

- Vulnerability: CVE-2021-39275

  - CVSS Score: 7.5
  - Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2020-28039

  - CVSS Score: 6.4
  - Description: is_protected_meta in wp-includes/meta.php in WordPress before 5.5.2 allows arbitrary file deletion because it does not properly determine whether a meta key is considered protected.

- Vulnerability: CVE-2020-28038

  - CVSS Score: 4.3
  - Description: WordPress before 5.5.2 allows stored XSS via post slugs.

- Vulnerability: CVE-2010-4518

- CVSS Score: 4.3
- Description: Cross-site scripting (XSS) vulnerability in wp-safe-search/wp-safe-search-jx.
  in the Safe Search plugin 0.7 for WordPress allows remote attackers
  to inject arbitrary web script or HTML via the v1 parameter.

• Vulnerability: CVE-2020-28033

  - CVSS Score: 5
  - Description: WordPress before 5.5.2 mishandles embeds from disabled sites on a
    multisite network, as demonstrated by allowing a spam embed.

• Vulnerability: CVE-2020-28032

  - CVSS Score: 7.5
  - Description: WordPress before 5.5.2 mishandles deserialization requests in
    wp-includes/Requests/Utility/FilteredIterator.php.

• Vulnerability: CVE-2020-28037

  - CVSS Score: 7.5
  - Description: is_blog_installed in wp-includes/functions.php in WordPress before
    5.5.2 improperly determines whether WordPress is already installed,
    which might allow an attacker to perform a new installation, leading
    to remote code execution (as well as a denial of service for the old
    installation).

• Vulnerability: CVE-2020-28036

  - CVSS Score: 7.5
  - Description: wp-includes/class-wp-xmlrpc-server.php in WordPress before 5.5.2
    allows attackers to gain privileges by using XML-RPC to comment on a
    post.

• Vulnerability: CVE-2020-28035

  - CVSS Score: 7.5
  - Description: WordPress before 5.5.2 allows attackers to gain privileges via
    XML-RPC.

• Vulnerability: CVE-2020-28034

  - CVSS Score: 4.3
  - Description: WordPress before 5.5.2 allows XSS associated with global variables.

• Vulnerability: CVE-2008-5752

  - CVSS Score: 4.3
  - Description: Directory traversal vulnerability in getConfig.php in the Page
    Flip Image Gallery plugin 0.2.2 and earlier for WordPress, when
    magic_quotes_gpc is disabled, allows remote attackers to read
    arbitrary files via a .. (dot dot) in the book_id parameter. NOTE:
    some of these details are obtained from third party information.

• Vulnerability: CVE-2022-31813

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-*
    headers to the origin server based on client side Connection
    header hop-by-hop mechanism. This may be used to bypass IP based
    authentication on the origin server/application.

• Vulnerability: CVE-2022-29404

  - CVSS Score: 5

– Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2022-22721

  – CVSS Score: 5.8
  – Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2022-22720

  – CVSS Score: 7.5
  – Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2017-15710

  – CVSS Score: 5
  – Description: In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.

- Vulnerability: CVE-2012-1010

  – CVSS Score: 7.5
  – Description: Unrestricted file upload vulnerability in actions.php in the AllWebMenus plugin before 1.1.8 for WordPress allows remote attackers to execute arbitrary PHP code by uploading a ZIP file containing a PHP file, then accessing it via a direct request to the file in an unspecified directory.

- Vulnerability: CVE-2012-1011

  – CVSS Score: 7.5
  – Description: actions.php in the AllWebMenus plugin 1.1.8 for WordPress allows remote attackers to bypass intended access restrictions to upload and execute arbitrary PHP code by setting the HTTP_REFERER to a certain value, then uploading a ZIP file containing a PHP file, then accessing it via a direct request to the file in an unspecified directory.

- Vulnerability: CVE-2018-12895

  – CVSS Score: 6.5

– Description: WordPress through 4.9.6 allows Author users to execute arbitrary
code by leveraging directory traversal in the wp-admin/post.php
thumb parameter, which is passed to the PHP unlink function and can
delete the wp-config.php file. This is related to missing filename
validation in the wp-includes/post.php wp_delete_attachment function.
The attacker must have capabilities for files and posts that are
normally available only to the Author, Editor, and Administrator
roles. The attack methodology is to delete wp-config.php and
then launch a new installation process to increase the attacker's
privileges.

- Vulnerability: CVE-2021-44224

  – CVSS Score: 6.4
  – Description: A crafted URI sent to httpd configured as a forward proxy
(ProxyRequests on) can cause a crash (NULL pointer dereference) or,
for configurations mixing forward and reverse proxy declarations, can
allow for requests to be directed to a declared Unix Domain Socket
endpoint (Server Side Request Forgery). This issue affects Apache
HTTP Server 2.4.7 up to 2.4.51 (included).

- Vulnerability: CVE-2021-44223

  – CVSS Score: 7.5
  – Description: WordPress before 5.8 lacks support for the Update URI plugin header.
This makes it easier for remote attackers to execute arbitrary code
via a supply-chain attack against WordPress installations that use
any plugin for which the slug satisfies the naming constraints of
the WordPress.org Plugin Directory but is not yet present in that
directory.

- Vulnerability: CVE-2006-20001

  – CVSS Score: N/A
  – Description: A carefully crafted If: request header can cause a memory read, or
write of a single zero byte, in a pool (heap) memory location beyond
the header value sent. This could cause the process to crash.This
issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2019-10092

  – CVSS Score: 4.3
  – Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting
issue was reported affecting the mod_proxy error page. An attacker
could cause the link on the error page to be malformed and instead
point to a page of their choice. This would only be exploitable
where a server was set up with proxying enabled but was misconfigured
in such a way that the Proxy Error page was displayed.

- Vulnerability: CVE-2017-7679

  – CVSS Score: 7.5
  – Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime
can read one byte past the end of a buffer when sending a malicious
Content-Type response header.

- Vulnerability: CVE-2019-20042

  – CVSS Score: 4.3
  – Description: In wp-includes/formatting.php in WordPress 3.7 to 5.3.0, the function
wp_targeted_link_rel() can be used in a particular way to result in
a stored cross-site scripting (XSS) vulnerability. This has been
patched in WordPress 5.3.1, along with all the previous WordPress
versions from 3.7 to 5.3 via a minor release.

- Vulnerability: CVE-2019-20043
  - CVSS Score: 5
  - Description: In in wp-includes/rest-api/endpoints/class-wp-rest-posts-controller.php in WordPress 3.7 to 5.3.0, authenticated users who do not have the rights to publish a post are able to mark posts as sticky or unsticky via the REST API. For example, the contributor role does not have such rights, but this allowed them to bypass that. This has been patched in WordPress 5.3.1, along with all the previous WordPress versions from 3.7 to 5.3 via a minor release.
- Vulnerability: CVE-2019-20041
  - CVSS Score: 7.5
  - Description: wp_kses_bad_protocol in wp-includes/kses.php in WordPress before 5.3.1 mishandles the HTML5 colon named entity, allowing attackers to bypass input sanitization, as demonstrated by the javascript: substring.
- Vulnerability: CVE-2018-20151
  - CVSS Score: 5
  - Description: In WordPress before 4.9.9 and 5.x before 5.0.1, the user-activation page could be read by a search engine's web crawler if an unusual configuration were chosen. The search engine could then index and display a user's e-mail address and (rarely) the password that was generated by default.
- Vulnerability: CVE-2018-20150
  - CVSS Score: 4.3
  - Description: In WordPress before 4.9.9 and 5.x before 5.0.1, crafted URLs could trigger XSS for certain use cases involving plugins.
- Vulnerability: CVE-2018-20153
  - CVSS Score: 3.5
  - Description: In WordPress before 4.9.9 and 5.x before 5.0.1, contributors could modify new comments made by users with greater privileges, possibly causing XSS.
- Vulnerability: CVE-2018-20152
  - CVSS Score: 4
  - Description: In WordPress before 4.9.9 and 5.x before 5.0.1, authors could bypass intended restrictions on post types via crafted input.
- Vulnerability: CVE-2009-4169
  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in wp-cumulus.php in the WP-Cumulus Plug-in before 1.22 for WordPress allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
- Vulnerability: CVE-2009-4168
  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in Roy Tanck tagcloud.swf, as used in the WP-Cumulus plugin before 1.23 for WordPress and the Joomulus module 2.0 and earlier for Joomla!, allows remote attackers to inject arbitrary web script or HTML via the tagcloud parameter in a tags action. Cross-site scripting (XSS) vulnerability in tagcloud.swf in the WP-Cumulus Plug-in before 1.23 for WordPress allows remote attackers to inject arbitrary web script or HTML via the tagcloud parameter.

757

- Vulnerability: CVE-2009-4672

  – CVSS Score: 7.5
  – Description: Directory traversal vulnerability in main.php in the WP-Lytebox plugin 1.3 for WordPress allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the pg parameter.

- Vulnerability: CVE-2011-4568

  – CVSS Score: 4.3
  – Description: Cross-site scripting (XSS) vulnerability in view/frontend-head.php in the Flowplayer plugin before 1.2.12 for WordPress allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2011-4671

  – CVSS Score: 7.5
  – Description: SQL injection vulnerability in adrotate/adrotate-out.php in the AdRotate plugin 3.6.6, and other versions before 3.6.8, for WordPress allows remote attackers to execute arbitrary SQL commands via the track parameter (aka redirect URL).

- Vulnerability: CVE-2011-1176

  – CVSS Score: 4.3
  – Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2011-4673

  – CVSS Score: 7.5
  – Description: SQL injection vulnerability in modules/sharedaddy.php in the Jetpack plugin for WordPress allows remote attackers to execute arbitrary SQL commands via the id parameter.

- Vulnerability: CVE-2018-10101

  – CVSS Score: 5.8
  – Description: Before WordPress 4.9.5, the URL validator assumed URLs with the hostname localhost were on the same host as the WordPress server.

- Vulnerability: CVE-2018-10100

  – CVSS Score: 5.8
  – Description: Before WordPress 4.9.5, the redirection URL for the login page was not validated or sanitized if forced to use HTTPS.

- Vulnerability: CVE-2018-10102

  – CVSS Score: 4.3
  – Description: Before WordPress 4.9.5, the version string was not escaped in the get_the_generator function, and could lead to XSS in a generator tag.

- Vulnerability: CVE-2008-6811

  – CVSS Score: 6.8

- Description: Unrestricted file upload vulnerability in image_processing.php in the e-Commerce Plugin 3.4 and earlier for Wordpress allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in wp-content/plugins/wp-shopping-cart/.

- Vulnerability: CVE-2011-4562

  - CVSS Score: 4.3
  - Description: Multiple cross-site scripting (XSS) vulnerabilities in (1) view/admin/log_item.php and (2) view/admin/log_item_details.php in the Redirection plugin 2.2.9 for WordPress allow remote attackers to inject arbitrary web script or HTML via the Referer HTTP header in a request to a post that does not exist.

- Vulnerability: CVE-2010-4630

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in pages/admin/surveys/create.php in the WP Survey And Quiz Tool plugin 1.2.1 for WordPress allows remote attackers to inject arbitrary web script or HTML via the action parameter.

- Vulnerability: CVE-2010-4637

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in feedlist/handler_image.php in the FeedList plugin 2.61.01 for WordPress allows remote attackers to inject arbitrary web script or HTML via the i parameter.

- Vulnerability: CVE-2011-0760

  - CVSS Score: 4.3
  - Description: Multiple cross-site request forgery (CSRF) vulnerabilities in the configuration screen in wp-relatedposts.php in the WP Related Posts plugin 1.0 for WordPress allow remote attackers to hijack the authentication of administrators for requests that insert cross-site scripting (XSS) sequences via the (1) wp_relatedposts_title, (2) wp_relatedposts_num, or (3) wp_relatedposts_type parameter.

- Vulnerability: CVE-2012-1786

  - CVSS Score: 5
  - Description: The Media Upload form in the Video Embed & Thumbnail Generator plugin before 2.0 for WordPress allows remote attackers to obtain the installation path via unknown vectors.

- Vulnerability: CVE-2019-9787

  - CVSS Score: 6.8
  - Description: WordPress before 5.1.1 does not properly filter comment content, leading to Remote Code Execution by unauthenticated users in a default configuration. This occurs because CSRF protection is mishandled, and because Search Engine Optimization of A elements is performed incorrectly, leading to XSS. The XSS results in administrative access, which allows arbitrary changes to .php files. This is related to wp-admin/includes/ajax-actions.php and wp-includes/comment.php.

- Vulnerability: CVE-2018-1302

  - CVSS Score: 4.3

- Description: When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.

- Vulnerability: CVE-2012-1785

  - CVSS Score: 7.5
  - Description: kg_callffmpeg.php in the Video Embed & Thumbnail Generator plugin before 2.0 for WordPress allows remote attackers to execute arbitrary commands via unspecified vectors.

- Vulnerability: CVE-2022-36760

  - CVSS Score: N/A
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2023-25690

  - CVSS Score: N/A
  - Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2010-4779

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in lib/includes/auth.inc.php in the WPtouch plugin 1.9.19.4 and 1.9.20 for WordPress allows remote attackers to inject arbitrary web script or HTML via the wptouch_settings parameter to include/adsense-new.php. NOTE: some of these details are obtained from third party information.

- Vulnerability: CVE-2019-10098

  - CVSS Score: 5.8
  - Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.

- Vulnerability: CVE-2020-28040

  - CVSS Score: 4.3
  - Description: WordPress before 5.5.2 allows CSRF attacks that change a theme's background image.

- Vulnerability: CVE-2011-3864

  − CVSS Score: 4.3
  − Description: Cross-site scripting (XSS) vulnerability in the The Erudite theme
                before 2.7.9 for WordPress allows remote attackers to inject
                arbitrary web script or HTML via the cpage parameter.

- Vulnerability: CVE-2011-3865

  − CVSS Score: 4.3
  − Description: Cross-site scripting (XSS) vulnerability in the Black-LetterHead
                theme before 1.6 for WordPress allows remote attackers to inject
                arbitrary web script or HTML via the PATH_INFO to index.php.

- Vulnerability: CVE-2022-26377

  − CVSS Score: 5
  − Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request
                Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server
                allows an attacker to smuggle requests to the AJP server it forwards
                requests to. This issue affects Apache HTTP Server Apache HTTP
                Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2011-3860

  − CVSS Score: 4.3
  − Description: Cross-site scripting (XSS) vulnerability in the Cover WP theme before
                1.6.6 for WordPress allows remote attackers to inject arbitrary web
                script or HTML via the s parameter.

- Vulnerability: CVE-2011-3861

  − CVSS Score: 4.3
  − Description: Cross-site scripting (XSS) vulnerability in the Web Minimalist 200901
                theme before 1.2 for WordPress allows remote attackers to inject
                arbitrary web script or HTML via the PATH_INFO to index.php.

- Vulnerability: CVE-2011-3862

  − CVSS Score: 4.3
  − Description: Cross-site scripting (XSS) vulnerability in the Morning Coffee theme
                before 3.6 for WordPress allows remote attackers to inject arbitrary
                web script or HTML via the PATH_INFO to index.php.

- Vulnerability: CVE-2011-3863

  − CVSS Score: 4.3
  − Description: Cross-site scripting (XSS) vulnerability in the RedLine theme before
                1.66 for WordPress allows remote attackers to inject arbitrary web
                script or HTML via the s parameter.

- Vulnerability: CVE-2020-26596

  − CVSS Score: 9
  − Description: The Dynamic OOO widget for the Elementor Pro plugin through 3.0.5
                for WordPress allows remote authenticated users to execute arbitrary
                code because only the Editor role is needed to upload executable PHP
                code via the PHP Raw snippet. NOTE: this issue can be mitigated by
                removing the Dynamic OOO widget or by restricting availability of the
                Editor role.

- Vulnerability: CVE-2022-30556

  − CVSS Score: 5

– Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- Vulnerability: CVE-2019-16223

  – CVSS Score: 3.5
  – Description: WordPress before 5.2.3 allows XSS in post previews by authenticated users.

- Vulnerability: CVE-2019-16222

  – CVSS Score: 4.3
  – Description: WordPress before 5.2.3 has an issue with URL sanitization in wp_kses_bad_protocol_once in wp-includes/kses.php that can lead to cross-site scripting (XSS) attacks.

- Vulnerability: CVE-2019-16221

  – CVSS Score: 4.3
  – Description: WordPress before 5.2.3 allows reflected XSS in the dashboard.

- Vulnerability: CVE-2019-16220

  – CVSS Score: 5.8
  – Description: In WordPress before 5.2.3, validation and sanitization of a URL in wp_validate_redirect in wp-includes/pluggable.php could lead to an open redirect if a provided URL path does not start with a forward slash.

- Vulnerability: CVE-2019-16780

  – CVSS Score: 3.5
  – Description: WordPress users with lower privileges (like contributors) can inject JavaScript code in the block editor using a specific payload, which is executed within the dashboard. This can lead to XSS if an admin opens the post in the editor. Execution of this attack does require an authenticated user. This has been patched in WordPress 5.3.1, along with all the previous WordPress versions from 3.7 to 5.3 via a minor release. Automatic updates are enabled by default for minor releases and we strongly recommend that you keep them enabled.

- Vulnerability: CVE-2019-16781

  – CVSS Score: 3.5
  – Description: In WordPress before 5.3.1, authenticated users with lower privileges (like contributors) can inject JavaScript code in the block editor, which is executed within the dashboard. It can lead to an admin opening the affected post in the editor leading to XSS.

- Vulnerability: CVE-2020-11023

  – CVSS Score: 4.3
  – Description: In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources – even after sanitizing it – to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

- Vulnerability: CVE-2021-40438

  – CVSS Score: 6.8

– Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server chosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

• Vulnerability: CVE-2011-0759

  – CVSS Score: 6.8
  – Description: Multiple cross-site request forgery (CSRF) vulnerabilities in the configuration page in the Recaptcha (aka WP-reCAPTCHA) plugin 2.9.8.2 for WordPress allow remote attackers to hijack the authentication of administrators for requests that disable the CAPTCHA requirement or insert cross-site scripting (XSS) sequences via the (1) recaptcha_opt_pubkey, (2) recaptcha_opt_privkey, (3) re_tabindex, (4) error_blank, (5) error_incorrect, (6) mailhide_pub, (7) mailhide_priv, (8) mh_replace_link, or (9) mh_replace_title parameter.

• Vulnerability: CVE-2020-11985

  – CVSS Score: 4.3
  – Description: IP address spoofing when proxying using mod_remoteip and mod_rewrite For configurations using proxying with mod_remoteip and certain mod_rewrite rules, an attacker could spoof their IP address for logging and PHP scripts. Note this issue was fixed in Apache HTTP Server 2.4.24 but was retrospectively allocated a low severity CVE in 2020.

• Vulnerability: CVE-2008-4732

  – CVSS Score: 7.5
  – Description: SQL injection vulnerability in ajax_comments.php in the WP Comment Remix plugin before 1.4.4 for WordPress allows remote attackers to execute arbitrary SQL commands via the p parameter.

• Vulnerability: CVE-2022-28614

  – CVSS Score: 5
  – Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

• Vulnerability: CVE-2013-5918

  – CVSS Score: 4.3
  – Description: Cross-site scripting (XSS) vulnerability in platinum_seo_pack.php in the Platinum SEO plugin before 1.3.8 for WordPress allows remote attackers to inject arbitrary web script or HTML via the s parameter.

• Vulnerability: CVE-2023-5561

  – CVSS Score: N/A
  – Description: WordPress does not properly restrict which user fields are searchable via the REST API, allowing unauthenticated attackers to discern the email addresses of users who have published public posts on an affected website via an Oracle style attack

• Vulnerability: CVE-2023-45802

  – CVSS Score: N/A

– Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a
time window were the request's memory resources were not reclaimed
immediately. Instead, de-allocation was deferred to connection
close. A client could send new requests and resets, keeping the
connection busy and open and causing the memory footprint to keep
on growing. On connection close, all resources were reclaimed, but
the process might run out of memory before that.This was found by
the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset
Exploit) with their own test client. During "normal" HTTP/2 use, the
probability to hit this bug is very low. The kept memory would not
become noticeable before the connection closes or times out.Users are
recommended to upgrade to version 2.4.58, which fixes the issue.

• Vulnerability: CVE-2016-8740

– CVSS Score: 5

– Description: The mod_http2 module in the Apache HTTP Server 2.4.17 through
2.4.23, when the Protocols configuration includes h2 or h2c, does
not restrict request-header length, which allows remote attackers
to cause a denial of service (memory consumption) via crafted
CONTINUATION frames in an HTTP/2 request.

• Vulnerability: CVE-2010-0673

– CVSS Score: 7.5

– Description: SQL injection vulnerability in cplphoto.php in the Copperleaf
Photolog plugin 0.16, and possibly earlier, for WordPress allows
remote attackers to execute arbitrary SQL commands via the postid
parameter.

• Vulnerability: CVE-2017-9798

– CVSS Score: 5

– Description: Apache httpd allows remote attackers to read secret data from process
memory if the Limit directive can be set in a user's .htaccess file,
or if httpd.conf has certain misconfigurations, aka Optionsbleed.
This affects the Apache HTTP Server through 2.2.34 and 2.4.x through
2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request
when attempting to read secret data. This is a use-after-free
issue and thus secret data is not always sent, and the specific data
depends on many factors including configuration. Exploitation with
.htaccess can be blocked with a patch to the ap_limit_section function
in server/core.c.

• Vulnerability: CVE-2012-6708

– CVSS Score: 4.3

– Description: jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS)
attacks. The jQuery(strInput) function does not differentiate
selectors from HTML in a reliable fashion. In vulnerable versions,
jQuery determined whether the input was HTML by looking for the '<'
character anywhere in the string, giving attackers more flexibility
when attempting to construct a malicious payload. In fixed versions,
jQuery only deems the input to be HTML if it explicitly starts with
the '<' character, limiting exploitability only to attackers who can
control the beginning of a string, which is far less common.

• Vulnerability: CVE-2012-3526

– CVSS Score: 5

– Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the
Apache HTTP Server allows remote attackers to cause a denial of
service (server or application crash) via multiple X-Forwarded-For
headers in a request.

- Vulnerability: CVE-2008-1982

  – CVSS Score: 7.5
  – Description: SQL injection vulnerability in ss_load.php in the Spreadsheet (wpSS)
  0.6 and earlier plugin for WordPress allows remote attackers to
  execute arbitrary SQL commands via the ss_id parameter.

- Vulnerability: CVE-2018-19296

  – CVSS Score: 6.8
  – Description: PHPMailer before 5.2.27 and 6.x before 6.0.6 is vulnerable to an
  object injection attack.

- Vulnerability: CVE-2016-8612

  – CVSS Score: 3.3
  – Description: Apache HTTP Server mod_cluster before version httpd 2.4.23 is
  vulnerable to an Improper Input Validation in the protocol parsing
  logic in the load balancer resulting in a Segmentation Fault in the
  serving httpd process.

- Vulnerability: CVE-2011-1669

  – CVSS Score: 5
  – Description: Directory traversal vulnerability in wp-download.php in the WP Custom
  Pages module 0.5.0.1 for WordPress allows remote attackers to read
  arbitrary files via ..%2F (encoded dot dot) sequences in the url
  parameter.

- Vulnerability: CVE-2009-2299

  – CVSS Score: 5
  – Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module
  before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before
  3.1.1-11637, a module for the Apache HTTP Server, allows remote
  attackers to cause a denial of service (memory consumption) via an
  HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2007-2627

  – CVSS Score: 6.8
  – Description: Cross-site scripting (XSS) vulnerability in sidebar.php in WordPress,
  when custom 404 pages that call get_sidebar are used, allows remote
  attackers to inject arbitrary web script or HTML via the query string
  (PHP_SELF), a different vulnerability than CVE-2007-1622.

- Vulnerability: CVE-2010-4277

  – CVSS Score: 4.3
  – Description: Cross-site scripting (XSS) vulnerability in lembedded-video.php in
  the Embedded Video plugin 4.1 for WordPress allows remote attackers
  to inject arbitrary web script or HTML via the content parameter to
  wp-admin/post.php.

- Vulnerability: CVE-2007-5800

  – CVSS Score: 6.8

- Description: Multiple PHP remote file inclusion vulnerabilities in the BackUpWordPress 0.4.2b and earlier plugin for WordPress allow remote attackers to execute arbitrary PHP code via a URL in the bkpwp_plugin_path parameter to (1) plugins/BackUp/Archive.php; and (2) Predicate.php, (3) Writer.php, (4) Reader.php, and other unspecified scripts under plugins/BackUp/Archive/.

- Vulnerability: CVE-2012-4360

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2010-2924

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in myLDlinker.php in the myLinksDump Plugin 1.2 for WordPress allows remote attackers to execute arbitrary SQL commands via the url parameter. NOTE: some of these details are obtained from third party information.

- Vulnerability: CVE-2012-4001

  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2019-8942

  - CVSS Score: 6.5
  - Description: WordPress before 4.9.9 and 5.x before 5.0.1 allows remote code execution because an _wp_attached_file Post Meta entry can be changed to an arbitrary string, such as one ending with a .jpg?file.php substring. An attacker with author privileges can execute arbitrary code by uploading a crafted image containing PHP code in the Exif metadata. Exploitation can leverage CVE-2019-8943.

- Vulnerability: CVE-2019-8943

  - CVSS Score: 4
  - Description: WordPress through 5.0.3 allows Path Traversal in wp_crop_image(). An attacker (who has privileges to crop an image) can write the output image to an arbitrary directory via a filename containing two image extensions and ../ sequences, such as a filename ending with the .jpg?/../../file.jpg substring.

- Vulnerability: CVE-2022-37436

  - CVSS Score: N/A
  - Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2018-17199

  - CVSS Score: 5

- Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session
  checks the session expiry time before decoding the session. This
  causes session expiry time to be ignored for mod_session_cookie
  sessions since the expiry time is loaded when the session is decoded.

- Vulnerability: CVE-2015-9251

  - CVSS Score: 4.3
  - Description: jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS)
    attacks when a cross-domain Ajax request is performed without the
    dataType option, causing text/javascript responses to be executed.

- Vulnerability: CVE-2010-4839

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in the Event Registration plugin 5.32 and
    earlier for WordPress allows remote attackers to execute arbitrary
    SQL commands via the event_id parameter in a register action.

- Vulnerability: CVE-2011-0740

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in magpie/scripts/magpie_slashbox.php
    in RSS Feed Reader 0.1 for WordPress allows remote attackers to
    inject arbitrary web script or HTML via the rss_url parameter.

- Vulnerability: CVE-2019-17669

  - CVSS Score: 7.5
  - Description: WordPress before 5.2.4 has a Server Side Request Forgery (SSRF)
    vulnerability because URL validation does not consider the
    interpretation of a name as a series of hex characters.

- Vulnerability: CVE-2022-43504

  - CVSS Score: N/A
  - Description: Improper authentication vulnerability in WordPress versions prior to
    6.0.3 allows a remote unauthenticated attacker to obtain the email
    address of the user who posted a blog using the WordPress Post by
    Email Feature. The developer also provides new patched releases for
    all versions since 3.7.

- Vulnerability: CVE-2019-10082

  - CVSS Score: 6.4
  - Description: In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input,
    the http/2 session handling could be made to read memory after being
    freed, during connection shutdown.

- Vulnerability: CVE-2017-9788

  - CVSS Score: 6.4
  - Description: In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value
    placeholder in [Proxy-]Authorization headers of type 'Digest' was
    not initialized or reset before or between successive key=value
    assignments by mod_auth_digest. Providing an initial key with no
    '=' assignment could reflect the stale value of uninitialized pool
    memory used by the prior request, leading to leakage of potentially
    confidential information, and a segfault in other cases resulting in
    denial of service.

- Vulnerability: CVE-2022-43500

  - CVSS Score: N/A

- Description: Cross-site scripting vulnerability in WordPress versions prior to 6.0.3 allows a remote unauthenticated attacker to inject an arbitrary script. The developer also provides new patched releases for all versions since 3.7.

- Vulnerability: CVE-2012-1205

  - CVSS Score: 7.5
  - Description: PHP remote file inclusion vulnerability in relocate-upload.php in Relocate Upload plugin before 0.20 for WordPress allows remote attackers to execute arbitrary PHP code via a URL in the abspath parameter.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2022-21663

  - CVSS Score: 6.5
  - Description: WordPress is a free and open-source content management system written in PHP and paired with a MariaDB database. On a multisite, users with Super Admin role can bypass explicit/additional hardening under certain conditions through object injection. This has been patched in WordPress version 5.8.3. Older affected versions are also fixed via security release, that go back till 3.7.37. We strongly recommend that you keep auto-updates enabled. There are no known workarounds for this issue.

- Vulnerability: CVE-2022-21662

  - CVSS Score: 3.5
  - Description: WordPress is a free and open-source content management system written in PHP and paired with a MariaDB database. Low-privileged authenticated users (like author) in WordPress core are able to execute JavaScript/perform stored XSS attack, which can affect high-privileged users. This has been patched in WordPress version 5.8.3. Older affected versions are also fixed via security release, that go back till 3.7.37. We strongly recommend that you keep auto-updates enabled. There are no known workarounds for this issue.

- Vulnerability: CVE-2022-21661

  - CVSS Score: 5
  - Description: WordPress is a free and open-source content management system written in PHP and paired with a MariaDB database. Due to improper sanitization in WP_Query, there can be cases where SQL injection is possible through plugins or themes that use it in a certain way. This has been patched in WordPress version 5.8.3. Older affected versions are also fixed via security release, that go back till 3.7.37. We strongly recommend that you keep auto-updates enabled. There are no known workarounds for this vulnerability.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2009-2122

  – CVSS Score: 7.5
  – Description: SQL injection vulnerability in viewimg.php in the Paolo Palmonari Photoracer plugin 1.0 for WordPress allows remote attackers to execute arbitrary SQL commands via the id parameter.

- Vulnerability: CVE-2022-21664

  – CVSS Score: 6.5
  – Description: WordPress is a free and open-source content management system written in PHP and paired with a MariaDB database. Due to lack of proper sanitization in one of the classes, there's potential for unintended SQL queries to be executed. This has been patched in WordPress version 5.8.3. Older affected versions are also fixed via security release, that go back till 4.1.34. We strongly recommend that you keep auto-updates enabled. There are no known workarounds for this issue.

- Vulnerability: CVE-2013-0941

  – CVSS Score: 2.1
  – Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  – CVSS Score: 4.3
  – Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2017-15715

  – CVSS Score: 6.8
  – Description: In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.

- Vulnerability: CVE-2018-1301

  – CVSS Score: 4.3
  – Description: A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.

- Vulnerability: CVE-2024-27316

  – CVSS Score: N/A

- Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered
  in nghttp2 in order to generate an informative HTTP 413 response.
  If a client does not stop sending headers, this leads to memory
  exhaustion.

- **Vulnerability:** CVE-2019-11358

  - CVSS Score: 4.3
  - Description: jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other
    products, mishandles jQuery.extend(true, {}, ...) because of
    Object.prototype pollution. If an unsanitized source object
    contained an enumerable __proto__ property, it could extend the native
    Object.prototype.

- **Vulnerability:** CVE-2009-4170

  - CVSS Score: 5
  - Description: WP-Cumulus Plug-in 1.20 for WordPress, and possibly other versions,
    allows remote attackers to obtain sensitive information via a crafted
    request to wp-cumulus.php, probably without parameters, which reveals
    the installation path in an error message.

- **Vulnerability:** CVE-2011-4803

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in wptouch/ajax.php in the WPTouch
    plugin for WordPress allows remote attackers to execute arbitrary
    SQL commands via the id parameter.

- **Vulnerability:** CVE-2018-1283

  - CVSS Score: 3.5
  - Description: In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to
    forward its session data to CGI applications (SessionEnv on, not
    the default), a remote user may influence their content by using a
    "Session" header. This comes from the "HTTP_SESSION" variable name
    used by mod_session to forward its data to CGIs, since the prefix
    "HTTP_" is also used by the Apache HTTP Server to pass HTTP header
    fields, per CGI specifications.

- **Vulnerability:** CVE-2018-1303

  - CVSS Score: 5
  - Description: A specially crafted HTTP request header could have crashed the Apache
    HTTP Server prior to version 2.4.30 due to an out of bound read while
    preparing data to be cached in shared memory. It could be used as
    a Denial of Service attack against users of mod_cache_socache. The
    vulnerability is considered as low risk since mod_cache_socache is not
    widely used, mod_cache_disk is not concerned by this vulnerability.

- **Vulnerability:** CVE-2017-3167

  - CVSS Score: 7.5
  - Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use
    of the ap_get_basic_auth_pw() by third-party modules outside of the
    authentication phase may lead to authentication requirements being
    bypassed.

- **Vulnerability:** CVE-2022-28615

  - CVSS Score: 6.4

- Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- Vulnerability: CVE-2012-2759

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in login-with-ajax.php in the Login With Ajax (aka login-with-ajax) plugin before 3.0.4.1 for WordPress allows remote attackers to inject arbitrary web script or HTML via the callback parameter in a lostpassword action to wp-login.php.

11.15 IP Address: 159.149.53.164

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 2

- High Vulnerabilities: 16

- Medium Vulnerabilities: 63

- Low Vulnerabilities: 5

- Total Vulnerabilities: 86

Services Running on IP Address

- Service: Apache httpd

  – Port: 80
  – Version: 2.4.37
  – Location: https://bac.unimi.it/

- Service: Apache httpd

  – Port: 443
  – Version: 2.4.59
  – Location: /

Vulnerabilities Found

- Vulnerability: CVE-2019-0215

  – CVSS Score: 6
  – Description: In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in mod_ssl when using per-location client certificate verification with TLSv1.3 allowed a client to bypass configured access control restrictions.

- Vulnerability: CVE-2013-4365

  – CVSS Score: 7.5
  – Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2022-28330

  – CVSS Score: 5
  – Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2021-32791

  – CVSS Score: 4.3
  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2021-32792

  – CVSS Score: 4.3

  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.

- Vulnerability: CVE-2023-31122

  – CVSS Score: N/A

  – Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2024-38476

  – CVSS Score: N/A

  – Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-27316

  – CVSS Score: N/A

  – Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

- Vulnerability: CVE-2024-38474

  – CVSS Score: N/A

  – Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2009-0796

  – CVSS Score: 2.6

  – Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2022-2068

  – CVSS Score: 10

- Description: In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze).

- Vulnerability: CVE-2021-3449

  - CVSS Score: 4.3
  - Description: An OpenSSL TLS server may crash if sent a maliciously crafted renegotiation ClientHello message from a client. If a TLSv1.2 renegotiation ClientHello omits the signature_algorithms extension (where it was present in the initial ClientHello), but includes a signature_algorithms_cert extension then a NULL pointer dereference will result, leading to a crash and a denial of service attack. A server is only vulnerable if it has TLSv1.2 and renegotiation enabled (which is the default configuration). OpenSSL TLS clients are not impacted by this issue. All OpenSSL 1.1.1 versions are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1k. OpenSSL 1.0.2 is not impacted by this issue. Fixed in OpenSSL 1.1.1k (Affected 1.1.1-1.1.1j).

- Vulnerability: CVE-2021-36160

  - CVSS Score: 5
  - Description: A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS). This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48 (inclusive).

- Vulnerability: CVE-2020-1927

  - CVSS Score: 5.8
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.

- Vulnerability: CVE-2023-0286

  - CVSS Score: N/A

– Description: There is a type confusion vulnerability relating to X.400 address processinginside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING butthe public structure definition for GENERAL_NAME incorrectly specified the typeof the x400Address field as ASN1_TYPE. This field is subsequently interpreted bythe OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than anASN1_STRING.When CRL checking is enabled (i.e. the application sets theX509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to passarbitrary pointers to a memcmp call, enabling them to read memory contents orenact a denial of service. In most cases, the attack requires the attacker toprovide both the certificate chain and CRL, neither of which need to have avalid signature. If the attacker only controls one of these inputs, the otherinput must already contain an X.400 address as a CRL distribution point, whichis uncommon. As such, this vulnerability is most likely to only affectapplications which have implemented their own functionality for retrieving CRLsover a network.

- Vulnerability: CVE-2023-3817

  – CVSS Score: N/A

  – Description: Issue summary: Checking excessively long DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH key or DH parameters may experience longdelays. Where the key or parameters that are being checked have been obtainedfrom an untrusted source this may lead to a Denial of Service.The function DH_check() performs various checks on DH parameters. After fixingCVE-2023-3446 it was discovered that a large q parameter value can also triggeran overly long computation during some of these checks. A correct q value,if present, cannot be larger than the modulus p parameter, thus it isunnecessary to perform these checks if q is larger than p.An application that calls DH_check() and supplies a key or parameters obtainedfrom an untrusted source could be vulnerable to a Denial of Service attack.The function DH_check() is itself called by a number of other OpenSSL functions.An application calling any of those other functions may similarly be affected.The other functions affected by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable are the OpenSSL dhparam and pkeyparam command line applicationswhen using the "-check" option.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2021-32786

  – CVSS Score: 5.8

  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, `oidc_validate_redirect_url()` does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring `mod_auth_openidc` to only allow redirection whose destination matches a given regular expression.

- Vulnerability: CVE-2021-32785

    - CVSS Score: 4.3
    - Description: mod_auth_openidc is an authentication/authorization module for the
                    Apache 2.x HTTP server that functions as an OpenID Connect Relying
                    Party, authenticating users against an OpenID Connect Provider. When
                    mod_auth_openidc versions prior to 2.4.9 are configured to use an
                    unencrypted Redis cache (‘OIDCCacheEncrypt off‘, ‘OIDCSessionType
                    server-cache‘, ‘OIDCCacheType redis‘), ‘mod_auth_openidc‘ wrongly
                    performed argument interpolation before passing Redis requests to
                    ‘hiredis‘, which would perform it again and lead to an uncontrolled
                    format string bug. Initial assessment shows that this bug does
                    not appear to allow gaining arbitrary code execution, but can
                    reliably provoke a denial of service by repeatedly crashing the
                    Apache workers. This bug has been corrected in version 2.4.9 by
                    performing argument interpolation only once, using the ‘hiredis‘
                    API. As a workaround, this vulnerability can be mitigated by setting
                    ‘OIDCCacheEncrypt‘ to ‘on‘, as cache keys are cryptographically
                    hashed before use when this option is enabled.

- Vulnerability: CVE-2020-9490

    - CVSS Score: 5
    - Description: Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted
                    value for the 'Cache-Digest' header in a HTTP/2 request would result
                    in a crash when the server actually tries to HTTP/2 PUSH a resource
                    afterwards. Configuring the HTTP/2 feature via "H2Push off" will
                    mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2007-4723

    - CVSS Score: 7.5
    - Description: Directory traversal vulnerability in Ragnarok Online Control Panel
                    4.3.4a, when the Apache HTTP Server is used, allows remote attackers
                    to bypass authentication via directory traversal sequences in a URI
                    that ends with the name of a publicly available page, as demonstrated
                    by a "/...../" sequence and an account_manage.php/login.php final
                    component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2021-44790

    - CVSS Score: 7.5
    - Description: A carefully crafted request body can cause a buffer overflow in the
                    mod_lua multipart parser (r:parsebody() called from Lua scripts).
                    The Apache httpd team is not aware of an exploit for the vulnerabilty
                    though it might be possible to craft one. This issue affects Apache
                    HTTP Server 2.4.51 and earlier.

- Vulnerability: CVE-2020-13938

    - CVSS Score: 2.1
    - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users
                    can stop httpd on Windows

- Vulnerability: CVE-2023-2650

    - CVSS Score: N/A

– Description: Issue summary: Processing some specially crafted ASN.1 object identifiers ordata containing them may be very slow.Impact summary: Applications that use OBJ_obj2txt() directly, or use any ofthe OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no messagesize limit may experience notable to very long delays when processing thosemessages, which may lead to a Denial of Service.An OBJECT IDENTIFIER is composed of a series of numbers – sub-identifiers -most of which have no size limit. OBJ_obj2txt() may be used to translatean ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSLtype ASN1_OBJECT) to its canonical numeric text form, which are thesub-identifiers of the OBJECT IDENTIFIER in decimal form, separated byperiods.When one of the sub-identifiers in the OBJECT IDENTIFIER is very large(these are sizes that are seen as absurdly large, taking up tens or hundredsof KiBs), the translation to a decimal number in text may take a very longtime. The time complexity is $O(n^2)$ with 'n' being the size of thesub-identifiers in bytes (*).With OpenSSL 3.0, support to fetch cryptographic algorithms using names /identifiers in string form was introduced. This includes using OBJECTIDENTIFIERs in canonical numeric text form as identifiers for fetchingalgorithms.Such OBJECT IDENTIFIERs may be received through the ASN.1 structureAlgorithmIdentifier, which is commonly used in multiple protocols to specifywhat cryptographic algorithm should be used to sign or verify, encrypt ordecrypt, or digest passed data.Applications that call OBJ_obj2txt() directly with untrusted data areaffected, with any version of OpenSSL. If the use is for the mere purposeof display, the severity is considered low.In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME,CMS, CMP/CRMF or TS. It also impacts anything that processes X.509certificates, including simple things like verifying its signature.The impact on TLS is relatively low, because all versions of OpenSSL have a100KiB limit on the peer's certificate chain. Additionally, this onlyimpacts clients, or servers that have explicitly enabled clientauthentication.In OpenSSL 1.1.1 and 1.0.2, this only affects displaying diverse objects,such as X.509 certificates. This is assumed to not happen in such a waythat it would cause a Denial of Service, so these versions are considerednot affected by this issue in such a way that it would be cause for concern,and the severity is therefore considered low.

- Vulnerability: CVE-2023-0215

– CVSS Score: N/A

- Description: The public API function BIO_new_NDEF is a helper function used for streamingASN.1 data via a BIO. It is primarily used internally to OpenSSL to support theSMIME, CMS and PKCS7 streaming capabilities, but may also be called directly byend user applications.The function receives a BIO from the caller, prepends a new BIO_f_asn1 filterBIO onto the front of it to form a BIO chain, and then returns the new head ofthe BIO chain to the caller. Under certain conditions, for example if a CMSrecipient public key is invalid, the new filter BIO is freed and the functionreturns a NULL result indicating a failure. However, in this case, the BIO chainis not properly cleaned up and the BIO passed by the caller still retainsinternal pointers to the previously freed filter BIO. If the caller then goes onto call BIO_pop() on the BIO then a use-after-free will occur. This will mostlikely result in a crash.This scenario occurs directly in the internal function B64_write_ASN1() whichmay cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() onthe BIO. This internal function is in turn called by the public API functionsPEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream,SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7.Other public API functions that may be impacted by this includei2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream andi2d_PKCS7_bio_stream.The OpenSSL cms and smime command line applications are similarly affected.

- Vulnerability: CVE-2020-35452

  - CVSS Score: 6.8
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

- Vulnerability: CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2020-1934

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

- Vulnerability: CVE-2022-36760

  - CVSS Score: N/A
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-4304

  - CVSS Score: N/A

- Description: A timing based side channel exists in the OpenSSL RSA Decryption
  implementationwhich could be sufficient to recover a plaintext
  across a network in aBleichenbacher style attack. To achieve a
  successful decryption an attackerwould have to be able to send a
  very large number of trial messages fordecryption. The vulnerability
  affects all RSA padding modes: PKCS#1 v1.5,RSA-OEAP and RSASVE.For
  example, in a TLS connection, RSA is commonly used by a client to
  send anencrypted pre-master secret to the server. An attacker that
  had observed agenuine connection between a client and a server could
  use this flaw to sendtrial messages to the server and record the time
  taken to process them. After asufficiently large number of messages
  the attacker could recover the pre-mastersecret used for the original
  connection and thus be able to decrypt theapplication data sent over
  that connection.

- Vulnerability: CVE-2019-9517

  - CVSS Score: 7.8
  - Description: Some HTTP/2 implementations are vulnerable to unconstrained interal
    data buffering, potentially leading to a denial of service. The
    attacker opens the HTTP/2 window so the peer can send without
    constraint; however, they leave the TCP window closed so the
    peer cannot actually write (many of) the bytes on the wire. The
    attacker then sends a stream of requests for a large response object.
    Depending on how the servers queue the responses, this can consume
    excess memory, CPU, or both.

- Vulnerability: CVE-2019-0217

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition
    in mod_auth_digest when running in a threaded server could allow a
    user with valid credentials to authenticate using another username,
    bypassing configured access control restrictions.

- Vulnerability: CVE-2019-0197

  - CVSS Score: 4.9
  - Description: A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38.
    When HTTP/2 was enabled for a http: host or H2Upgrade was enabled
    for h2 on a https: host, an Upgrade request from http/1.1 to
    http/2 that was not the first request on a connection could lead
    to a misconfiguration and crash. Server that never enabled the
    h2 protocol or that only enabled it for https: and did not set
    "H2Upgrade on" are unaffected by this issue.

- Vulnerability: CVE-2019-0196

  - CVSS Score: 5
  - Description: A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38.
    Using fuzzed network input, the http/2 request handling could be
    made to access freed memory in string comparison when determining the
    method of a request and thus process the request incorrectly.

- Vulnerability: CVE-2019-0190

  - CVSS Score: 5
  - Description: A bug exists in the way mod_ssl handled client renegotiations. A
    remote attacker could send a carefully crafted request that would
    cause mod_ssl to enter a loop leading to a denial of service. This
    bug can be only triggered with Apache HTTP Server version 2.4.37
    when using OpenSSL version 1.1.1 or later, due to an interaction in
    changes to handling of renegotiation attempts.

779

- Vulnerability: CVE-2021-33193

  – CVSS Score: 5
  – Description: A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.

- Vulnerability: CVE-2019-0211

  – CVSS Score: 7.2
  – Description: In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.

- Vulnerability: CVE-2019-17567

  – CVSS Score: 5
  – Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

- Vulnerability: CVE-2022-31813

  – CVSS Score: 7.5
  – Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

- Vulnerability: CVE-2012-4360

  – CVSS Score: 4.3
  – Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2023-4807

  – CVSS Score: N/A

- Description: Issue summary: The POLY1305 MAC (message authentication code) implementationcontains a bug that might corrupt the internal state of applications on theWindows 64 platform when running on newer X86_64 processors supporting theAVX512-IFMA instructions.Impact summary: If in an application that uses the OpenSSL library an attackercan influence whether the POLY1305 MAC algorithm is used, the applicationstate might be corrupted with various application dependent consequences.The POLY1305 MAC (message authentication code) implementation in OpenSSL doesnot save the contents of non-volatile XMM registers on Windows 64 platformwhen calculating the MAC of data larger than 64 bytes. Before returning tothe caller all the XMM registers are set to zero rather than restoring theirprevious content. The vulnerable code is used only on newer x86_64 processorssupporting the AVX512-IFMA instructions.The consequences of this kind of internal application state corruption canbe various – from no consequences, if the calling application does notdepend on the contents of non-volatile XMM registers at all, to the worstconsequences, where the attacker could get complete control of the applicationprocess. However given the contents of the registers are just zeroized sothe attacker cannot put arbitrary values inside, the most likely consequence,if any, would be an incorrect result of some application dependentcalculations or a crash leading to a denial of service.The POLY1305 MAC algorithm is most frequently used as part of theCHACHA20-POLY1305 AEAD (authenticated encryption with associated data)algorithm. The most common usage of this AEAD cipher is with TLS protocolversions 1.2 and 1.3 and a malicious client can influence whether this AEADcipher is used by the server. This implies that server applications usingOpenSSL can be potentially impacted. However we are currently not aware ofany concrete application that would be affected by this issue therefore weconsider this a Low severity security issue.As a workaround the AVX512-IFMA instructions support can be disabled atruntime by setting the environment variable OPENSSL_ia32cap: OPENSSL_ia32cap=:~0x200000The FIPS provider is not affected by this issue.

- Vulnerability: CVE-2009-3767

  - CVSS Score: 4.3
  - Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other versions, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2021-26690

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service

- Vulnerability: CVE-2021-26691

  - CVSS Score: 7.5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow

- Vulnerability: CVE-2019-0220

- CVSS Score: 5
- Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.

- Vulnerability: CVE-2024-38477

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- Vulnerability: CVE-2021-39275

  - CVSS Score: 7.5
  - Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2018-17189

  - CVSS Score: 5
  - Description: In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 (mod_http2) connections.

- Vulnerability: CVE-2022-29404

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2006-20001

  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2020-11993

  - CVSS Score: 4.3
  - Description: Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2021-3711
  - CVSS Score: 7.5
  - Description: In order to decrypt SM2 encrypted data an application is expected to call the API function EVP_PKEY_decrypt(). Typically an application will call this function twice. The first time, on entry, the "out" parameter can be NULL and, on exit, the "outlen" parameter is populated with the buffer size required to hold the decrypted plaintext. The application can then allocate a sufficiently sized buffer and call EVP_PKEY_decrypt() again, but this time passing a non-NULL value for the "out" parameter. A bug in the implementation of the SM2 decryption code means that the calculation of the buffer size required to hold the plaintext returned by the first call to EVP_PKEY_decrypt() can be smaller than the actual size required by the second call. This can lead to a buffer overflow when EVP_PKEY_decrypt() is called by the application a second time with a buffer that is too small. A malicious attacker who is able present SM2 content for decryption to an application could cause attacker chosen data to overflow the buffer by up to a maximum of 62 bytes altering the contents of other data held after the buffer, possibly changing application behaviour or causing the application to crash. The location of the buffer is application dependent but is typically heap allocated. Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k).

- Vulnerability: CVE-2024-0727
  - CVSS Score: N/A
  - Description: Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSLto crash leading to a potential Denial of Service attackImpact summary: Applications loading files in the PKCS12 format from untrustedsources might terminate abruptly.A file in PKCS12 format can contain certificates and keys and may come from anuntrusted source. The PKCS12 specification allows certain fields to be NULL, butOpenSSL does not correctly check for this case. This can lead to a NULL pointerdereference that results in OpenSSL crashing. If an application processes PKCS12files from an untrusted source using the OpenSSL APIs then that application willbe vulnerable to this issue.OpenSSL APIs that are vulnerable to this are: PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a similar issue in SMIME_write_PKCS7(). However since thisfunction is related to writing data we do not consider it security significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.

- Vulnerability: CVE-2009-3766
  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when OpenSSL is used, does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

- Vulnerability: CVE-2021-44224
  - CVSS Score: 6.4

- Description: A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).

- Vulnerability: CVE-2009-3765

  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2022-22721

  - CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2022-22720

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2019-10092

  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

- Vulnerability: CVE-2021-3712

  - CVSS Score: 5.8

– Description: ASN.1 strings are represented internally within OpenSSL as an
            ASN1_STRING structure which contains a buffer holding the string
            data and a field holding the buffer length. This contrasts with
            normal C strings which are repesented as a buffer for the string
            data which is terminated with a NUL (0) byte. Although not a
            strict requirement, ASN.1 strings that are parsed using OpenSSL's
            own "d2i" functions (and other similar parsing functions) as well
            as any string whose value has been set with the ASN1_STRING_set()
            function will additionally NUL terminate the byte array in the
            ASN1_STRING structure. However, it is possible for applications
            to directly construct valid ASN1_STRING structures which do not NUL
            terminate the byte array by directly setting the "data" and "length"
            fields in the ASN1_STRING array. This can also happen by using
            the ASN1_STRING_set0() function. Numerous OpenSSL functions that
            print ASN.1 data have been found to assume that the ASN1_STRING byte
            array will be NUL terminated, even though this is not guaranteed for
            strings that have been directly constructed. Where an application
            requests an ASN.1 structure to be printed, and where that ASN.1
            structure contains ASN1_STRINGs that have been directly constructed
            by the application without NUL terminating the "data" field, then
            a read buffer overrun can occur. The same thing can also occur
            during name constraints processing of certificates (for example
            if a certificate has been directly constructed by the application
            instead of loading it via the OpenSSL parsing functions, and the
            certificate contains non NUL terminated ASN1_STRING structures).
            It can also occur in the X509_get1_email(), X509_REQ_get1_email()
            and X509_get1_ocsp() functions. If a malicious actor can cause an
            application to directly construct an ASN1_STRING and then process it
            through one of the affected OpenSSL functions then this issue could
            be hit. This might result in a crash (causing a Denial of Service
            attack). It could also result in the disclosure of private memory
            contents (such as private keys, or sensitive plaintext). Fixed in
            OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za
            (Affected 1.0.2-1.0.2y).

- Vulnerability: CVE-2023-0464

  – CVSS Score: N/A

  – Description: A security vulnerability has been identified in all supported
            versionsof OpenSSL related to the verification of X.509 certificate
            chainsthat include policy constraints. Attackers may be able to
            exploit thisvulnerability by creating a malicious certificate chain
            that triggersexponential use of computational resources, leading
            to a denial-of-service(DoS) attack on affected systems.Policy
            processing is disabled by default but can be enabled by passingthe
            '-policy' argument to the command line utilities or by calling
            the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0465

  – CVSS Score: N/A

- Description: Applications that use a non-default option when verifying
certificates may bevulnerable to an attack from a malicious CA
to circumvent certain checks.Invalid certificate policies in leaf
certificates are silently ignored byOpenSSL and other certificate
policy checks are skipped for that certificate.A malicious CA could
use this to deliberately assert invalid certificate policiesin order
to circumvent policy checking on the certificate altogether.Policy
processing is disabled by default but can be enabled by passingthe
'-policy' argument to the command line utilities or by calling
the'X509_VERIFY_PARAM_set1_policies()' function.

- **Vulnerability:** CVE-2023-0466

  - CVSS Score: N/A
  - Description: The function X509_VERIFY_PARAM_add0_policy() is documented
toimplicitly enable the certificate policy check when doing
certificateverification. However the implementation of the
function does notenable the check which allows certificates
with invalid or incorrectpolicies to pass the certificate
verification.As suddenly enabling the policy check could break
existing deployments it wasdecided to keep the existing behavior of
the X509_VERIFY_PARAM_add0_policy()function.Instead the applications
that require OpenSSL to perform certificatepolicy check need
to use X509_VERIFY_PARAM_set1_policies() or explicitlyenable the
policy check by calling X509_VERIFY_PARAM_set_flags() withthe
X509_V_FLAG_POLICY_CHECK flag argument.Certificate policy checks
are disabled by default in OpenSSL and are notcommonly used by
applications.

- **Vulnerability:** CVE-2019-10098

  - CVSS Score: 5.8
  - Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with
mod_rewrite that were intended to be self-referential might be fooled
by encoded newlines and redirect instead to an unexpected URL within
the request URL.

- **Vulnerability:** CVE-2019-10097

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4.32-2.4.39, when mod_remoteip was configured
to use a trusted intermediary proxy server using the "PROXY"
protocol, a specially crafted PROXY header could trigger a stack
buffer overflow or NULL pointer deference. This vulnerability
could only be triggered by a trusted proxy and not by untrusted HTTP
clients.

- **Vulnerability:** CVE-2021-40438

  - CVSS Score: 6.8
  - Description: A crafted request uri-path can cause mod_proxy to forward the request
to an origin server choosen by the remote user. This issue affects
Apache HTTP Server 2.4.48 and earlier.

- **Vulnerability:** CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk
Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP
Server does not properly handle certain configuration sections that
specify NiceValue but not AssignUserID, which might allow remote
attackers to gain privileges by leveraging the root uid and root gid
of an mpm-itk process.

- Vulnerability: CVE-2022-23943

  – CVSS Score: 7.5
  – Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

- Vulnerability: CVE-2018-17199

  – CVSS Score: 5
  – Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

- Vulnerability: CVE-2021-23841

  – CVSS Score: 4.3
  – Description: The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack. The function X509_issuer_and_serial_hash() is never directly called by OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on certificates that may have been obtained from untrusted sources. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2021-34798

  – CVSS Score: 5
  – Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2023-25690

  – CVSS Score: N/A
  – Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2020-11984

- CVSS Score: 7.5
- Description: Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE

- **Vulnerability: CVE-2021-4160**

  - CVSS Score: 4.3
  - Description: There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that is available to premium support customers only. It will be made available in 1.0.2zc when it is released. The issue only affects OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0). Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL 1.0.2zc-dev (Affected 1.0.2-1.0.2zb).

- **Vulnerability: CVE-2022-26377**

  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- **Vulnerability: CVE-2019-10081**

  - CVSS Score: 5
  - Description: HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example configured with "H2PushResource", could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client.

- **Vulnerability: CVE-2019-10082**

  - CVSS Score: 6.4
  - Description: In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.

- **Vulnerability: CVE-2024-40898**

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2023-27522

  – CVSS Score: N/A

  – Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.Special characters in the origin response header can truncate/split the response forwarded to the client.

- Vulnerability: CVE-2022-0778

  – CVSS Score: 5

  – Description: The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: – TLS clients consuming server certificates – TLS servers consuming client certificates – Hosting providers taking certificates or private keys from customers – Certificate authorities parsing certification requests from subscribers – Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

- Vulnerability: CVE-2022-2097

  – CVSS Score: 5

  – Description: AES OCB mode for 32-bit x86 platforms using the AES-NI assembly optimised implementation will not encrypt the entirety of the data under some circumstances. This could reveal sixteen bytes of data that was preexisting in the memory that wasn't written. In the special case of "in place" encryption, sixteen bytes of the plaintext would be revealed. Since OpenSSL does not support OCB based cipher suites for TLS and DTLS, they are both unaffected. Fixed in OpenSSL 3.0.5 (Affected 3.0.0-3.0.4). Fixed in OpenSSL 1.1.1q (Affected 1.1.1-1.1.1p).

- Vulnerability: CVE-2020-1971

  – CVSS Score: 4.3

- Description: The X.509 GeneralName type is a generic type for representing
  different types of names. One of those name types is known as
  EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which
  compares different instances of a GENERAL_NAME to see if they
  are equal or not. This function behaves incorrectly when both
  GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference
  and a crash may occur leading to a possible denial of service
  attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two
  purposes: 1) Comparing CRL distribution point names between an
  available CRL and a CRL distribution point embedded in an X509
  certificate 2) When verifying that a timestamp response token signer
  matches the timestamp authority name (exposed via the API functions
  TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can
  control both items being compared then that attacker could trigger
  a crash. For example if the attacker can trick a client or server
  into checking a malicious certificate against a malicious CRL then
  this may occur. Note that some applications automatically download
  CRLs based on a URL embedded in a certificate. This checking happens
  prior to the signatures on the certificate and CRL being verified.
  OpenSSL's s_server, s_client and verify tools have support for the
  "-crl_download" option which implements automatic CRL downloading and
  this attack has been demonstrated to work against those tools. Note
  that an unrelated bug means that affected versions of OpenSSL cannot
  parse or construct correct encodings of EDIPARTYNAME. However it is
  possible to construct a malformed EDIPARTYNAME that OpenSSL's parser
  will accept and hence trigger this attack. All OpenSSL 1.1.1 and
  1.0.2 versions are affected by this issue. Other OpenSSL releases
  are out of support and have not been checked. Fixed in OpenSSL
  1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected
  1.0.2-1.0.2w).

- Vulnerability: CVE-2009-1390

  - CVSS Score: 6.8
  - Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2)
    GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS
    certificate in the chain is accepted instead of verifying the entire
    chain, which allows remote attackers to spoof trusted servers via a
    man-in-the-middle attack.

- Vulnerability: CVE-2012-3526

  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the
    Apache HTTP Server allows remote attackers to cause a denial of
    service (server or application crash) via multiple X-Forwarded-For
    headers in a request.

- Vulnerability: CVE-2023-5678

  - CVSS Score: N/A

- Description: Issue summary: Generating excessively long X9.42 DH keys or checkingexcessively long X9.42 DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_generate_key() togenerate an X9.42 DH key may experience long delays. Likewise, applicationsthat use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check()to check an X9.42 DH key or X9.42 DH parameters may experience long delays.Where the key or parameters that are being checked have been obtained froman untrusted source this may lead to a Denial of Service.While DH_check() performs all the necessary checks (as of CVE-2023-3817),DH_check_pub_key() doesn't make any of these checks, and is thereforevulnerable for excessively large P and Q parameters.Likewise, while DH_generate_key() performs a check for an excessively largeP, it doesn't check for an excessively large Q.An application that calls DH_generate_key() or DH_check_pub_key() andsupplies a key or parameters obtained from an untrusted source could bevulnerable to a Denial of Service attack.DH_generate_key() and DH_check_pub_key() are also called by a number ofother OpenSSL functions. An application calling any of those otherfunctions may similarly be affected. The other functions affected by thisare DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate().Also vulnerable are the OpenSSL pkey command line application when using the"-pubcheck" option, as well as the OpenSSL genpkey command line application.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2022-1292

  - CVSS Score: 10
  - Description: The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n). Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).

- Vulnerability: CVE-2012-4001

  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2022-37436

  - CVSS Score: N/A

- Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2021-23840

  - CVSS Score: 5
  - Description: Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissable length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2022-4450

  - CVSS Score: N/A
  - Description: The function PEM_read_bio_ex() reads a PEM file from a BIO and parses anddecodes the "name" (e.g. "CERTIFICATE"), any header data and the payload data.If the function succeeds then the "name_out", "header" and "data" arguments arepopulated with pointers to buffers containing the relevant decoded data. Thecaller is responsible for freeing those buffers. It is possible to construct aPEM file that results in 0 bytes of payload data. In this case PEM_read_bio_ex()will return a failure code but will populate the header argument with a pointerto a buffer that has already been freed. If the caller also frees this bufferthen a double free will occur. This will most likely lead to a crash. Thiscould be exploited by an attacker who has the ability to supply malicious PEMfiles for parsing to achieve a denial of service attack.The functions PEM_read_bio() and PEM_read() are simple wrappers aroundPEM_read_bio_ex() and therefore these functions are also directly affected.These functions are also called indirectly by a number of other OpenSSLfunctions including PEM_X509_INFO_read_bio_ex() andSSL_CTX_use_serverinfo_file() which are also vulnerable. Some OpenSSL internaluses of these functions are not vulnerable because the caller does not free theheader argument if PEM_read_bio_ex() returns a failure code. These locationsinclude the PEM_read_bio_TYPE() functions as well as the decoders introduced inOpenSSL 3.0.The OpenSSL asn1parse command line application is also impacted by this issue.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5

- Description: SQL injection vulnerability in mysql/mysql-auth.pl in the
  mod_authnz_external module 3.2.5 and earlier for the Apache HTTP
  Server allows remote attackers to execute arbitrary SQL commands
  via the user field.

- **Vulnerability:** CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5
    for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM
    Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows
    use an improper encryption algorithm and a weak key for maintaining
    the stored data of the node secret for the SecurID Authentication
    API, which allows local users to obtain sensitive information via
    cryptographic attacks on this data.

- **Vulnerability:** CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication
    Agent 7.1 before 7.1.1 for Web for Internet Information Services,
    and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to
    inject arbitrary web script or HTML via unspecified vectors.

- **Vulnerability:** CVE-2023-45802

  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a
    time window were the request's memory resources were not reclaimed
    immediately. Instead, de-allocation was deferred to connection
    close. A client could send new requests and resets, keeping the
    connection busy and open and causing the memory footprint to keep
    on growing. On connection close, all resources were reclaimed, but
    the process might run out of memory before that.This was found by
    the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset
    Exploit) with their own test client. During "normal" HTTP/2 use, the
    probability to hit this bug is very low. The kept memory would not
    become noticeable before the connection closes or times out.Users are
    recommended to upgrade to version 2.4.58, which fixes the issue.

- **Vulnerability:** CVE-2022-28615

  - CVSS Score: 6.4
  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose
    information due to a read beyond bounds in ap_strcmp_match() when
    provided with an extremely large input buffer. While no code
    distributed with the server can be coerced into such a call,
    third-party modules or lua scripts that use ap_strcmp_match() may
    hypothetically be affected.

- **Vulnerability:** CVE-2022-28614

  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier
    may read unintended memory if an attacker can cause the server to
    reflect very large input using ap_rwrite() or ap_rputs(), such as
    with mod_luas r:puts() function. Modules compiled and distributed
    separately from Apache HTTP Server that use the 'ap_rputs' function
    and may pass it a very large (INT_MAX or larger) string must be
    compiled against current headers to resolve the issue.

- **Vulnerability:** CVE-2013-0941

- CVSS Score: 2.1
- Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2012-4001

  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2024-38476

  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-38477

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-38474

  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2024-40898

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2011-1176

- CVSS Score: 4.3
- Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2009-0796

  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2013-4365

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2012-3526

  - CVSS Score: 5

– Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the
                   Apache HTTP Server allows remote attackers to cause a denial of
                   service (server or application crash) via multiple X-Forwarded-For
                   headers in a request.

- Vulnerability: CVE-2012-4360

  – CVSS Score: 4.3

  – Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module
                   0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote
                   attackers to inject arbitrary web script or HTML via unspecified
                   vectors.

11.16 IP Address: 159.149.53.217

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 2

- High Vulnerabilities: 13

- Medium Vulnerabilities: 56

- Low Vulnerabilities: 3

- Total Vulnerabilities: 74

Services Running on IP Address

- Service: Apache httpd

    - Port: 443
    - Version: 2.4.37
    - Location: https://www.unimi.it/

Vulnerabilities Found

- Vulnerability: CVE-2019-0215

    - CVSS Score: 6
    - Description: In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in mod_ssl when using per-location client certificate verification with TLSv1.3 allowed a client to bypass configured access control restrictions.

- Vulnerability: CVE-2013-4365

    - CVSS Score: 7.5
    - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2022-28330

    - CVSS Score: 5
    - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2021-32791

    - CVSS Score: 4.3
    - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2021-32792

    - CVSS Score: 4.3

- Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using `OIDCPreservePost On`.

- Vulnerability: CVE-2023-31122
  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2024-38476
  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-27316
  - CVSS Score: N/A
  - Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

- Vulnerability: CVE-2024-38474
  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2009-0796
  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2022-2068
  - CVSS Score: 10

- Description: In addition to the c_rehash shell command injection identified in
  CVE-2022-1292, further circumstances where the c_rehash script
  does not properly sanitise shell metacharacters to prevent command
  injection were found by code review. When the CVE-2022-1292 was
  fixed it was not discovered that there are other places in the
  script where the file names of certificates being hashed were
  possibly passed to a command executed through the shell. This
  script is distributed by some operating systems in a manner where
  it is automatically executed. On such operating systems, an
  attacker could execute arbitrary commands with the privileges of
  the script. Use of the c_rehash script is considered obsolete and
  should be replaced by the OpenSSL rehash command line tool. Fixed in
  OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL
  1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected
  1.0.2-1.0.2ze).

- Vulnerability: CVE-2021-3449

  - CVSS Score: 4.3
  - Description: An OpenSSL TLS server may crash if sent a maliciously crafted
    renegotiation ClientHello message from a client. If a TLSv1.2
    renegotiation ClientHello omits the signature_algorithms extension
    (where it was present in the initial ClientHello), but includes a
    signature_algorithms_cert extension then a NULL pointer dereference
    will result, leading to a crash and a denial of service attack. A
    server is only vulnerable if it has TLSv1.2 and renegotiation enabled
    (which is the default configuration). OpenSSL TLS clients are not
    impacted by this issue. All OpenSSL 1.1.1 versions are affected
    by this issue. Users of these versions should upgrade to OpenSSL
    1.1.1k. OpenSSL 1.0.2 is not impacted by this issue. Fixed in
    OpenSSL 1.1.1k (Affected 1.1.1-1.1.1j).

- Vulnerability: CVE-2021-36160

  - CVSS Score: 5
  - Description: A carefully crafted request uri-path can cause mod_proxy_uwsgi to read
    above the allocated memory and crash (DoS). This issue affects Apache
    HTTP Server versions 2.4.30 to 2.4.48 (inclusive).

- Vulnerability: CVE-2020-1927

  - CVSS Score: 5.8
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with
    mod_rewrite that were intended to be self-referential might be fooled
    by encoded newlines and redirect instead to an an unexpected URL
    within the request URL.

- Vulnerability: CVE-2023-0286

  - CVSS Score: N/A

– Description: There is a type confusion vulnerability relating to X.400 address processinginside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING butthe public structure definition for GENERAL_NAME incorrectly specified the typeof the x400Address field as ASN1_TYPE. This field is subsequently interpreted bythe OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than anASN1_STRING.When CRL checking is enabled (i.e. the application sets theX509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to passarbitrary pointers to a memcmp call, enabling them to read memory contents orenact a denial of service. In most cases, the attack requires the attacker toprovide both the certificate chain and CRL, neither of which need to have avalid signature. If the attacker only controls one of these inputs, the otherinput must already contain an X.400 address as a CRL distribution point, whichis uncommon. As such, this vulnerability is most likely to only affectapplications which have implemented their own functionality for retrieving CRLsover a network.

- Vulnerability: CVE-2023-3817

  – CVSS Score: N/A

  – Description: Issue summary: Checking excessively long DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH key or DH parameters may experience longdelays. Where the key or parameters that are being checked have been obtainedfrom an untrusted source this may lead to a Denial of Service.The function DH_check() performs various checks on DH parameters. After fixingCVE-2023-3446 it was discovered that a large q parameter value can also triggeran overly long computation during some of these checks. A correct q value,if present, cannot be larger than the modulus p parameter, thus it isunnecessary to perform these checks if q is larger than p.An application that calls DH_check() and supplies a key or parameters obtainedfrom an untrusted source could be vulnerable to a Denial of Service attack.The function DH_check() is itself called by a number of other OpenSSL functions.An application calling any of those other functions may similarly be affected.The other functions affected by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable are the OpenSSL dhparam and pkeyparam command line applicationswhen using the "-check" option.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2021-32786

  – CVSS Score: 5.8

  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, 'oidc_validate_redirect_url()' does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring 'mod_auth_openidc' to only allow redirection whose destination matches a given regular expression.

- Vulnerability: CVE-2021-32785

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache ('OIDCCacheEncrypt off', 'OIDCSessionType server-cache', 'OIDCCacheType redis'), 'mod_auth_openidc' wrongly performed argument interpolation before passing Redis requests to 'hiredis', which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the 'hiredis' API. As a workaround, this vulnerability can be mitigated by setting 'OIDCCacheEncrypt' to 'on', as cache keys are cryptographically hashed before use when this option is enabled.

- Vulnerability: CVE-2020-9490

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2021-44790

  - CVSS Score: 7.5
  - Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

- Vulnerability: CVE-2020-13938

  - CVSS Score: 2.1
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

- Vulnerability: CVE-2023-2650

  - CVSS Score: N/A

- Description: Issue summary: Processing some specially crafted ASN.1 object identifiers ordata containing them may be very slow.Impact summary: Applications that use OBJ_obj2txt() directly, or use any ofthe OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no messagesize limit may experience notable to very long delays when processing thosemessages, which may lead to a Denial of Service.An OBJECT IDENTIFIER is composed of a series of numbers - sub-identifiers -most of which have no size limit. OBJ_obj2txt() may be used to translatean ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSLtype ASN1_OBJECT) to its canonical numeric text form, which are thesub-identifiers of the OBJECT IDENTIFIER in decimal form, separated byperiods.When one of the sub-identifiers in the OBJECT IDENTIFIER is very large(these are sizes that are seen as absurdly large, taking up tens or hundredsof KiBs), the translation to a decimal number in text may take a very longtime. The time complexity is $O(n^2)$ with 'n' being the size of thesub-identifiers in bytes (*).With OpenSSL 3.0, support to fetch cryptographic algorithms using names /identifiers in string form was introduced. This includes using OBJECTIDENTIFIERs in canonical numeric text form as identifiers for fetchingalgorithms.Such OBJECT IDENTIFIERs may be received through the ASN.1 structureAlgorithmIdentifier, which is commonly used in multiple protocols to specifywhat cryptographic algorithm should be used to sign or verify, encrypt ordecrypt, or digest passed data.Applications that call OBJ_obj2txt() directly with untrusted data areaffected, with any version of OpenSSL. If the use is for the mere purposeof display, the severity is considered low.In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME,CMS, CMP/CRMF or TS. It also impacts anything that processes X.509certificates, including simple things like verifying its signature.The impact on TLS is relatively low, because all versions of OpenSSL have a100KiB limit on the peer's certificate chain. Additionally, this onlyimpacts clients, or servers that have explicitly enabled clientauthentication.In OpenSSL 1.1.1 and 1.0.2, this only affects displaying diverse objects,such as X.509 certificates. This is assumed to not happen in such a waythat it would cause a Denial of Service, so these versions are considerednot affected by this issue in such a way that it would be cause for concern,and the severity is therefore considered low.

- Vulnerability: CVE-2023-0215

  - CVSS Score: N/A

- Description: The public API function BIO_new_NDEF is a helper function used for streamingASN.1 data via a BIO. It is primarily used internally to OpenSSL to support theSMIME, CMS and PKCS7 streaming capabilities, but may also be called directly byend user applications.The function receives a BIO from the caller, prepends a new BIO_f_asn1 filterBIO onto the front of it to form a BIO chain, and then returns the new head ofthe BIO chain to the caller. Under certain conditions, for example if a CMSrecipient public key is invalid, the new filter BIO is freed and the functionreturns a NULL result indicating a failure. However, in this case, the BIO chainis not properly cleaned up and the BIO passed by the caller still retainsinternal pointers to the previously freed filter BIO. If the caller then goes onto call BIO_pop() on the BIO then a use-after-free will occur. This will mostlikely result in a crash.This scenario occurs directly in the internal function B64_write_ASN1() whichmay cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() onthe BIO. This internal function is in turn called by the public API functionsPEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream,SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7.Other public API functions that may be impacted by this includei2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream andi2d_PKCS7_bio_stream.The OpenSSL cms and smime command line applications are similarly affected.

- Vulnerability: CVE-2020-35452

  - CVSS Score: 6.8
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

- Vulnerability: CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2020-1934

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

- Vulnerability: CVE-2022-36760

  - CVSS Score: N/A
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-4304

  - CVSS Score: N/A

- Description: A timing based side channel exists in the OpenSSL RSA Decryption implementationwhich could be sufficient to recover a plaintext across a network in aBleichenbacher style attack. To achieve a successful decryption an attackerwould have to be able to send a very large number of trial messages fordecryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5,RSA-OEAP and RSASVE.For example, in a TLS connection, RSA is commonly used by a client to send anencrypted pre-master secret to the server. An attacker that had observed agenuine connection between a client and a server could use this flaw to sendtrial messages to the server and record the time taken to process them. After asufficiently large number of messages the attacker could recover the pre-mastersecret used for the original connection and thus be able to decrypt theapplication data sent over that connection.

• Vulnerability: CVE-2019-9517

  - CVSS Score: 7.8
  - Description: Some HTTP/2 implementations are vulnerable to unconstrained interal data buffering, potentially leading to a denial of service. The attacker opens the HTTP/2 window so the peer can send without constraint; however, they leave the TCP window closed so the peer cannot actually write (many of) the bytes on the wire. The attacker then sends a stream of requests for a large response object. Depending on how the servers queue the responses, this can consume excess memory, CPU, or both.

• Vulnerability: CVE-2019-0217

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.

• Vulnerability: CVE-2019-0197

  - CVSS Score: 4.9
  - Description: A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue.

• Vulnerability: CVE-2019-0196

  - CVSS Score: 5
  - Description: A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.

• Vulnerability: CVE-2019-0190

  - CVSS Score: 5
  - Description: A bug exists in the way mod_ssl handled client renegotiations. A remote attacker could send a carefully crafted request that would cause mod_ssl to enter a loop leading to a denial of service. This bug can be only triggered with Apache HTTP Server version 2.4.37 when using OpenSSL version 1.1.1 or later, due to an interaction in changes to handling of renegotiation attempts.

- Vulnerability: CVE-2021-33193

  - CVSS Score: 5
  - Description: A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.

- Vulnerability: CVE-2019-0211

  - CVSS Score: 7.2
  - Description: In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.

- Vulnerability: CVE-2019-17567

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

- Vulnerability: CVE-2022-31813

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

- Vulnerability: CVE-2012-4360

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2023-4807

  - CVSS Score: N/A

- Description: Issue summary: The POLY1305 MAC (message authentication code)
             implementationcontains a bug that might corrupt the internal state
             of applications on theWindows 64 platform when running on newer
             X86‿64 processors supporting theAVX512-IFMA instructions.Impact
             summary: If in an application that uses the OpenSSL library an
             attackercan influence whether the POLY1305 MAC algorithm is used,
             the applicationstate might be corrupted with various application
             dependent consequences.The POLY1305 MAC (message authentication
             code) implementation in OpenSSL doesnot save the contents of
             non-volatile XMM registers on Windows 64 platformwhen calculating
             the MAC of data larger than 64 bytes. Before returning tothe
             caller all the XMM registers are set to zero rather than restoring
             theirprevious content. The vulnerable code is used only on newer
             x86‿64 processorssupporting the AVX512-IFMA instructions.The
             consequences of this kind of internal application state corruption
             canbe various – from no consequences, if the calling application
             does notdepend on the contents of non-volatile XMM registers at
             all, to the worstconsequences, where the attacker could get complete
             control of the applicationprocess. However given the contents of
             the registers are just zeroized sothe attacker cannot put arbitrary
             values inside, the most likely consequence,if any, would be an
             incorrect result of some application dependentcalculations or a crash
             leading to a denial of service.The POLY1305 MAC algorithm is most
             frequently used as part of theCHACHA20-POLY1305 AEAD (authenticated
             encryption with associated data)algorithm. The most common usage
             of this AEAD cipher is with TLS protocolversions 1.2 and 1.3 and
             a malicious client can influence whether this AEADcipher is used
             by the server. This implies that server applications usingOpenSSL
             can be potentially impacted. However we are currently not aware
             ofany concrete application that would be affected by this issue
             therefore weconsider this a Low severity security issue.As a
             workaround the AVX512-IFMA instructions support can be disabled
             atruntime by setting the environment variable OPENSSL‿ia32cap:
             OPENSSL‿ia32cap=:˜0x200000The FIPS provider is not affected by this
             issue.

- Vulnerability: CVE-2009-3767

  - CVSS Score: 4.3
  - Description: libraries/libldap/tls‿o.c in OpenLDAP 2.2 and 2.4, and possibly other
             versions, when OpenSSL is used, does not properly handle a '\{}0'
             character in a domain name in the subject's Common Name (CN) field
             of an X.509 certificate, which allows man-in-the-middle attackers
             to spoof arbitrary SSL servers via a crafted certificate issued by a
             legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2021-26690

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted
             Cookie header handled by mod‿session can cause a NULL pointer
             dereference and crash, leading to a possible Denial Of Service

- Vulnerability: CVE-2021-26691

  - CVSS Score: 7.5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted
             SessionHeader sent by an origin server could cause a heap overflow

- Vulnerability: CVE-2019-0220

- CVSS Score: 5
- Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.

- Vulnerability: CVE-2024-38477

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- Vulnerability: CVE-2021-39275

  - CVSS Score: 7.5
  - Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2018-17189

  - CVSS Score: 5
  - Description: In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 (mod_http2) connections.

- Vulnerability: CVE-2022-29404

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2006-20001

  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2020-11993

  - CVSS Score: 4.3
  - Description: Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2021-3711

    - CVSS Score: 7.5
    - Description: In order to decrypt SM2 encrypted data an application is expected to call the API function EVP_PKEY_decrypt(). Typically an application will call this function twice. The first time, on entry, the "out" parameter can be NULL and, on exit, the "outlen" parameter is populated with the buffer size required to hold the decrypted plaintext. The application can then allocate a sufficiently sized buffer and call EVP_PKEY_decrypt() again, but this time passing a non-NULL value for the "out" parameter. A bug in the implementation of the SM2 decryption code means that the calculation of the buffer size required to hold the plaintext returned by the first call to EVP_PKEY_decrypt() can be smaller than the actual size required by the second call. This can lead to a buffer overflow when EVP_PKEY_decrypt() is called by the application a second time with a buffer that is too small. A malicious attacker who is able present SM2 content for decryption to an application could cause attacker chosen data to overflow the buffer by up to a maximum of 62 bytes altering the contents of other data held after the buffer, possibly changing application behaviour or causing the application to crash. The location of the buffer is application dependent but is typically heap allocated. Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k).

- Vulnerability: CVE-2024-0727

    - CVSS Score: N/A
    - Description: Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSLto crash leading to a potential Denial of Service attackImpact summary: Applications loading files in the PKCS12 format from untrustedsources might terminate abruptly.A file in PKCS12 format can contain certificates and keys and may come from anuntrusted source. The PKCS12 specification allows certain fields to be NULL, butOpenSSL does not correctly check for this case. This can lead to a NULL pointerdereference that results in OpenSSL crashing. If an application processes PKCS12files from an untrusted source using the OpenSSL APIs then that application willbe vulnerable to this issue.OpenSSL APIs that are vulnerable to this are: PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a similar issue in SMIME_write_PKCS7(). However since thisfunction is related to writing data we do not consider it security significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.

- Vulnerability: CVE-2009-3766

    - CVSS Score: 6.8
    - Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when OpenSSL is used, does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

- Vulnerability: CVE-2021-44224

    - CVSS Score: 6.4

- Description: A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).

- Vulnerability: CVE-2009-3765

  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2022-22721

  - CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2022-22720

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2019-10092

  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

- Vulnerability: CVE-2021-3712

  - CVSS Score: 5.8

- Description: ASN.1 strings are represented internally within OpenSSL as an
  ASN1_STRING structure which contains a buffer holding the string
  data and a field holding the buffer length. This contrasts with
  normal C strings which are repesented as a buffer for the string
  data which is terminated with a NUL (0) byte. Although not a
  strict requirement, ASN.1 strings that are parsed using OpenSSL's
  own "d2i" functions (and other similar parsing functions) as well
  as any string whose value has been set with the ASN1_STRING_set()
  function will additionally NUL terminate the byte array in the
  ASN1_STRING structure. However, it is possible for applications
  to directly construct valid ASN1_STRING structures which do not NUL
  terminate the byte array by directly setting the "data" and "length"
  fields in the ASN1_STRING array. This can also happen by using
  the ASN1_STRING_set0() function. Numerous OpenSSL functions that
  print ASN.1 data have been found to assume that the ASN1_STRING byte
  array will be NUL terminated, even though this is not guaranteed for
  strings that have been directly constructed. Where an application
  requests an ASN.1 structure to be printed, and where that ASN.1
  structure contains ASN1_STRINGs that have been directly constructed
  by the application without NUL terminating the "data" field, then
  a read buffer overrun can occur. The same thing can also occur
  during name constraints processing of certificates (for example
  if a certificate has been directly constructed by the application
  instead of loading it via the OpenSSL parsing functions, and the
  certificate contains non NUL terminated ASN1_STRING structures).
  It can also occur in the X509_get1_email(), X509_REQ_get1_email()
  and X509_get1_ocsp() functions. If a malicious actor can cause an
  application to directly construct an ASN1_STRING and then process it
  through one of the affected OpenSSL functions then this issue could
  be hit. This might result in a crash (causing a Denial of Service
  attack). It could also result in the disclosure of private memory
  contents (such as private keys, or sensitive plaintext). Fixed in
  OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za
  (Affected 1.0.2-1.0.2y).

- Vulnerability: CVE-2023-0464

  - CVSS Score: N/A

  - Description: A security vulnerability has been identified in all supported
    versionsof OpenSSL related to the verification of X.509 certificate
    chainsthat include policy constraints. Attackers may be able to
    exploit thisvulnerability by creating a malicious certificate chain
    that triggersexponential use of computational resources, leading
    to a denial-of-service(DoS) attack on affected systems.Policy
    processing is disabled by default but can be enabled by passingthe
    '-policy' argument to the command line utilities or by calling
    the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0465

  - CVSS Score: N/A

- Description: Applications that use a non-default option when verifying
certificates may bevulnerable to an attack from a malicious CA
to circumvent certain checks.Invalid certificate policies in leaf
certificates are silently ignored byOpenSSL and other certificate
policy checks are skipped for that certificate.A malicious CA could
use this to deliberately assert invalid certificate policiesin order
to circumvent policy checking on the certificate altogether.Policy
processing is disabled by default but can be enabled by passingthe
'-policy' argument to the command line utilities or by calling
the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0466

  - CVSS Score: N/A
  - Description: The function X509_VERIFY_PARAM_add0_policy() is documented
toimplicitly enable the certificate policy check when doing
certificateverification. However the implementation of the
function does notenable the check which allows certificates
with invalid or incorrectpolicies to pass the certificate
verification.As suddenly enabling the policy check could break
existing deployments it wasdecided to keep the existing behavior of
the X509_VERIFY_PARAM_add0_policy()function.Instead the applications
that require OpenSSL to perform certificatepolicy check need
to use X509_VERIFY_PARAM_set1_policies() or explicitlyenable the
policy check by calling X509_VERIFY_PARAM_set_flags() withthe
X509_V_FLAG_POLICY_CHECK flag argument.Certificate policy checks
are disabled by default in OpenSSL and are notcommonly used by
applications.

- Vulnerability: CVE-2019-10098

  - CVSS Score: 5.8
  - Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with
mod_rewrite that were intended to be self-referential might be fooled
by encoded newlines and redirect instead to an unexpected URL within
the request URL.

- Vulnerability: CVE-2019-10097

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4.32-2.4.39, when mod_remoteip was configured
to use a trusted intermediary proxy server using the "PROXY"
protocol, a specially crafted PROXY header could trigger a stack
buffer overflow or NULL pointer deference. This vulnerability
could only be triggered by a trusted proxy and not by untrusted HTTP
clients.

- Vulnerability: CVE-2021-40438

  - CVSS Score: 6.8
  - Description: A crafted request uri-path can cause mod_proxy to forward the request
to an origin server choosen by the remote user. This issue affects
Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk
Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP
Server does not properly handle certain configuration sections that
specify NiceValue but not AssignUserID, which might allow remote
attackers to gain privileges by leveraging the root uid and root gid
of an mpm-itk process.

- Vulnerability: CVE-2022-23943

  – CVSS Score: 7.5
  – Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

- Vulnerability: CVE-2018-17199

  – CVSS Score: 5
  – Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

- Vulnerability: CVE-2021-23841

  – CVSS Score: 4.3
  – Description: The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack. The function X509_issuer_and_serial_hash() is never directly called by OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on certificates that may have been obtained from untrusted sources. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2021-34798

  – CVSS Score: 5
  – Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2023-25690

  – CVSS Score: N/A
  – Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "⁀/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2020-11984

- CVSS Score: 7.5
- Description: Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE

- Vulnerability: CVE-2021-4160

  - CVSS Score: 4.3
  - Description: There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that is available to premium support customers only. It will be made available in 1.0.2zc when it is released. The issue only affects OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0). Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL 1.0.2zc-dev (Affected 1.0.2-1.0.2zb).

- Vulnerability: CVE-2022-26377

  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2019-10081

  - CVSS Score: 5
  - Description: HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example configured with "H2PushResource", could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client.

- Vulnerability: CVE-2019-10082

  - CVSS Score: 6.4
  - Description: In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.

- Vulnerability: CVE-2024-40898

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2023-27522

  – CVSS Score: N/A

  – Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.Special characters in the origin response header can truncate/split the response forwarded to the client.

- Vulnerability: CVE-2022-0778

  – CVSS Score: 5

  – Description: The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - TLS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

- Vulnerability: CVE-2022-2097

  – CVSS Score: 5

  – Description: AES OCB mode for 32-bit x86 platforms using the AES-NI assembly optimised implementation will not encrypt the entirety of the data under some circumstances. This could reveal sixteen bytes of data that was preexisting in the memory that wasn't written. In the special case of "in place" encryption, sixteen bytes of the plaintext would be revealed. Since OpenSSL does not support OCB based cipher suites for TLS and DTLS, they are both unaffected. Fixed in OpenSSL 3.0.5 (Affected 3.0.0-3.0.4). Fixed in OpenSSL 1.1.1q (Affected 1.1.1-1.1.1p).

- Vulnerability: CVE-2020-1971

  – CVSS Score: 4.3

- Description: The X.509 GeneralName type is a generic type for representing
  different types of names. One of those name types is known as
  EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which
  compares different instances of a GENERAL_NAME to see if they
  are equal or not. This function behaves incorrectly when both
  GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference
  and a crash may occur leading to a possible denial of service
  attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two
  purposes: 1) Comparing CRL distribution point names between an
  available CRL and a CRL distribution point embedded in an X509
  certificate 2) When verifying that a timestamp response token signer
  matches the timestamp authority name (exposed via the API functions
  TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can
  control both items being compared then that attacker could trigger
  a crash. For example if the attacker can trick a client or server
  into checking a malicious certificate against a malicious CRL then
  this may occur. Note that some applications automatically download
  CRLs based on a URL embedded in a certificate. This checking happens
  prior to the signatures on the certificate and CRL being verified.
  OpenSSL's s_server, s_client and verify tools have support for the
  "-crl_download" option which implements automatic CRL downloading and
  this attack has been demonstrated to work against those tools. Note
  that an unrelated bug means that affected versions of OpenSSL cannot
  parse or construct correct encodings of EDIPARTYNAME. However it is
  possible to construct a malformed EDIPARTYNAME that OpenSSL's parser
  will accept and hence trigger this attack. All OpenSSL 1.1.1 and
  1.0.2 versions are affected by this issue. Other OpenSSL releases
  are out of support and have not been checked. Fixed in OpenSSL
  1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected
  1.0.2-1.0.2w).

- Vulnerability: CVE-2009-1390

  - CVSS Score: 6.8
  - Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2)
    GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS
    certificate in the chain is accepted instead of verifying the entire
    chain, which allows remote attackers to spoof trusted servers via a
    man-in-the-middle attack.

- Vulnerability: CVE-2012-3526

  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the
    Apache HTTP Server allows remote attackers to cause a denial of
    service (server or application crash) via multiple X-Forwarded-For
    headers in a request.

- Vulnerability: CVE-2023-5678

  - CVSS Score: N/A

- Description: Issue summary: Generating excessively long X9.42 DH keys or checkingexcessively long X9.42 DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_generate_key() togenerate an X9.42 DH key may experience long delays. Likewise, applicationsthat use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check()to check an X9.42 DH key or X9.42 DH parameters may experience long delays.Where the key or parameters that are being checked have been obtained froman untrusted source this may lead to a Denial of Service.While DH_check() performs all the necessary checks (as of CVE-2023-3817),DH_check_pub_key() doesn't make any of these checks, and is thereforevulnerable for excessively large P and Q parameters.Likewise, while DH_generate_key() performs a check for an excessively largeP, it doesn't check for an excessively large Q.An application that calls DH_generate_key() or DH_check_pub_key() andsupplies a key or parameters obtained from an untrusted source could bevulnerable to a Denial of Service attack.DH_generate_key() and DH_check_pub_key() are also called by a number ofother OpenSSL functions. An application calling any of those otherfunctions may similarly be affected. The other functions affected by thisare DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate().Also vulnerable are the OpenSSL pkey command line application when using the"-pubcheck" option, as well as the OpenSSL genpkey command line application.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2022-1292

  - CVSS Score: 10
  - Description: The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n). Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).

- Vulnerability: CVE-2012-4001

  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2022-37436

  - CVSS Score: N/A

- Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2021-23840

  - CVSS Score: 5
  - Description: Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissable length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2022-4450

  - CVSS Score: N/A
  - Description: The function PEM_read_bio_ex() reads a PEM file from a BIO and parses anddecodes the "name" (e.g. "CERTIFICATE"), any header data and the payload data.If the function succeeds then the "name_out", "header" and "data" arguments arepopulated with pointers to buffers containing the relevant decoded data. Thecaller is responsible for freeing those buffers. It is possible to construct aPEM file that results in 0 bytes of payload data. In this case PEM_read_bio_ex()will return a failure code but will populate the header argument with a pointerto a buffer that has already been freed. If the caller also frees this bufferthen a double free will occur. This will most likely lead to a crash. Thiscould be exploited by an attacker who has the ability to supply malicious PEMfiles for parsing to achieve a denial of service attack.The functions PEM_read_bio() and PEM_read() are simple wrappers aroundPEM_read_bio_ex() and therefore these functions are also directly affected.These functions are also called indirectly by a number of other OpenSSLfunctions including PEM_X509_INFO_read_bio_ex() andSSL_CTX_use_serverinfo_file() which are also vulnerable. Some OpenSSL internaluses of these functions are not vulnerable because the caller does not free theheader argument if PEM_read_bio_ex() returns a failure code. These locationsinclude the PEM_read_bio_TYPE() functions as well as the decoders introduced inOpenSSL 3.0.The OpenSSL asn1parse command line application is also impacted by this issue.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5

- Description: SQL injection vulnerability in mysql/mysql-auth.pl in the
  mod_authnz_external module 3.2.5 and earlier for the Apache HTTP
  Server allows remote attackers to execute arbitrary SQL commands
  via the user field.

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5
    for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM
    Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows
    use an improper encryption algorithm and a weak key for maintaining
    the stored data of the node secret for the SecurID Authentication
    API, which allows local users to obtain sensitive information via
    cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication
    Agent 7.1 before 7.1.1 for Web for Internet Information Services,
    and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to
    inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2023-45802

  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a
    time window were the request's memory resources were not reclaimed
    immediately. Instead, de-allocation was deferred to connection
    close. A client could send new requests and resets, keeping the
    connection busy and open and causing the memory footprint to keep
    on growing. On connection close, all resources were reclaimed, but
    the process might run out of memory before that.This was found by
    the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset
    Exploit) with their own test client. During "normal" HTTP/2 use, the
    probability to hit this bug is very low. The kept memory would not
    become noticeable before the connection closes or times out.Users are
    recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-28615

  - CVSS Score: 6.4
  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose
    information due to a read beyond bounds in ap_strcmp_match() when
    provided with an extremely large input buffer. While no code
    distributed with the server can be coerced into such a call,
    third-party modules or lua scripts that use ap_strcmp_match() may
    hypothetically be affected.

- Vulnerability: CVE-2022-28614

  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier
    may read unintended memory if an attacker can cause the server to
    reflect very large input using ap_rwrite() or ap_rputs(), such as
    with mod_luas r:puts() function. Modules compiled and distributed
    separately from Apache HTTP Server that use the 'ap_rputs' function
    and may pass it a very large (INT_MAX or larger) string must be
    compiled against current headers to resolve the issue.

11.17   IP Address: 159.149.53.191

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 2

- High Vulnerabilities: 11

- Medium Vulnerabilities: 82

- Low Vulnerabilities: 8

- Total Vulnerabilities: 103

Services Running on IP Address

- Service: N/A

    - Port: 443
    - Version: N/A
    - Location:

Vulnerabilities Found

- Vulnerability: CVE-2014-0117

    - CVSS Score: 4.3
    - Description: The mod_proxy module in the Apache HTTP Server 2.4.x before 2.4.10, when a reverse proxy is enabled, allows remote attackers to cause a denial of service (child-process crash) via a crafted HTTP Connection header.

- Vulnerability: CVE-2017-7679

    - CVSS Score: 7.5
    - Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

- Vulnerability: CVE-2017-9798

    - CVSS Score: 5
    - Description: Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.

- Vulnerability: CVE-2015-3185

    - CVSS Score: 4.3
    - Description: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

- Vulnerability: CVE-2015-3184

  - CVSS Score: 5
  - Description: mod_authz_svn in Apache Subversion 1.7.x before 1.7.21 and 1.8.x before 1.8.14, when using Apache httpd 2.4.x, does not properly restrict anonymous access, which allows remote anonymous users to read hidden files via the path name.

- Vulnerability: CVE-2015-3183

  - CVSS Score: 5
  - Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

- Vulnerability: CVE-2013-4365

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2018-5407

  - CVSS Score: 1.9
  - Description: Simultaneous Multi-threading (SMT) in processors can enable local users to exploit software vulnerable to timing attacks via a side-channel timing attack on 'port contention'.

- Vulnerability: CVE-2022-28330

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2021-32791

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2021-32792

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.

- Vulnerability: CVE-2024-38476

- CVSS Score: N/A
- Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- **Vulnerability: CVE-2024-38477**

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- **Vulnerability: CVE-2023-31122**

  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- **Vulnerability: CVE-2009-0796**

  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- **Vulnerability: CVE-2022-2068**

  - CVSS Score: 10
  - Description: In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze).

- **Vulnerability: CVE-2014-0118**

  - CVSS Score: 4.3
  - Description: The deflate_in_filter function in mod_deflate.c in the mod_deflate module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.

- **Vulnerability: CVE-2013-6438**

  - CVSS Score: 5

- Description: The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.

- Vulnerability: CVE-2020-1927

  - CVSS Score: 5.8
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.

- Vulnerability: CVE-2023-0286

  - CVSS Score: N/A
  - Description: There is a type confusion vulnerability relating to X.400 address processinginside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING butthe public structure definition for GENERAL_NAME incorrectly specified the typeof the x400Address field as ASN1_TYPE. This field is subsequently interpreted bythe OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than anASN1_STRING.When CRL checking is enabled (i.e. the application sets theX509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to passarbitrary pointers to a memcmp call, enabling them to read memory contents orenact a denial of service. In most cases, the attack requires the attacker toprovide both the certificate chain and CRL, neither of which need to have avalid signature. If the attacker only controls one of these inputs, the otherinput must already contain an X.400 address as a CRL distribution point, whichis uncommon. As such, this vulnerability is most likely to only affectapplications which have implemented their own functionality for retrieving CRLsover a network.

- Vulnerability: CVE-2023-3817

  - CVSS Score: N/A
  - Description: Issue summary: Checking excessively long DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH key or DH parameters may experience longdelays. Where the key or parameters that are being checked have been obtainedfrom an untrusted source this may lead to a Denial of Service.The function DH_check() performs various checks on DH parameters. After fixingCVE-2023-3446 it was discovered that a large q parameter value can also triggeran overly long computation during some of these checks. A correct q value,if present, cannot be larger than the modulus p parameter, thus it isunnecessary to perform these checks if q is larger than p.An application that calls DH_check() and supplies a key or parameters obtainedfrom an untrusted source could be vulnerable to a Denial of Service attack.The function DH_check() is itself called by a number of other OpenSSL functions.An application calling any of those other functions may similarly be affected.The other functions affected by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable are the OpenSSL dhparam and pkeyparam command line applicationswhen using the "-check" option.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2017-3167

- CVSS Score: 7.5
- Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.

- Vulnerability: CVE-2021-32786

  - CVSS Score: 5.8
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, 'oidc_validate_redirect_url()' does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring 'mod_auth_openidc' to only allow redirection whose destination matches a given regular expression.

- Vulnerability: CVE-2021-32785

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache ('OIDCCacheEncrypt off', 'OIDCSessionType server-cache', 'OIDCCacheType redis'), 'mod_auth_openidc' wrongly performed argument interpolation before passing Redis requests to 'hiredis', which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the 'hiredis' API. As a workaround, this vulnerability can be mitigated by setting 'OIDCCacheEncrypt' to 'on', as cache keys are cryptographically hashed before use when this option is enabled.

- Vulnerability: CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2021-44790

  - CVSS Score: 7.5
  - Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

- Vulnerability: CVE-2016-4975

  – CVSS Score: 4.3
  – Description: Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).

- Vulnerability: CVE-2020-13938

  – CVSS Score: 2.1
  – Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

- Vulnerability: CVE-2023-2650

  – CVSS Score: N/A
  – Description: Issue summary: Processing some specially crafted ASN.1 object identifiers ordata containing them may be very slow.Impact summary: Applications that use OBJ_obj2txt() directly, or use any ofthe OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no messagesize limit may experience notable to very long delays when processing thosemessages, which may lead to a Denial of Service.An OBJECT IDENTIFIER is composed of a series of numbers – sub-identifiers -most of which have no size limit. OBJ_obj2txt() may be used to translatean ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSLtype ASN1_OBJECT) to its canonical numeric text form, which are thesub-identifiers of the OBJECT IDENTIFIER in decimal form, separated byperiods.When one of the sub-identifiers in the OBJECT IDENTIFIER is very large(these are sizes that are seen as absurdly large, taking up tens or hundredsof KiBs), the translation to a decimal number in text may take a very longtime. The time complexity is $O(n^2)$ with 'n' being the size of thesub-identifiers in bytes (*).With OpenSSL 3.0, support to fetch cryptographic algorithms using names /identifiers in string form was introduced. This includes using OBJECTIDENTIFIERs in canonical numeric text form as identifiers for fetchingalgorithms.Such OBJECT IDENTIFIERs may be received through the ASN.1 structureAlgorithmIdentifier, which is commonly used in multiple protocols to specifywhat cryptographic algorithm should be used to sign or verify, encrypt ordecrypt, or digest passed data.Applications that call OBJ_obj2txt() directly with untrusted data areaffected, with any version of OpenSSL. If the use is for the mere purposeof display, the severity is considered low.In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME,CMS, CMP/CRMF or TS. It also impacts anything that processes X.509certificates, including simple things like verifying its signature.The impact on TLS is relatively low, because all versions of OpenSSL have a100KiB limit on the peer's certificate chain. Additionally, this onlyimpacts clients, or servers that have explicitly enabled clientauthentication.In OpenSSL 1.1.1 and 1.0.2, this only affects displaying diverse objects,such as X.509 certificates. This is assumed to not happen in such a waythat it would cause a Denial of Service, so these versions are considerednot affected by this issue in such a way that it would be cause for concern,and the severity is therefore considered low.

- Vulnerability: CVE-2023-0215

  – CVSS Score: N/A

- Description: The public API function BIO_new_NDEF is a helper function used for streamingASN.1 data via a BIO. It is primarily used internally to OpenSSL to support theSMIME, CMS and PKCS7 streaming capabilities, but may also be called directly byend user applications.The function receives a BIO from the caller, prepends a new BIO_f_asn1 filterBIO onto the front of it to form a BIO chain, and then returns the new head ofthe BIO chain to the caller. Under certain conditions, for example if a CMSrecipient public key is invalid, the new filter BIO is freed and the functionreturns a NULL result indicating a failure. However, in this case, the BIO chainis not properly cleaned up and the BIO passed by the caller still retainsinternal pointers to the previously freed filter BIO. If the caller then goes onto call BIO_pop() on the BIO then a use-after-free will occur. This will mostlikely result in a crash.This scenario occurs directly in the internal function B64_write_ASN1() whichmay cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() onthe BIO. This internal function is in turn called by the public API functionsPEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream,SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7.Other public API functions that may be impacted by this includei2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream andi2d_PKCS7_bio_stream.The OpenSSL cms and smime command line applications are similarly affected.

- Vulnerability: CVE-2020-35452

  - CVSS Score: 6.8
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

- Vulnerability: CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2020-1934

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

- Vulnerability: CVE-2022-36760

  - CVSS Score: N/A
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-4304

  - CVSS Score: N/A

- Description: A timing based side channel exists in the OpenSSL RSA Decryption implementationwhich could be sufficient to recover a plaintext across a network in aBleichenbacher style attack. To achieve a successful decryption an attackerwould have to be able to send a very large number of trial messages fordecryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5,RSA-OEAP and RSASVE.For example, in a TLS connection, RSA is commonly used by a client to send anencrypted pre-master secret to the server. An attacker that had observed agenuine connection between a client and a server could use this flaw to sendtrial messages to the server and record the time taken to process them. After asufficiently large number of messages the attacker could recover the pre-mastersecret used for the original connection and thus be able to decrypt theapplication data sent over that connection.

- **Vulnerability: CVE-2019-1563**

  - CVSS Score: 4.3

  - Description: In situations where an attacker receives automated notification of the success or failure of a decryption attempt an attacker, after sending a very large number of messages to be decrypted, can recover a CMS/PKCS7 transported encryption key or decrypt any RSA encrypted message that was encrypted with the public RSA key, using a Bleichenbacher padding oracle attack. Applications are not affected if they use a certificate together with the private RSA key to the CMS_decrypt or PKCS7_decrypt functions to select the correct recipient info to decrypt. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).

- **Vulnerability: CVE-2014-3523**

  - CVSS Score: 5

  - Description: Memory leak in the winnt_accept function in server/mpm/winnt/child.c in the WinNT MPM in the Apache HTTP Server 2.4.x before 2.4.10 on Windows, when the default AcceptFilter is enabled, allows remote attackers to cause a denial of service (memory consumption) via crafted requests.

- **Vulnerability: CVE-2013-5704**

  - CVSS Score: 5

  - Description: The mod_headers module in the Apache HTTP Server 2.2.22 allows remote attackers to bypass "RequestHeader unset" directives by placing a header in the trailer portion of data sent with chunked transfer coding. NOTE: the vendor states "this is not a security issue in httpd as such."

- **Vulnerability: CVE-2019-17567**

  - CVSS Score: 5

  - Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

- **Vulnerability: CVE-2022-31813**

  - CVSS Score: 7.5

– Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-*
headers to the origin server based on client side Connection
header hop-by-hop mechanism. This may be used to bypass IP based
authentication on the origin server/application.

• Vulnerability: CVE-2012-4360

– CVSS Score: 4.3
– Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module
0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote
attackers to inject arbitrary web script or HTML via unspecified
vectors.

• Vulnerability: CVE-2014-0231

– CVSS Score: 5
– Description: The mod_cgid module in the Apache HTTP Server before 2.4.10 does not
have a timeout mechanism, which allows remote attackers to cause a
denial of service (process hang) via a request to a CGI script that
does not read from its stdin file descriptor.

• Vulnerability: CVE-2021-26690

– CVSS Score: 5
– Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted
Cookie header handled by mod_session can cause a NULL pointer
dereference and crash, leading to a possible Denial Of Service

• Vulnerability: CVE-2021-26691

– CVSS Score: 7.5
– Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted
SessionHeader sent by an origin server could cause a heap overflow

• Vulnerability: CVE-2019-0220

– CVSS Score: 5
– Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38.
When the path component of a request URL contains multiple
consecutive slashes ('/'), directives such as LocationMatch and
RewriteRule must account for duplicates in regular expressions while
other aspects of the servers processing will implicitly collapse
them.

• Vulnerability: CVE-2022-30556

– CVSS Score: 5
– Description: Apache HTTP Server 2.4.53 and earlier may return lengths to
applications calling r:wsread() that point past the end of the
storage allocated for the buffer.

• Vulnerability: CVE-2021-39275

– CVSS Score: 7.5
– Description: ap_escape_quotes() may write beyond the end of a buffer when given
malicious input. No included modules pass untrusted data to these
functions, but third-party / external modules may. This issue
affects Apache HTTP Server 2.4.48 and earlier.

• Vulnerability: CVE-2014-3581

– CVSS Score: 5

– Description: The cache_merge_headers_out function in modules/cache/cache_util.c in the mod_cache module in the Apache HTTP Server before 2.4.11 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty HTTP Content-Type header.

- Vulnerability: CVE-2016-0736

    – CVSS Score: 5

    – Description: In Apache HTTP Server versions 2.4.0 to 2.4.23, mod_session_crypto was encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This made it vulnerable to padding oracle attacks, particularly with CBC.

- Vulnerability: CVE-2022-29404

    – CVSS Score: 5

    – Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2018-1312

    – CVSS Score: 6.8

    – Description: In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

- Vulnerability: CVE-2006-20001

    – CVSS Score: N/A

    – Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2017-15710

    – CVSS Score: 5

    – Description: In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.

- Vulnerability: CVE-2014-0226

    – CVSS Score: 6.8

- Description: Race condition in the mod_status module in the Apache HTTP Server
before 2.4.10 allows remote attackers to cause a denial of
service (heap-based buffer overflow), or possibly obtain sensitive
credential information or execute arbitrary code, via a crafted
request that triggers improper scoreboard handling within the
status_handler function in modules/generators/mod_status.c and the
lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

- **Vulnerability:** CVE-2024-0727

  - CVSS Score: N/A

  - Description: Issue summary: Processing a maliciously formatted PKCS12 file
may lead OpenSSLto crash leading to a potential Denial of Service
attackImpact summary: Applications loading files in the PKCS12
format from untrustedsources might terminate abruptly.A file in
PKCS12 format can contain certificates and keys and may come from
anuntrusted source. The PKCS12 specification allows certain fields
to be NULL, butOpenSSL does not correctly check for this case.
This can lead to a NULL pointerdereference that results in OpenSSL
crashing. If an application processes PKCS12files from an untrusted
source using the OpenSSL APIs then that application willbe vulnerable
to this issue.OpenSSL APIs that are vulnerable to this are:
PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(),
PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a
similar issue in SMIME_write_PKCS7(). However since thisfunction
is related to writing data we do not consider it security
significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected
by this issue.

- **Vulnerability:** CVE-2009-3766

  - CVSS Score: 6.8

  - Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when
OpenSSL is used, does not verify the domain name in the subject's
Common Name (CN) field of an X.509 certificate, which allows
man-in-the-middle attackers to spoof SSL servers via an arbitrary
valid certificate.

- **Vulnerability:** CVE-2009-3767

  - CVSS Score: 4.3

  - Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other
versions, when OpenSSL is used, does not properly handle a '\{}0'
character in a domain name in the subject's Common Name (CN) field
of an X.509 certificate, which allows man-in-the-middle attackers
to spoof arbitrary SSL servers via a crafted certificate issued by a
legitimate Certification Authority, a related issue to CVE-2009-2408.

- **Vulnerability:** CVE-2009-3765

  - CVSS Score: 6.8

  - Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does
not properly handle a '\{}0' character in a domain name in the
subject's Common Name (CN) field of an X.509 certificate, which
allows man-in-the-middle attackers to spoof arbitrary SSL servers via
a crafted certificate issued by a legitimate Certification Authority,
a related issue to CVE-2009-2408.

- **Vulnerability:** CVE-2022-22721

  - CVSS Score: 5.8

- Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

• Vulnerability: CVE-2022-22720

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

• Vulnerability: CVE-2019-10092

  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

• Vulnerability: CVE-2021-3712

  - CVSS Score: 5.8
  - Description: ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own "d2i" functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the "data" and "length" fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the "data" field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). It can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y).

• Vulnerability: CVE-2023-0464

- CVSS Score: N/A
- Description: A security vulnerability has been identified in all supported versionsof OpenSSL related to the verification of X.509 certificate chainsthat include policy constraints. Attackers may be able to exploit thisvulnerability by creating a malicious certificate chain that triggersexponential use of computational resources, leading to a denial-of-service(DoS) attack on affected systems.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0465

  - CVSS Score: N/A
  - Description: Applications that use a non-default option when verifying certificates may bevulnerable to an attack from a malicious CA to circumvent certain checks.Invalid certificate policies in leaf certificates are silently ignored byOpenSSL and other certificate policy checks are skipped for that certificate.A malicious CA could use this to deliberately assert invalid certificate policiesin order to circumvent policy checking on the certificate altogether.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.

- Vulnerability: CVE-2023-0466

  - CVSS Score: N/A
  - Description: The function X509_VERIFY_PARAM_add0_policy() is documented toimplicitly enable the certificate policy check when doing certificateverification. However the implementation of the function does notenable the check which allows certificates with invalid or incorrectpolicies to pass the certificate verification.As suddenly enabling the policy check could break existing deployments it wasdecided to keep the existing behavior of the X509_VERIFY_PARAM_add0_policy()function.Instead the applications that require OpenSSL to perform certificatepolicy check need to use X509_VERIFY_PARAM_set1_policies() or explicitlyenable the policy check by calling X509_VERIFY_PARAM_set_flags() withthe X509_V_FLAG_POLICY_CHECK flag argument.Certificate policy checks are disabled by default in OpenSSL and are notcommonly used by applications.

- Vulnerability: CVE-2019-10098

  - CVSS Score: 5.8
  - Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.

- Vulnerability: CVE-2015-0228

  - CVSS Score: 5
  - Description: The lua_websocket_read function in lua_request.c in the mod_lua module in the Apache HTTP Server through 2.4.12 allows remote attackers to cause a denial of service (child-process crash) by sending a crafted WebSocket Ping frame after a Lua script has called the wsupgrade function.

- Vulnerability: CVE-2016-5387

- CVSS Score: 6.8
- Description: The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.

• Vulnerability: CVE-2017-15715

- CVSS Score: 6.8
- Description: In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.

• Vulnerability: CVE-2021-40438

- CVSS Score: 6.8
- Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

• Vulnerability: CVE-2011-1176

- CVSS Score: 4.3
- Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

• Vulnerability: CVE-2022-23943

- CVSS Score: 7.5
- Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

• Vulnerability: CVE-2018-17199

- CVSS Score: 5
- Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

• Vulnerability: CVE-2021-23841

- CVSS Score: 4.3

– Description: The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack. The function X509_issuer_and_serial_hash() is never directly called by OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on certificates that may have been obtained from untrusted sources. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2018-1301

    – CVSS Score: 4.3
    – Description: A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.

- Vulnerability: CVE-2018-1302

    – CVSS Score: 4.3
    – Description: When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.

- Vulnerability: CVE-2018-1303

    – CVSS Score: 5
    – Description: A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache. The vulnerability is considered as low risk since mod_cache_socache is not widely used, mod_cache_disk is not concerned by this vulnerability.

- Vulnerability: CVE-2021-34798

    – CVSS Score: 5
    – Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2023-25690

    – CVSS Score: N/A

- Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- **Vulnerability: CVE-2020-11985**

  - CVSS Score: 4.3
  - Description: IP address spoofing when proxying using mod_remoteip and mod_rewrite For configurations using proxying with mod_remoteip and certain mod_rewrite rules, an attacker could spoof their IP address for logging and PHP scripts. Note this issue was fixed in Apache HTTP Server 2.4.24 but was retrospectively allocated a low severity CVE in 2020.

- **Vulnerability: CVE-2021-4160**

  - CVSS Score: 4.3
  - Description: There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that is available to premium support customers only. It will be made available in 1.0.2zc when it is released. The issue only affects OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0). Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL 1.0.2zc-dev (Affected 1.0.2-1.0.2zb).

- **Vulnerability: CVE-2013-4352**

  - CVSS Score: 4.3
  - Description: The cache_invalidate function in modules/cache/cache_storage.c in the mod_cache module in the Apache HTTP Server 2.4.6, when a caching forward proxy is enabled, allows remote HTTP servers to cause a denial of service (NULL pointer dereference and daemon crash) via vectors that trigger a missing hostname value.

- **Vulnerability: CVE-2022-26377**

  - CVSS Score: 5

– Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

• Vulnerability: CVE-2014-0098

  – CVSS Score: 5
  – Description: The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.

• Vulnerability: CVE-2016-8743

  – CVSS Score: 5
  – Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

• Vulnerability: CVE-2024-40898

  – CVSS Score: N/A
  – Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

• Vulnerability: CVE-2024-38474

  – CVSS Score: N/A
  – Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

• Vulnerability: CVE-2022-0778

  – CVSS Score: 5

- Description: The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - TLS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

- Vulnerability: CVE-2020-1971

  - CVSS Score: 4.3

– Description: The X.509 GeneralName type is a generic type for representing
different types of names. One of those name types is known as
EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which
compares different instances of a GENERAL_NAME to see if they
are equal or not. This function behaves incorrectly when both
GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference
and a crash may occur leading to a possible denial of service
attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two
purposes: 1) Comparing CRL distribution point names between an
available CRL and a CRL distribution point embedded in an X509
certificate 2) When verifying that a timestamp response token signer
matches the timestamp authority name (exposed via the API functions
TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can
control both items being compared then that attacker could trigger
a crash. For example if the attacker can trick a client or server
into checking a malicious certificate against a malicious CRL then
this may occur. Note that some applications automatically download
CRLs based on a URL embedded in a certificate. This checking happens
prior to the signatures on the certificate and CRL being verified.
OpenSSL's s_server, s_client and verify tools have support for the
"-crl_download" option which implements automatic CRL downloading and
this attack has been demonstrated to work against those tools. Note
that an unrelated bug means that affected versions of OpenSSL cannot
parse or construct correct encodings of EDIPARTYNAME. However it is
possible to construct a malformed EDIPARTYNAME that OpenSSL's parser
will accept and hence trigger this attack. All OpenSSL 1.1.1 and
1.0.2 versions are affected by this issue. Other OpenSSL releases
are out of support and have not been checked. Fixed in OpenSSL
1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected
1.0.2-1.0.2w).

- **Vulnerability: CVE-2009-1390**

  – CVSS Score: 6.8
  – Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2)
GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS
certificate in the chain is accepted instead of verifying the entire
chain, which allows remote attackers to spoof trusted servers via a
man-in-the-middle attack.

- **Vulnerability: CVE-2012-3526**

  – CVSS Score: 5
  – Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the
Apache HTTP Server allows remote attackers to cause a denial of
service (server or application crash) via multiple X-Forwarded-For
headers in a request.

- **Vulnerability: CVE-2023-5678**

  – CVSS Score: N/A

- Description: Issue summary: Generating excessively long X9.42 DH keys or checkingexcessively long X9.42 DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_generate_key() togenerate an X9.42 DH key may experience long delays. Likewise, applicationsthat use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check()to check an X9.42 DH key or X9.42 DH parameters may experience long delays.Where the key or parameters that are being checked have been obtained froman untrusted source this may lead to a Denial of Service.While DH_check() performs all the necessary checks (as of CVE-2023-3817),DH_check_pub_key() doesn't make any of these checks, and is thereforevulnerable for excessively large P and Q parameters.Likewise, while DH_generate_key() performs a check for an excessively largeP, it doesn't check for an excessively large Q.An application that calls DH_generate_key() or DH_check_pub_key() andsupplies a key or parameters obtained from an untrusted source could bevulnerable to a Denial of Service attack.DH_generate_key() and DH_check_pub_key() are also called by a number ofother OpenSSL functions. An application calling any of those otherfunctions may similarly be affected. The other functions affected by thisare DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate().Also vulnerable are the OpenSSL pkey command line application when using the"-pubcheck" option, as well as the OpenSSL genpkey command line application.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2017-3736

  - CVSS Score: 4
  - Description: There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

- Vulnerability: CVE-2017-3737

  - CVSS Score: 4.3

- Description: OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.

- Vulnerability: CVE-2019-1547

  - CVSS Score: 1.9

  - Description: Normally in OpenSSL EC groups always have a co-factor present and this is used in side channel resistant code paths. However, in some cases, it is possible to construct a group using explicit parameters (instead of using a named curve). In those cases it is possible that such a group does not have the cofactor present. This can occur even where all the parameters match a known named curve. If such a curve is used then OpenSSL falls back to non-side channel resistant code paths which may result in full key recovery during an ECDSA signature operation. In order to be vulnerable an attacker would have to have the ability to time the creation of a large number of signatures where explicit parameters with no co-factor present are in use by an application using libcrypto. For the avoidance of doubt libssl is not vulnerable because explicit parameters are never used. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).

- Vulnerability: CVE-2017-3735

  - CVSS Score: 5

  - Description: While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL before 1.0.2m and 1.1.0g.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5

  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2022-1292

  - CVSS Score: 10

- Description: The c_rehash script does not properly sanitise shell metacharacters
to prevent command injection. This script is distributed by
some operating systems in a manner where it is automatically
executed. On such operating systems, an attacker could execute
arbitrary commands with the privileges of the script. Use of the
c_rehash script is considered obsolete and should be replaced by the
OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected
3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n).
Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).

- Vulnerability: CVE-2017-3738

  - CVSS Score: 4.3
  - Description: There is an overflow bug in the AVX2 Montgomery multiplication
procedure used in exponentiation with 1024-bit moduli. No EC
algorithms are affected. Analysis suggests that attacks against
RSA and DSA as a result of this defect would be very difficult to
perform and are not believed likely. Attacks against DH1024 are
considered just feasible, because most of the work necessary to
deduce information about a private key may be performed offline. The
amount of resources required for such an attack would be significant.
However, for an attack on TLS to be meaningful, the server would have
to share the DH1024 private key among multiple clients, which is no
longer an option since CVE-2016-0701. This only affects processors
that support the AVX2 but not ADX extensions like Intel Haswell
(4th generation). Note: The impact from this issue is similar to
CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version
1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n.
Due to the low severity of this issue we are not issuing a new
release of OpenSSL 1.1.0 at this time. The fix will be included in
OpenSSL 1.1.0h when it becomes available. The fix is also available
in commit e502cc86d in the OpenSSL git repository.

- Vulnerability: CVE-2012-4001

  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server
does not properly verify its host name, which allows remote attackers
to trigger HTTP requests to arbitrary hosts via unspecified vectors,
as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2022-37436

  - CVSS Score: N/A
  - Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause
the response headers to be truncated early, resulting in some headers
being incorporated into the response body. If the later headers have
any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2021-23840

  - CVSS Score: 5

– Description: Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissable length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

- Vulnerability: CVE-2018-0737

  – CVSS Score: 4.3

  – Description: The OpenSSL RSA Key generation algorithm has been shown to be vulnerable to a cache timing side channel attack. An attacker with sufficient access to mount cache timing attacks during the RSA key generation process could recover the private key. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2b-1.0.2o).

- Vulnerability: CVE-2018-0734

  – CVSS Score: 4.3

  – Description: The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.1a (Affected 1.1.1). Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.0.2q (Affected 1.0.2-1.0.2p).

- Vulnerability: CVE-2018-0732

  – CVSS Score: 5

  – Description: During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime value to the client. This will cause the client to spend an unreasonably long period of time generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2-1.0.2o).

- Vulnerability: CVE-2017-9788

  – CVSS Score: 6.4

  – Description: In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.

- Vulnerability: CVE-2018-0739

  – CVSS Score: 4.3

- Description: Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o (Affected 1.0.2b-1.0.2n).

- Vulnerability: CVE-2014-8109

  - CVSS Score: 4.3
  - Description: mod_lua.c in the mod_lua module in the Apache HTTP Server 2.3.x and 2.4.x through 2.4.10 does not support an httpd configuration in which the same Lua authorization provider is used with different arguments within different contexts, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives, as demonstrated by a configuration that specifies authorization for one group to access a certain directory, and authorization for a second group to access a second directory.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2016-2161

  - CVSS Score: 5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.23, malicious input to mod_auth_digest can cause the server to crash, and each instance continues to crash even for subsequently valid requests.

- Vulnerability: CVE-2016-8612

  - CVSS Score: 3.3
  - Description: Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.

- Vulnerability: CVE-2019-1552

  - CVSS Score: 1.9

- Description: OpenSSL has internal defaults for a directory tree where it
  can find a configuration file as well as certificates used for
  verification in TLS. This directory is most commonly referred to
  as OPENSSLDIR, and is configurable with the --prefix / --openssldir
  configuration options. For OpenSSL versions 1.1.0 and 1.1.1, the
  mingw configuration targets assume that resulting programs and
  libraries are installed in a Unix-like environment and the default
  prefix for program installation as well as for OPENSSLDIR should be
  '/usr/local'. However, mingw programs are Windows programs, and as
  such, find themselves looking at sub-directories of 'C:/usr/local',
  which may be world writable, which enables untrusted users to modify
  OpenSSL's default configuration, insert CA certificates, modify (or
  even replace) existing engine modules, etc. For OpenSSL 1.0.2,
  '/usr/local/ssl' is used as default for OPENSSLDIR on all Unix and
  Windows targets, including Visual C builds. However, some build
  instructions for the diverse Windows targets on 1.0.2 encourage
  you to specify your own --prefix. OpenSSL versions 1.1.1, 1.1.0
  and 1.0.2 are affected by this issue. Due to the limited scope
  of affected deployments this has been assessed as low severity and
  therefore we are not creating new releases at this time. Fixed
  in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL
  1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected
  1.0.2-1.0.2s).

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5
    for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM
    Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows
    use an improper encryption algorithm and a weak key for maintaining
    the stored data of the node secret for the SecurID Authentication
    API, which allows local users to obtain sensitive information via
    cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication
    Agent 7.1 before 7.1.1 for Web for Internet Information Services,
    and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to
    inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2019-1551

  - CVSS Score: 5
  - Description: There is an overflow bug in the x64_64 Montgomery squaring procedure
    used in exponentiation with 512-bit moduli. No EC algorithms are
    affected. Analysis suggests that attacks against 2-prime RSA1024,
    3-prime RSA1536, and DSA1024 as a result of this defect would be
    very difficult to perform and are not believed likely. Attacks
    against DH512 are considered just feasible. However, for an attack
    the target would have to re-use the DH512 private key, which is not
    recommended anyway. Also applications directly using the low level
    API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME. Fixed
    in OpenSSL 1.1.1e (Affected 1.1.1-1.1.1d). Fixed in OpenSSL 1.0.2u
    (Affected 1.0.2-1.0.2t).

- Vulnerability: CVE-2019-1559

  - CVSS Score: 4.3

– Description: If an application encounters a fatal protocol error and then calls
SSL_shutdown() twice (once to send a close_notify, and once to
receive one) then OpenSSL can respond differently to the calling
application if a 0 byte record is received with invalid padding
compared to if a 0 byte record is received with an invalid MAC. If
the application then behaves differently based on that in a way that
is detectable to the remote peer, then this amounts to a padding
oracle that could be used to decrypt data. In order for this to be
exploitable "non-stitched" ciphersuites must be in use. Stitched
ciphersuites are optimised implementations of certain commonly
used ciphersuites. Also the application must call SSL_shutdown()
twice even if a protocol error has occurred (applications should
not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected
1.0.2-1.0.2q).

- Vulnerability: CVE-2023-45802

    – CVSS Score: N/A

    – Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a
time window were the request's memory resources were not reclaimed
immediately. Instead, de-allocation was deferred to connection
close. A client could send new requests and resets, keeping the
connection busy and open and causing the memory footprint to keep
on growing. On connection close, all resources were reclaimed, but
the process might run out of memory before that.This was found by
the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset
Exploit) with their own test client. During "normal" HTTP/2 use, the
probability to hit this bug is very low. The kept memory would not
become noticeable before the connection closes or times out.Users are
recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2018-1283

    – CVSS Score: 3.5

    – Description: In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to
forward its session data to CGI applications (SessionEnv on, not
the default), a remote user may influence their content by using a
"Session" header. This comes from the "HTTP_SESSION" variable name
used by mod_session to forward its data to CGIs, since the prefix
"HTTP_" is also used by the Apache HTTP Server to pass HTTP header
fields, per CGI specifications.

- Vulnerability: CVE-2020-1968

    – CVSS Score: 4.3

    – Description: The Raccoon attack exploits a flaw in the TLS specification which
can lead to an attacker being able to compute the pre-master
secret in connections which have used a Diffie-Hellman (DH) based
ciphersuite. In such a case this would result in the attacker being
able to eavesdrop on all encrypted communications sent over that TLS
connection. The attack can only be exploited if an implementation
re-uses a DH secret across multiple TLS connections. Note that this
issue only impacts DH ciphersuites and not ECDH ciphersuites. This
issue affects OpenSSL 1.0.2 which is out of support and no longer
receiving public updates. OpenSSL 1.1.1 is not vulnerable to this
issue. Fixed in OpenSSL 1.0.2w (Affected 1.0.2-1.0.2v).

- Vulnerability: CVE-2019-0217

    – CVSS Score: 6

– Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition
                in mod_auth_digest when running in a threaded server could allow a
                user with valid credentials to authenticate using another username,
                bypassing configured access control restrictions.

- Vulnerability: CVE-2022-28615

  – CVSS Score: 6.4

  – Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose
                  information due to a read beyond bounds in ap_strcmp_match() when
                  provided with an extremely large input buffer. While no code
                  distributed with the server can be coerced into such a call,
                  third-party modules or lua scripts that use ap_strcmp_match() may
                  hypothetically be affected.

- Vulnerability: CVE-2022-28614

  – CVSS Score: 5

  – Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier
                  may read unintended memory if an attacker can cause the server to
                  reflect very large input using ap_rwrite() or ap_rputs(), such as
                  with mod_luas r:puts() function. Modules compiled and distributed
                  separately from Apache HTTP Server that use the 'ap_rputs' function
                  and may pass it a very large (INT_MAX or larger) string must be
                  compiled against current headers to resolve the issue.

11.18 IP Address: 159.149.119.18

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 1

- High Vulnerabilities: 13

- Medium Vulnerabilities: 81

- Low Vulnerabilities: 7

- Total Vulnerabilities: 102

Services Running on IP Address

- Service: Apache httpd

  – Port: 80
  – Version: 2.2.26
  – Location: /

- Service: Heimdal Kerberos

  – Port: 88
  – Version: N/A
  – Location:

- Service: Apple remote desktop vnc

  – Port: 5900
  – Version: N/A
  – Location:

Vulnerabilities Found

- Vulnerability: CVE-2012-0027

  – CVSS Score: 5
  – Description: The GOST ENGINE in OpenSSL before 1.0.0f does not properly handle invalid parameters for the GOST block cipher, which allows remote attackers to cause a denial of service (daemon crash) via crafted data from a TLS client.

- Vulnerability: CVE-2017-7679

  – CVSS Score: 7.5
  – Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

- Vulnerability: CVE-2017-9798

  – CVSS Score: 5
  – Description: Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.

846

- Vulnerability: CVE-2015-3183

  – CVSS Score: 5
  – Description: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

- Vulnerability: CVE-2013-4365

  – CVSS Score: 7.5
  – Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2021-32785

  – CVSS Score: 4.3
  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache (‘OIDCCacheEncrypt off‘, ‘OIDCSessionType server-cache‘, ‘OIDCCacheType redis‘), ‘mod_auth_openidc‘ wrongly performed argument interpolation before passing Redis requests to ‘hiredis‘, which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the ‘hiredis‘ API. As a workaround, this vulnerability can be mitigated by setting ‘OIDCCacheEncrypt‘ to ‘on‘, as cache keys are cryptographically hashed before use when this option is enabled.

- Vulnerability: CVE-2016-2176

  – CVSS Score: 6.4
  – Description: The X509_NAME_oneline function in crypto/x509/x509_obj.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to obtain sensitive information from process stack memory or cause a denial of service (buffer over-read) via crafted EBCDIC ASN.1 data.

- Vulnerability: CVE-2021-32791

  – CVSS Score: 4.3
  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2021-32792

  – CVSS Score: 4.3

— Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.

- Vulnerability: CVE-2023-31122

  — CVSS Score: N/A

  — Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2009-0796

  — CVSS Score: 2.6

  — Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2011-4108

  — CVSS Score: 4.3

  — Description: The DTLS implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f performs a MAC check only if certain padding is valid, which makes it easier for remote attackers to recover plaintext via a padding oracle attack.

- Vulnerability: CVE-2010-4252

  — CVSS Score: 7.5

  — Description: OpenSSL before 1.0.0c, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol.

- Vulnerability: CVE-2014-0118

  — CVSS Score: 4.3

  — Description: The deflate_in_filter function in mod_deflate.c in the mod_deflate module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.

- Vulnerability: CVE-2013-6438

  — CVSS Score: 5

  — Description: The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.

- Vulnerability: CVE-2011-2688

  — CVSS Score: 7.5

  — Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2016-0703

  – CVSS Score: 4.3
  – Description: The get_client_master_key function in s2_srvr.c in the SSLv2
                  implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r,
                  1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero
                  CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher,
                  which allows man-in-the-middle attackers to determine the MASTER-KEY
                  value and decrypt TLS ciphertext data by leveraging a Bleichenbacher
                  RSA padding oracle, a related issue to CVE-2016-0800.

- Vulnerability: CVE-2017-3167

  – CVSS Score: 7.5
  – Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use
                  of the ap_get_basic_auth_pw() by third-party modules outside of the
                  authentication phase may lead to authentication requirements being
                  bypassed.

- Vulnerability: CVE-2015-3195

  – CVSS Score: 5
  – Description: The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in
                  OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q,
                  and 1.0.2 before 1.0.2e mishandles errors caused by malformed
                  X509_ATTRIBUTE data, which allows remote attackers to obtain
                  sensitive information from process memory by triggering a decoding
                  failure in a PKCS#7 or CMS application.

- Vulnerability: CVE-2015-0228

  – CVSS Score: 5
  – Description: The lua_websocket_read function in lua_request.c in the mod_lua module
                  in the Apache HTTP Server through 2.4.12 allows remote attackers to
                  cause a denial of service (child-process crash) by sending a crafted
                  WebSocket Ping frame after a Lua script has called the wsupgrade
                  function.

- Vulnerability: CVE-2021-4044

  – CVSS Score: 5
  – Description: Internally libssl in OpenSSL calls X509_verify_cert() on the client
                  side to verify a certificate supplied by a server. That function
                  may return a negative return value to indicate an internal error (for
                  example out of memory). Such a negative return value is mishandled
                  by OpenSSL and will cause an IO function (such as SSL_connect() or
                  SSL_do_handshake()) to not indicate success and a subsequent call
                  to SSL_get_error() to return the value SSL_ERROR_WANT_RETRY_VERIFY.
                  This return value is only supposed to be returned by OpenSSL if the
                  application has previously called SSL_CTX_set_cert_verify_callback().
                  Since most applications do not do this the SSL_ERROR_WANT_RETRY_VERIFY
                  return value from SSL_get_error() will be totally unexpected and
                  applications may not behave correctly as a result. The exact
                  behaviour will depend on the application but it could result in
                  crashes, infinite loops or other similar incorrect responses. This
                  issue is made more serious in combination with a separate bug in
                  OpenSSL 3.0 that will cause X509_verify_cert() to indicate an internal
                  error when processing a certificate chain. This will occur where a
                  certificate does not include the Subject Alternative Name extension
                  but where a Certificate Authority has enforced name constraints.
                  This issue can occur even with valid chains. By combining the two
                  issues an attacker could induce incorrect, application dependent
                  behaviour. Fixed in OpenSSL 3.0.1 (Affected 3.0.0).

- Vulnerability: CVE-2021-32786

  – CVSS Score: 5.8

  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, 'oidc_validate_redirect_url()' does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring 'mod_auth_openidc' to only allow redirection whose destination matches a given regular expression.

- Vulnerability: CVE-2017-3169

  – CVSS Score: 7.5

  – Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.

- Vulnerability: CVE-2007-4723

  – CVSS Score: 7.5

  – Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2021-44790

  – CVSS Score: 7.5

  – Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

- Vulnerability: CVE-2016-2109

  – CVSS Score: 7.8

  – Description: The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in the ASN.1 BIO implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (memory consumption) via a short invalid encoding.

- Vulnerability: CVE-2016-2108

  – CVSS Score: 10

  – Description: The ASN.1 implementation in OpenSSL before 1.0.1o and 1.0.2 before 1.0.2c allows remote attackers to execute arbitrary code or cause a denial of service (buffer underflow and memory corruption) via an ANY field in crafted serialized data, aka the "negative zero" issue.

- Vulnerability: CVE-2016-2107

  – CVSS Score: 2.6

– Description: The AES-NI implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h does not consider memory allocation during a certain padding check, which allows remote attackers to obtain sensitive cleartext information via a padding-oracle attack against an AES CBC session. NOTE: this vulnerability exists because of an incorrect fix for CVE-2013-0169.

- Vulnerability: CVE-2016-2106

  – CVSS Score: 5
  – Description: Integer overflow in the EVP_EncryptUpdate function in crypto/evp/evp_enc.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of data.

- Vulnerability: CVE-2016-4975

  – CVSS Score: 4.3
  – Description: Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).

- Vulnerability: CVE-2022-22719

  – CVSS Score: 5
  – Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2021-34798

  – CVSS Score: 5
  – Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2013-5704

  – CVSS Score: 5
  – Description: The mod_headers module in the Apache HTTP Server 2.2.22 allows remote attackers to bypass "RequestHeader unset" directives by placing a header in the trailer portion of data sent with chunked transfer coding. NOTE: the vendor states "this is not a security issue in httpd as such."

- Vulnerability: CVE-2022-28330

  – CVSS Score: 5
  – Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2022-31813

  – CVSS Score: 7.5
  – Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

- Vulnerability: CVE-2012-4360

  – CVSS Score: 4.3

- Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2015-0287

  - CVSS Score: 5
  - Description: The ASN1_item_ex_d2i function in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not reinitialize CHOICE and ADB data structures, which might allow attackers to cause a denial of service (invalid write operation and memory corruption) by leveraging an application that relies on ASN.1 structure reuse.

- Vulnerability: CVE-2024-40898

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2010-5298

  - CVSS Score: 4
  - Description: Race condition in the ssl3_read_bytes function in s3_pkt.c in OpenSSL through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, allows remote attackers to inject data across sessions or cause a denial of service (use-after-free and parsing error) via an SSL connection in a multithreaded environment.

- Vulnerability: CVE-2014-0231

  - CVSS Score: 5
  - Description: The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.

- Vulnerability: CVE-2014-3510

  - CVSS Score: 4.3
  - Description: The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote DTLS servers to cause a denial of service (NULL pointer dereference and client application crash) via a crafted handshake message in conjunction with a (1) anonymous DH or (2) anonymous ECDH ciphersuite.

- Vulnerability: CVE-2014-8275

  - CVSS Score: 5
  - Description: OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not enforce certain constraints on certificate data, which allows remote attackers to defeat a fingerprint-based certificate-blacklist protection mechanism by including crafted data within a certificate's unsigned portion, related to crypto/asn1/a_verify.c, crypto/dsa/dsa_asn1.c, crypto/ecdsa/ecs_vrf.c, and crypto/x509/x_all.c.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5

- Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- **Vulnerability:** CVE-2021-39275

  - CVSS Score: 7.5
  - Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

- **Vulnerability:** CVE-2011-4577

  - CVSS Score: 4.3
  - Description: OpenSSL before 0.9.8s and 1.x before 1.0.0f, when RFC 3779 support is enabled, allows remote attackers to cause a denial of service (assertion failure) via an X.509 certificate containing certificate-extension data associated with (1) IP address blocks or (2) Autonomous System (AS) identifiers.

- **Vulnerability:** CVE-2011-4576

  - CVSS Score: 5
  - Description: The SSL 3.0 implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly initialize data structures for block cipher padding, which might allow remote attackers to obtain sensitive information by decrypting the padding data sent by an SSL peer.

- **Vulnerability:** CVE-2011-1945

  - CVSS Score: 2.6
  - Description: The elliptic curve cryptography (ECC) subsystem in OpenSSL 1.0.0d and earlier, when the Elliptic Curve Digital Signature Algorithm (ECDSA) is used for the ECDHE_ECDSA cipher suite, does not properly implement curves over binary fields, which makes it easier for context-dependent attackers to determine private keys via a timing attack and a lattice calculation.

- **Vulnerability:** CVE-2022-29404

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- **Vulnerability:** CVE-2006-20001

  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- **Vulnerability:** CVE-2014-3505

  - CVSS Score: 5
  - Description: Double free vulnerability in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (application crash) via crafted DTLS packets that trigger an error condition.

- **Vulnerability:** CVE-2014-3506

- CVSS Score: 5
- Description: d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via crafted DTLS handshake messages that trigger memory allocations corresponding to large length values.

- Vulnerability: CVE-2014-3507

  - CVSS Score: 5
  - Description: Memory leak in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via zero-length DTLS fragments that trigger improper handling of the return value of a certain insert function.

- Vulnerability: CVE-2014-0226

  - CVSS Score: 6.8
  - Description: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

- Vulnerability: CVE-2009-3766

  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when OpenSSL is used, does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

- Vulnerability: CVE-2009-3767

  - CVSS Score: 4.3
  - Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other versions, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2009-3765

  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2014-3508

  - CVSS Score: 4.3

– Description: The OBJ_obj2txt function in crypto/objects/obj_dat.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i, when pretty printing is used, does not ensure the presence of '\{}0' characters, which allows context-dependent attackers to obtain sensitive information from process stack memory by reading output from X509_name_oneline, X509_name_print_ex, and unspecified other functions.

- Vulnerability: CVE-2022-22721

  – CVSS Score: 5.8
  – Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2022-22720

  – CVSS Score: 7.5
  – Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2015-4000

  – CVSS Score: 4.3
  – Description: The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the "Logjam" issue.

- Vulnerability: CVE-2016-5387

  – CVSS Score: 6.8
  – Description: The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.

- Vulnerability: CVE-2021-40438

  – CVSS Score: 6.8
  – Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2011-1176

  – CVSS Score: 4.3
  – Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2015-0209

- CVSS Score: 6.8
- Description: Use-after-free vulnerability in the d2i_ECPrivateKey function in crypto/ec/ec_asn1.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via a malformed Elliptic Curve (EC) private-key file that is improperly handled during import.

- Vulnerability: CVE-2018-1301

  - CVSS Score: 4.3
  - Description: A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.

- Vulnerability: CVE-2018-1302

  - CVSS Score: 4.3
  - Description: When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.

- Vulnerability: CVE-2018-1303

  - CVSS Score: 5
  - Description: A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache. The vulnerability is considered as low risk since mod_cache_socache is not widely used, mod_cache_disk is not concerned by this vulnerability.

- Vulnerability: CVE-2015-0204

  - CVSS Score: 4.3
  - Description: The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct RSA-to-EXPORT_RSA downgrade attacks and facilitate brute-force decryption by offering a weak ephemeral RSA key in a noncompliant role, related to the "FREAK" issue. NOTE: the scope of this CVE is only client code based on OpenSSL, not EXPORT_RSA issues associated with servers or other TLS implementations.

- Vulnerability: CVE-2014-3571

  - CVSS Score: 5
  - Description: OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted DTLS message that is processed with a different read operation for the handshake header than for the handshake body, related to the dtls1_get_record function in d1_pkt.c and the ssl3_read_n function in s3_pkt.c.

- Vulnerability: CVE-2014-3570

- CVSS Score: 5
- Description: The BN_sqr implementation in OpenSSL before 0.9.8zd, 1.0.0 before
  1.0.0p, and 1.0.1 before 1.0.1k does not properly calculate
  the square of a BIGNUM value, which might make it easier for
  remote attackers to defeat cryptographic protection mechanisms
  via unspecified vectors, related to crypto/bn/asm/mips.pl,
  crypto/bn/asm/x86_64-gcc.c, and crypto/bn/bn_asm.c.

- Vulnerability: CVE-2014-3572

  - CVSS Score: 5
  - Description: The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before
    0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote
    SSL servers to conduct ECDHE-to-ECDH downgrade attacks and trigger a
    loss of forward secrecy by omitting the ServerKeyExchange message.

- Vulnerability: CVE-2016-8612

  - CVSS Score: 3.3
  - Description: Apache HTTP Server mod_cluster before version httpd 2.4.23 is
    vulnerable to an Improper Input Validation in the protocol parsing
    logic in the load balancer resulting in a Segmentation Fault in the
    serving httpd process.

- Vulnerability: CVE-2014-0098

  - CVSS Score: 5
  - Description: The log_cookie function in mod_log_config.c in the mod_log_config
    module in the Apache HTTP Server before 2.4.8 allows remote attackers
    to cause a denial of service (segmentation fault and daemon crash)
    via a crafted cookie that is not properly handled during truncation.

- Vulnerability: CVE-2016-8743

  - CVSS Score: 5
  - Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was
    liberal in the whitespace accepted from requests and sent in response
    lines and headers. Accepting these different behaviors represented a
    security concern when httpd participates in any chain of proxies or
    interacts with back-end application servers, either through mod_proxy
    or using conventional CGI mechanisms, and may result in request
    smuggling, response splitting and cache pollution.

- Vulnerability: CVE-2015-0286

  - CVSS Score: 5
  - Description: The ASN1_TYPE_cmp function in crypto/asn1/a_type.c in OpenSSL before
    0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before
    1.0.2a does not properly perform boolean-type comparisons, which
    allows remote attackers to cause a denial of service (invalid read
    operation and application crash) via a crafted X.509 certificate to
    an endpoint that uses the certificate-verification feature.

- Vulnerability: CVE-2015-0289

  - CVSS Score: 5
  - Description: The PKCS#7 implementation in OpenSSL before 0.9.8zf, 1.0.0
    before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a
    does not properly handle a lack of outer ContentInfo, which
    allows attackers to cause a denial of service (NULL pointer
    dereference and application crash) by leveraging an application
    that processes arbitrary PKCS#7 data and providing malformed
    data with ASN.1 encoding, related to crypto/pkcs7/pk7_doit.c and
    crypto/pkcs7/pk7_lib.c.

- Vulnerability: CVE-2015-0288

    - CVSS Score: 5
    - Description: The X509_to_X509_REQ function in crypto/x509/x509_req.c in OpenSSL
                    before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2
                    before 1.0.2a might allow attackers to cause a denial of service
                    (NULL pointer dereference and application crash) via an invalid
                    certificate key.

- Vulnerability: CVE-2016-7056

    - CVSS Score: 2.1
    - Description: A timing attack flaw was found in OpenSSL 1.0.1u and before that
                    could allow a malicious user with local access to recover ECDSA P-256
                    private keys.

- Vulnerability: CVE-2014-0076

    - CVSS Score: 1.9
    - Description: The Montgomery ladder implementation in OpenSSL through 1.0.0l
                    does not ensure that certain swap operations have a constant-time
                    behavior, which makes it easier for local users to obtain ECDSA
                    nonces via a FLUSH+RELOAD cache side-channel attack.

- Vulnerability: CVE-2015-1789

    - CVSS Score: 4.3
    - Description: The X509_cmp_time function in crypto/x509/x509_vfy.c in OpenSSL
                    before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2
                    before 1.0.2b allows remote attackers to cause a denial of service
                    (out-of-bounds read and application crash) via a crafted length field
                    in ASN1_TIME data, as demonstrated by an attack against a server that
                    supports client authentication with a custom verification callback.

- Vulnerability: CVE-2015-1788

    - CVSS Score: 4.3
    - Description: The BN_GF2m_mod_inv function in crypto/bn/bn_gf2m.c in OpenSSL before
                    0.9.8s, 1.0.0 before 1.0.0e, 1.0.1 before 1.0.1n, and 1.0.2 before
                    1.0.2b does not properly handle ECParameters structures in which
                    the curve is over a malformed binary polynomial field, which allows
                    remote attackers to cause a denial of service (infinite loop) via a
                    session that uses an Elliptic Curve algorithm, as demonstrated by an
                    attack against a server that supports client authentication.

- Vulnerability: CVE-2009-1390

    - CVSS Score: 6.8
    - Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2)
                    GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS
                    certificate in the chain is accepted instead of verifying the entire
                    chain, which allows remote attackers to spoof trusted servers via a
                    man-in-the-middle attack.

- Vulnerability: CVE-2012-3526

    - CVSS Score: 5
    - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the
                    Apache HTTP Server allows remote attackers to cause a denial of
                    service (server or application crash) via multiple X-Forwarded-For
                    headers in a request.

- Vulnerability: CVE-2014-3566

- CVSS Score: 4.3
- Description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

- Vulnerability: CVE-2014-3567

  - CVSS Score: 7.1
  - Description: Memory leak in the tls_decrypt_ticket function in t1_lib.c in OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted session ticket that triggers an integrity-check failure.

- Vulnerability: CVE-2017-3735

  - CVSS Score: 5
  - Description: While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL before 1.0.2m and 1.1.0g.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2014-3568

  - CVSS Score: 4.3
  - Description: OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j does not properly enforce the no-ssl3 build option, which allows remote attackers to bypass intended access restrictions via an SSL 3.0 handshake, related to s23_clnt.c and s23_srvr.c.

- Vulnerability: CVE-2015-0293

  - CVSS Score: 5
  - Description: The SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a allows remote attackers to cause a denial of service (s2_lib.c assertion failure and daemon exit) via a crafted CLIENT-MASTER-KEY message.

- Vulnerability: CVE-2012-4001

  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2022-37436

  - CVSS Score: N/A
  - Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2017-9788

  – CVSS Score: 6.4
  – Description: In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.

- Vulnerability: CVE-2015-1790

  – CVSS Score: 5
  – Description: The PKCS7_dataDecodefunction in crypto/pkcs7/pk7_doit.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a PKCS#7 blob that uses ASN.1 encoding and lacks inner EncryptedContent data.

- Vulnerability: CVE-2015-1791

  – CVSS Score: 6.8
  – Description: Race condition in the ssl3_get_new_session_ticket function in ssl/s3_clnt.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b, when used for a multi-threaded client, allows remote attackers to cause a denial of service (double free and application crash) or possibly have unspecified other impact by providing a NewSessionTicket during an attempt to reuse a ticket that had been obtained earlier.

- Vulnerability: CVE-2015-1792

  – CVSS Score: 5
  – Description: The do_free_upto function in crypto/cms/cms_smime.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (infinite loop) via vectors that trigger a NULL value of a BIO data structure, as demonstrated by an unrecognized X.660 OID for a hash function.

- Vulnerability: CVE-2013-2765

  – CVSS Score: 5
  – Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2011-4619

  – CVSS Score: 5
  – Description: The Server Gated Cryptography (SGC) implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly handle handshake restarts, which allows remote attackers to cause a denial of service (CPU consumption) via unspecified vectors.

- Vulnerability: CVE-2013-0941

  – CVSS Score: 2.1

- Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2013-6449

  - CVSS Score: 4.3
  - Description: The ssl_get_algorithm2 function in ssl/s3_lib.c in OpenSSL before 1.0.2 obtains a certain version number from an incorrect data structure, which allows remote attackers to cause a denial of service (daemon crash) via crafted traffic from a TLS 1.2 client.

- Vulnerability: CVE-2020-7042

  - CVSS Score: 5
  - Description: An issue was discovered in openfortivpn 1.11.0 when used with OpenSSL 1.0.2 or later. tunnel.c mishandles certificate validation because the hostname check operates on uninitialized memory. The outcome is that a valid certificate is never accepted (only a malformed certificate may be accepted).

- Vulnerability: CVE-2020-7043

  - CVSS Score: 6.4
  - Description: An issue was discovered in openfortivpn 1.11.0 when used with OpenSSL before 1.0.2. tunnel.c mishandles certificate validation because hostname comparisons do not consider '\{}0' characters, as demonstrated by a good.example.com\{}x00evil.example.com attack.

- Vulnerability: CVE-2020-7041

  - CVSS Score: 5
  - Description: An issue was discovered in openfortivpn 1.11.0 when used with OpenSSL 1.0.2 or later. tunnel.c mishandles certificate validation because an X509_check_host negative error code is interpreted as a successful return value.

- Vulnerability: CVE-2023-45802

  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-28615

  – CVSS Score: 6.4
  – Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- Vulnerability: CVE-2022-28614

  – CVSS Score: 5
  – Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

- Vulnerability: CVE-2016-0704

  – CVSS Score: 4.3
  – Description: An oracle protection mechanism in the get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a overwrites incorrect MASTER-KEY bytes during use of export cipher suites, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.

11.19   IP Address: 159.149.205.26

- Organization: UNI-Milano

- Operating System: Unix

- Critical Vulnerabilities: 1

- High Vulnerabilities: 11

- Medium Vulnerabilities: 60

- Low Vulnerabilities: 5

- Total Vulnerabilities: 77

Services Running on IP Address

- Service: ProFTPD

  - Port: 21
  - Version: 1.3.2c
  - Location:

- Service: OpenSSH

  - Port: 22
  - Version: 5.3p1 Debian 3ubuntu7.1
  - Location:

- Service: Apache httpd

  - Port: 80
  - Version: 2.2.14
  - Location: /

Vulnerabilities Found

- Vulnerability: CVE-2010-2068

  - CVSS Score: 5
  - Description: mod_proxy_http.c in mod_proxy_http in the Apache HTTP Server 2.2.9
                  through 2.2.15, 2.3.4-alpha, and 2.3.5-alpha on Windows, NetWare, and
                  OS/2, in certain configurations involving proxy worker pools, does
                  not properly detect timeouts, which allows remote attackers to obtain
                  a potentially sensitive response intended for a different client in
                  opportunistic circumstances via a normal HTTP request.

- Vulnerability: CVE-2014-0118

  - CVSS Score: 4.3
  - Description: The deflate_in_filter function in mod_deflate.c in the mod_deflate
                  module in the Apache HTTP Server before 2.4.10, when request body
                  decompression is enabled, allows remote attackers to cause a denial
                  of service (resource consumption) via crafted request data that
                  decompresses to a much larger size.

- Vulnerability: CVE-2011-4317

  - CVSS Score: 4.3

– Description: The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42,
2.0.x through 2.0.64, and 2.2.x through 2.2.21, when the Revision
1179239 patch is in place, does not properly interact with use
of (1) RewriteRule and (2) ProxyPassMatch pattern matches for
configuration of a reverse proxy, which allows remote attackers to
send requests to intranet servers via a malformed URI containing an @
(at sign) character and a : (colon) character in invalid positions.
NOTE: this vulnerability exists because of an incomplete fix for
CVE-2011-3368.

• Vulnerability: CVE-2011-3607

– CVSS Score: 4.4
– Description: Integer overflow in the ap_pregsub function in server/util.c in the
Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21,
when the mod_setenvif module is enabled, allows local users to gain
privileges via a .htaccess file with a crafted SetEnvIf directive,
in conjunction with a crafted HTTP request header, leading to a
heap-based buffer overflow.

• Vulnerability: CVE-2017-7679

– CVSS Score: 7.5
– Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime
can read one byte past the end of a buffer when sending a malicious
Content-Type response header.

• Vulnerability: CVE-2009-3560

– CVSS Score: 5
– Description: The big2_toUtf8 function in lib/xmltok.c in libexpat in Expat 2.0.1,
as used in the XML-Twig module for Perl, allows context-dependent
attackers to cause a denial of service (application crash) via an
XML document with malformed UTF-8 sequences that trigger a buffer
over-read, related to the doProlog function in lib/xmlparse.c, a
different vulnerability than CVE-2009-2625 and CVE-2009-3720.

• Vulnerability: CVE-2011-1176

– CVSS Score: 4.3
– Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk
Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP
Server does not properly handle certain configuration sections that
specify NiceValue but not AssignUserID, which might allow remote
attackers to gain privileges by leveraging the root uid and root gid
of an mpm-itk process.

• Vulnerability: CVE-2021-34798

– CVSS Score: 5
– Description: Malformed requests may cause the server to dereference a NULL
pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

• Vulnerability: CVE-2010-0425

– CVSS Score: 10
– Description: modules/arch/win32/mod_isapi.c in mod_isapi in the Apache HTTP Server
2.0.37 through 2.0.63, 2.2.0 through 2.2.14, and 2.3.x before 2.3.7,
when running on Windows, does not ensure that request processing is
complete before calling isapi_unload for an ISAPI .dll module, which
allows remote attackers to execute arbitrary code via unspecified
vectors related to a crafted request, a reset packet, and "orphaned
callback pointers."

- Vulnerability: CVE-2010-1623

  - CVSS Score: 5
  - Description: Memory leak in the apr_brigade_split_line function in
    buckets/apr_brigade.c in the Apache Portable Runtime Utility library
    (aka APR-util) before 1.3.10, as used in the mod_reqtimeout module in
    the Apache HTTP Server and other software, allows remote attackers
    to cause a denial of service (memory consumption) via unspecified
    vectors related to the destruction of an APR bucket.

- Vulnerability: CVE-2012-4557

  - CVSS Score: 5
  - Description: The mod_proxy_ajp module in the Apache HTTP Server 2.2.12 through
    2.2.21 places a worker node into an error state upon detection of a
    long request-processing time, which allows remote attackers to cause
    a denial of service (worker consumption) via an expensive request.

- Vulnerability: CVE-2010-0434

  - CVSS Score: 4.3
  - Description: The ap_read_request function in server/protocol.c in the Apache HTTP
    Server 2.2.x before 2.2.15, when a multithreaded MPM is used, does
    not properly handle headers in subrequests in certain circumstances
    involving a parent request that has a body, which might allow remote
    attackers to obtain sensitive information via a crafted request
    that triggers access to memory locations associated with an earlier
    request.

- Vulnerability: CVE-2022-29404

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a
    lua script that calls r:parsebody(0) may cause a denial of service
    due to no default limit on possible input size.

- Vulnerability: CVE-2015-3183

  - CVSS Score: 5
  - Description: The chunked transfer coding implementation in the Apache HTTP
    Server before 2.4.14 does not properly parse chunk headers,
    which allows remote attackers to conduct HTTP request smuggling
    attacks via a crafted request, related to mishandling of large
    chunk-size values and invalid chunk-extension characters in
    modules/http/http_filters.c.

- Vulnerability: CVE-2012-0883

  - CVSS Score: 6.9
  - Description: envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2
    places a zero-length directory name in the LD_LIBRARY_PATH, which
    allows local users to gain privileges via a Trojan horse DSO in the
    current working directory during execution of apachectl.

- Vulnerability: CVE-2013-4365

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function
    in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache
    HTTP Server allows remote attackers to have an unspecified impact via
    unknown vectors.

- Vulnerability: CVE-2022-22720

– CVSS Score: 7.5

– Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

• Vulnerability: CVE-2017-3169

  – CVSS Score: 7.5

  – Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.

• Vulnerability: CVE-2022-28330

  – CVSS Score: 5

  – Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

• Vulnerability: CVE-2012-3499

  – CVSS Score: 4.3

  – Description: Multiple cross-site scripting (XSS) vulnerabilities in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via vectors involving hostnames and URIs in the (1) mod_imagemap, (2) mod_info, (3) mod_ldap, (4) mod_proxy_ftp, and (5) mod_status modules.

• Vulnerability: CVE-2012-4558

  – CVSS Score: 4.3

  – Description: Multiple cross-site scripting (XSS) vulnerabilities in the balancer_handler function in the manager interface in mod_proxy_balancer.c in the mod_proxy_balancer module in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via a crafted string.

• Vulnerability: CVE-2021-32791

  – CVSS Score: 4.3

  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

• Vulnerability: CVE-2021-32792

  – CVSS Score: 4.3

  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.

• Vulnerability: CVE-2013-1896

  – CVSS Score: 4.3

- Description: mod_dav.c in the Apache HTTP Server before 2.2.25 does not properly
determine whether DAV is enabled for a URI, which allows remote
attackers to cause a denial of service (segmentation fault) via a
MERGE request in which the URI is configured for handling by the
mod_dav_svn module, but a certain href attribute in XML data refers to
a non-DAV URI.

- Vulnerability: CVE-2016-8612

  - CVSS Score: 3.3
  - Description: Apache HTTP Server mod_cluster before version httpd 2.4.23 is
vulnerable to an Improper Input Validation in the protocol parsing
logic in the load balancer resulting in a Segmentation Fault in the
serving httpd process.

- Vulnerability: CVE-2014-0226

  - CVSS Score: 6.8
  - Description: Race condition in the mod_status module in the Apache HTTP Server
before 2.4.10 allows remote attackers to cause a denial of
service (heap-based buffer overflow), or possibly obtain sensitive
credential information or execute arbitrary code, via a crafted
request that triggers improper scoreboard handling within the
status_handler function in modules/generators/mod_status.c and the
lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module
before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before
3.1.1-11637, a module for the Apache HTTP Server, allows remote
attackers to cause a denial of service (memory consumption) via an
HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2023-31122

  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP
Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2016-4975

  - CVSS Score: 4.3
  - Description: Possible CRLF injection allowing HTTP response splitting attacks for
sites which use mod_userdir. This issue was mitigated by changes
made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the
"Location" or other outbound header key or value. Fixed in Apache
HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP
Server 2.2.32 (Affected 2.2.0-2.2.31).

- Vulnerability: CVE-2022-22721

  - CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than
350MB (defaults to 1M) on 32 bit systems an integer overflow happens
which later causes out of bounds writes. This issue affects Apache
HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2006-20001

  - CVSS Score: N/A

- Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2009-3720

  - CVSS Score: 5
  - Description: The updatePosition function in lib/xmltok_impl.c in libexpat in Expat 2.0.1, as used in Python, PyXML, w3c-libwww, and other software, allows context-dependent attackers to cause a denial of service (application crash) via an XML document with crafted UTF-8 sequences that trigger a buffer over-read, a different vulnerability than CVE-2009-2625.

- Vulnerability: CVE-2013-5704

  - CVSS Score: 5
  - Description: The mod_headers module in the Apache HTTP Server 2.2.22 allows remote attackers to bypass "RequestHeader unset" directives by placing a header in the trailer portion of data sent with chunked transfer coding. NOTE: the vendor states "this is not a security issue in httpd as such."

- Vulnerability: CVE-2010-0408

  - CVSS Score: 5
  - Description: The ap_proxy_ajp_request function in mod_proxy_ajp.c in mod_proxy_ajp in the Apache HTTP Server 2.2.x before 2.2.15 does not properly handle certain situations in which a client sends no request body, which allows remote attackers to cause a denial of service (backend server outage) via a crafted request, related to use of a 500 error code instead of the appropriate 400 error code.

- Vulnerability: CVE-2014-0098

  - CVSS Score: 5
  - Description: The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.

- Vulnerability: CVE-2012-3526

  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2022-31813

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

- Vulnerability: CVE-2012-4001

  - CVSS Score: 5

– Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

• Vulnerability: CVE-2011-3368

  – CVSS Score: 5

  – Description: The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21 does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an initial @ (at sign) character.

• Vulnerability: CVE-2012-2687

  – CVSS Score: 2.6

  – Description: Multiple cross-site scripting (XSS) vulnerabilities in the make_variant_list function in mod_negotiation.c in the mod_negotiation module in the Apache HTTP Server 2.4.x before 2.4.3, when the MultiViews option is enabled, allow remote attackers to inject arbitrary web script or HTML via a crafted filename that is not properly handled during construction of a variant list.

• Vulnerability: CVE-2022-37436

  – CVSS Score: N/A

  – Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

• Vulnerability: CVE-2016-5387

  – CVSS Score: 6.8

  – Description: The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.

• Vulnerability: CVE-2012-4360

  – CVSS Score: 4.3

  – Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

• Vulnerability: CVE-2021-40438

  – CVSS Score: 6.8

  – Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

• Vulnerability: CVE-2011-4415

  – CVSS Score: 1.2

- Description: The ap_pregsub function in server/util.c in the Apache HTTP
              Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the
              mod_setenvif module is enabled, does not restrict the size of values
              of environment variables, which allows local users to cause a denial
              of service (memory consumption or NULL pointer dereference) via a
              .htaccess file with a crafted SetEnvIf directive, in conjunction with
              a crafted HTTP request header, related to (1) the "len +=" statement
              and (2) the apr_pcalloc function call, a different vulnerability than
              CVE-2011-3607.

- Vulnerability: CVE-2013-6438

  - CVSS Score: 5
  - Description: The dav_xml_get_cdata function in main/util.c in the mod_dav module
                in the Apache HTTP Server before 2.4.8 does not properly remove
                whitespace characters from CDATA sections, which allows remote
                attackers to cause a denial of service (daemon crash) via a crafted
                DAV WRITE request.

- Vulnerability: CVE-2012-0031

  - CVSS Score: 4.6
  - Description: scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might
                allow local users to cause a denial of service (daemon crash during
                shutdown) or possibly have unspecified other impact by modifying a
                certain type field within a scoreboard shared memory segment, leading
                to an invalid call to the free function.

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5
                for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM
                Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows
                use an improper encryption algorithm and a weak key for maintaining
                the stored data of the node secret for the SecurID Authentication
                API, which allows local users to obtain sensitive information via
                cryptographic attacks on this data.

- Vulnerability: CVE-2008-0455

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_negotiation
                module in the Apache HTTP Server 2.2.6 and earlier in the 2.2.x
                series, 2.0.61 and earlier in the 2.0.x series, and 1.3.39 and
                earlier in the 1.3.x series allows remote authenticated users to
                inject arbitrary web script or HTML by uploading a file with a
                name containing XSS sequences and a file extension, which leads to
                injection within a (1) "406 Not Acceptable" or (2) "300 Multiple
                Choices" HTTP response when the extension is omitted in a request for
                the file.

- Vulnerability: CVE-2017-9788

  - CVSS Score: 6.4
  - Description: In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value
                placeholder in [Proxy-]Authorization headers of type 'Digest' was
                not initialized or reset before or between successive key=value
                assignments by mod_auth_digest. Providing an initial key with no
                '=' assignment could reflect the stale value of uninitialized pool
                memory used by the prior request, leading to leakage of potentially
                confidential information, and a segfault in other cases resulting in
                denial of service.

- Vulnerability: CVE-2010-1452

  - CVSS Score: 5
  - Description: The (1) mod_cache and (2) mod_dav modules in the Apache HTTP Server 2.2.x before 2.2.16 allow remote attackers to cause a denial of service (process crash) via a request that lacks a path.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2011-3348

  - CVSS Score: 4.3
  - Description: The mod_proxy_ajp module in the Apache HTTP Server before 2.2.21, when used with mod_proxy_balancer in certain configurations, allows remote attackers to cause a denial of service (temporary "error state" in the backend server) via a malformed HTTP request.

- Vulnerability: CVE-2018-1301

  - CVSS Score: 4.3
  - Description: A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.

- Vulnerability: CVE-2018-1302

  - CVSS Score: 4.3
  - Description: When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.

- Vulnerability: CVE-2018-1303

  - CVSS Score: 5
  - Description: A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache. The vulnerability is considered as low risk since mod_cache_socache is not widely used, mod_cache_disk is not concerned by this vulnerability.

- Vulnerability: CVE-2017-3167

  - CVSS Score: 7.5
  - Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.

- Vulnerability: CVE-2017-9798

- CVSS Score: 5
- Description: Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.

- Vulnerability: CVE-2012-0053

  - CVSS Score: 4.3
  - Description: protocol.c in the Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header information during construction of Bad Request (aka 400) error documents, which allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a (1) long or (2) malformed header in conjunction with crafted web script.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2009-3555

  - CVSS Score: 5.8
  - Description: The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0, mod_ssl in the Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a "plaintext injection" attack, aka the "Project Mogul" issue.

- Vulnerability: CVE-2021-32786

  - CVSS Score: 5.8
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, `oidc_validate_redirect_url()` does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring `mod_auth_openidc` to only allow redirection whose destination matches a given regular expression.

- Vulnerability: CVE-2021-32785

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the
                 Apache 2.x HTTP server that functions as an OpenID Connect Relying
                 Party, authenticating users against an OpenID Connect Provider. When
                 mod_auth_openidc versions prior to 2.4.9 are configured to use an
                 unencrypted Redis cache ('OIDCCacheEncrypt off', 'OIDCSessionType
                 server-cache', 'OIDCCacheType redis'), 'mod_auth_openidc' wrongly
                 performed argument interpolation before passing Redis requests to
                 'hiredis', which would perform it again and lead to an uncontrolled
                 format string bug. Initial assessment shows that this bug does
                 not appear to allow gaining arbitrary code execution, but can
                 reliably provoke a denial of service by repeatedly crashing the
                 Apache workers. This bug has been corrected in version 2.4.9 by
                 performing argument interpolation only once, using the 'hiredis'
                 API. As a workaround, this vulnerability can be mitigated by setting
                 'OIDCCacheEncrypt' to 'on', as cache keys are cryptographically
                 hashed before use when this option is enabled.

- Vulnerability: CVE-2007-6750

  - CVSS Score: 5
  - Description: The Apache HTTP Server 1.x and 2.x allows remote attackers to cause
                 a denial of service (daemon outage) via partial HTTP requests, as
                 demonstrated by Slowloris, related to the lack of the mod_reqtimeout
                 module in versions before 2.2.15.

- Vulnerability: CVE-2015-0228

  - CVSS Score: 5
  - Description: The lua_websocket_read function in lua_request.c in the mod_lua module
                 in the Apache HTTP Server through 2.4.12 allows remote attackers to
                 cause a denial of service (child-process crash) by sending a crafted
                 WebSocket Ping frame after a Lua script has called the wsupgrade
                 function.

- Vulnerability: CVE-2021-44790

  - CVSS Score: 7.5
  - Description: A carefully crafted request body can cause a buffer overflow in the
                 mod_lua multipart parser (r:parsebody() called from Lua scripts).
                 The Apache httpd team is not aware of an exploit for the vulnerabilty
                 though it might be possible to craft one. This issue affects Apache
                 HTTP Server 2.4.51 and earlier.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication
                 Agent 7.1 before 7.1.1 for Web for Internet Information Services,
                 and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to
                 inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2011-3639

  - CVSS Score: 4.3

- Description: The mod_proxy module in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x before 2.2.18, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers by using the HTTP/0.9 protocol with a malformed URI containing an initial @ (at sign) character. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-3368.

- Vulnerability: CVE-2011-0419

  - CVSS Score: 4.3
  - Description: Stack consumption vulnerability in the fnmatch implementation in apr_fnmatch.c in the Apache Portable Runtime (APR) library before 1.4.3 and the Apache HTTP Server before 2.2.18, and in fnmatch.c in libc in NetBSD 5.1, OpenBSD 4.8, FreeBSD, Apple Mac OS X 10.6, Oracle Solaris 10, and Android, allows context-dependent attackers to cause a denial of service (CPU and memory consumption) via *? sequences in the first argument, as demonstrated by attacks against mod_autoindex in httpd.

- Vulnerability: CVE-2014-0231

  - CVSS Score: 5
  - Description: The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.

- Vulnerability: CVE-2013-1862

  - CVSS Score: 5.1
  - Description: mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary commands via an HTTP request containing an escape sequence for a terminal emulator.

- Vulnerability: CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2023-45802

  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-28614

  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier
    may read unintended memory if an attacker can cause the server to
    reflect very large input using ap_rwrite() or ap_rputs(), such as
    with mod_luas r:puts() function. Modules compiled and distributed
    separately from Apache HTTP Server that use the 'ap_rputs' function
    and may pass it a very large (INT_MAX or larger) string must be
    compiled against current headers to resolve the issue.

- Vulnerability: CVE-2009-0796

  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in
    Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the
    Apache HTTP Server, when /perl-status is accessible, allows remote
    attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2016-8743

  - CVSS Score: 5
  - Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was
    liberal in the whitespace accepted from requests and sent in response
    lines and headers. Accepting these different behaviors represented a
    security concern when httpd participates in any chain of proxies or
    interacts with back-end application servers, either through mod_proxy
    or using conventional CGI mechanisms, and may result in request
    smuggling, response splitting and cache pollution.

- Vulnerability: CVE-2024-40898

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in
    server/vhost context, allows to potentially leak NTML hashes to
    a malicious server via SSRF and malicious requests.Users are
    recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory
    area which could cause the process to crash. This issue affects
    Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2022-28615

  - CVSS Score: 6.4
  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose
    information due to a read beyond bounds in ap_strcmp_match() when
    provided with an extremely large input buffer. While no code
    distributed with the server can be coerced into such a call,
    third-party modules or lua scripts that use ap_strcmp_match() may
    hypothetically be affected.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to
    applications calling r:wsread() that point past the end of the
    storage allocated for the buffer.

- Vulnerability: CVE-2011-3192

– CVSS Score: 7.8

  – Description: The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through
               2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause
               a denial of service (memory and CPU consumption) via a Range header
               that expresses multiple overlapping ranges, as exploited in the wild
               in August 2011, a different vulnerability than CVE-2007-0086.

- Vulnerability: CVE-2021-39275

  – CVSS Score: 7.5

  – Description: ap_escape_quotes() may write beyond the end of a buffer when given
               malicious input. No included modules pass untrusted data to these
               functions, but third-party / external modules may. This issue
               affects Apache HTTP Server 2.4.48 and earlier.

11.20   IP Address: 159.149.136.4

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 1

- High Vulnerabilities: 7

- Medium Vulnerabilities: 26

- Low Vulnerabilities: 4

- Total Vulnerabilities: 38

Services Running on IP Address

- Service: OpenSSH

  - Port: 22
  - Version: 9.0
  - Location:

- Service: Apache httpd

  - Port: 80
  - Version: 2.4.58
  - Location: https://wikirank.di.unimi.it/

- Service: Apache httpd

  - Port: 443
  - Version: 2.4.58
  - Location: http://prng.di.unimi.it/

- Service: N/A

  - Port: 993
  - Version: N/A
  - Location:

Vulnerabilities Found

- Vulnerability: CVE-2008-3844

  - CVSS Score: 9.3
  - Description: Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, as signed in August 2008 using a legitimate Red Hat GPG key, contain an externally introduced modification (Trojan Horse) that allows the package authors to have an unknown impact. NOTE: since the malicious packages were not distributed from any official Red Hat sources, the scope of this issue is restricted to users who may have obtained these packages through unofficial distribution points. As of 20080827, no unofficial distributions of this software are known.

- Vulnerability: CVE-2023-51767

  - CVSS Score: N/A

- Description: OpenSSH through 9.6, when common types of DRAM are used, might allow row hammer attacks (for authentication bypass) because the integer value of authenticated in mm_answer_authpassword does not resist flips of a single bit. NOTE: this is applicable to a certain threat model of attacker-victim co-location in which the attacker has user privileges.

- Vulnerability: CVE-2023-48795

  - CVSS Score: N/A

  - Description: The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.

- Vulnerability: CVE-2023-38408

  - CVSS Score: N/A

  - Description: The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009.

- Vulnerability: CVE-2007-2768

  - CVSS Score: 4.3

  - Description: OpenSSH, when using OPIE (One-Time Passwords in Everything) for PAM, allows remote attackers to determine the existence of certain user accounts, which displays a different response if the user account exists and is configured to use one-time passwords (OTP), a similar issue to CVE-2007-2243.

- Vulnerability: CVE-2023-28531

- CVSS Score: N/A
- Description: ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.

- **Vulnerability: CVE-2023-51384**

  - CVSS Score: N/A
  - Description: In ssh-agent in OpenSSH before 9.6, certain destination constraints can be incompletely applied. When destination constraints are specified during addition of PKCS#11-hosted private keys, these constraints are only applied to the first key, even if a PKCS#11 token returns multiple keys.

- **Vulnerability: CVE-2023-51385**

  - CVSS Score: N/A
  - Description: In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.

- **Vulnerability: CVE-2024-6387**

  - CVSS Score: N/A
  - Description: A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period.

- **Vulnerability: CVE-2009-2299**

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- **Vulnerability: CVE-2024-27316**

  - CVSS Score: N/A
  - Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

- **Vulnerability: CVE-2009-1390**

  - CVSS Score: 6.8
  - Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2) GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS certificate in the chain is accepted instead of verifying the entire chain, which allows remote attackers to spoof trusted servers via a man-in-the-middle attack.

- **Vulnerability: CVE-2013-4365**

  - CVSS Score: 7.5

– Description: Heap-based buffer overflow in the `fcgid_header_bucket_read` function in `fcgid_bucket.c` in the `mod_fcgid` module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2012-3526

  – CVSS Score: 5

  – Description: The reverse proxy add forward module (`mod_rpaf`) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2023-5678

  – CVSS Score: N/A

  – Description: Issue summary: Generating excessively long X9.42 DH keys or checkingexcessively long X9.42 DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_generate_key() togenerate an X9.42 DH key may experience long delays. Likewise, applicationsthat use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check()to check an X9.42 DH key or X9.42 DH parameters may experience long delays.Where the key or parameters that are being checked have been obtained froman untrusted source this may lead to a Denial of Service.While DH_check() performs all the necessary checks (as of CVE-2023-3817),DH_check_pub_key() doesn't make any of these checks, and is thereforevulnerable for excessively large P and Q parameters.Likewise, while DH_generate_key() performs a check for an excessively largeP, it doesn't check for an excessively large Q.An application that calls DH_generate_key() or DH_check_pub_key() andsupplies a key or parameters obtained from an untrusted source could bevulnerable to a Denial of Service attack.DH_generate_key() and DH_check_pub_key() are also called by a number ofother OpenSSL functions. An application calling any of those otherfunctions may similarly be affected. The other functions affected by thisare DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate().Also vulnerable are the OpenSSL pkey command line application when using the"-pubcheck" option, as well as the OpenSSL genpkey command line application.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2009-3766

  – CVSS Score: 6.8

  – Description: `mutt_ssl.c` in mutt 1.5.16 and other versions before 1.5.19, when OpenSSL is used, does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

- Vulnerability: CVE-2024-38477

  – CVSS Score: N/A

  – Description: null pointer dereference in `mod_proxy` in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-38474

- CVSS Score: N/A

- Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

• Vulnerability: CVE-2009-3765

  - CVSS Score: 6.8

  - Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

• Vulnerability: CVE-2019-0190

  - CVSS Score: 5

  - Description: A bug exists in the way mod_ssl handled client renegotiations. A remote attacker could send a carefully crafted request that would cause mod_ssl to enter a loop leading to a denial of service. This bug can be only triggered with Apache HTTP Server version 2.4.37 when using OpenSSL version 1.1.1 or later, due to an interaction in changes to handling of renegotiation attempts.

• Vulnerability: CVE-2009-0796

  - CVSS Score: 2.6

  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

• Vulnerability: CVE-2024-0727

  - CVSS Score: N/A

  - Description: Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSLto crash leading to a potential Denial of Service attackImpact summary: Applications loading files in the PKCS12 format from untrustedsources might terminate abruptly.A file in PKCS12 format can contain certificates and keys and may come from anuntrusted source. The PKCS12 specification allows certain fields to be NULL, butOpenSSL does not correctly check for this case. This can lead to a NULL pointerdereference that results in OpenSSL crashing. If an application processes PKCS12files from an untrusted source using the OpenSSL APIs then that application willbe vulnerable to this issue.OpenSSL APIs that are vulnerable to this are: PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a similar issue in SMIME_write_PKCS7(). However since thisfunction is related to writing data we do not consider it security significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.

• Vulnerability: CVE-2012-4001

  - CVSS Score: 5

- Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2012-4360

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2023-3817

  - CVSS Score: N/A
  - Description: Issue summary: Checking excessively long DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH key or DH parameters may experience longdelays. Where the key or parameters that are being checked have been obtainedfrom an untrusted source this may lead to a Denial of Service.The function DH_check() performs various checks on DH parameters. After fixingCVE-2023-3446 it was discovered that a large q parameter value can also triggeran overly long computation during some of these checks. A correct q value,if present, cannot be larger than the modulus p parameter, thus it isunnecessary to perform these checks if q is larger than p.An application that calls DH_check() and supplies a key or parameters obtainedfrom an untrusted source could be vulnerable to a Denial of Service attack.The function DH_check() is itself called by a number of other OpenSSL functions.An application calling any of those other functions may similarly be affected.The other functions affected by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable are the OpenSSL dhparam and pkeyparam command line applicationswhen using the "-check" option.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2023-4807

  - CVSS Score: N/A

– Description: Issue summary: The POLY1305 MAC (message authentication code) implementationcontains a bug that might corrupt the internal state of applications on theWindows 64 platform when running on newer X86_64 processors supporting theAVX512-IFMA instructions.Impact summary: If in an application that uses the OpenSSL library an attackercan influence whether the POLY1305 MAC algorithm is used, the applicationstate might be corrupted with various application dependent consequences.The POLY1305 MAC (message authentication code) implementation in OpenSSL doesnot save the contents of non-volatile XMM registers on Windows 64 platformwhen calculating the MAC of data larger than 64 bytes. Before returning tothe caller all the XMM registers are set to zero rather than restoring theirprevious content. The vulnerable code is used only on newer x86_64 processorssupporting the AVX512-IFMA instructions.The consequences of this kind of internal application state corruption canbe various – from no consequences, if the calling application does notdepend on the contents of non-volatile XMM registers at all, to the worstconsequences, where the attacker could get complete control of the applicationprocess. However given the contents of the registers are just zeroized sothe attacker cannot put arbitrary values inside, the most likely consequence,if any, would be an incorrect result of some application dependentcalculations or a crash leading to a denial of service.The POLY1305 MAC algorithm is most frequently used as part of theCHACHA20-POLY1305 AEAD (authenticated encryption with associated data)algorithm. The most common usage of this AEAD cipher is with TLS protocolversions 1.2 and 1.3 and a malicious client can influence whether this AEADcipher is used by the server. This implies that server applications usingOpenSSL can be potentially impacted. However we are currently not aware ofany concrete application that would be affected by this issue therefore weconsider this a Low severity security issue.As a workaround the AVX512-IFMA instructions support can be disabled atruntime by setting the environment variable OPENSSL_ia32cap: OPENSSL_ia32cap=:~0x200000The FIPS provider is not affected by this issue.

- Vulnerability: CVE-2023-6129

  – CVSS Score: N/A

– Description: Issue summary: The POLY1305 MAC (message authentication code) implementationcontains a bug that might corrupt the internal state of applications runningon PowerPC CPU based platforms if the CPU provides vector instructions.Impact summary: If an attacker can influence whether the POLY1305 MACalgorithm is used, the application state might be corrupted with variousapplication dependent consequences.The POLY1305 MAC (message authentication code) implementation in OpenSSL forPowerPC CPUs restores the contents of vector registers in a different orderthan they are saved. Thus the contents of some of these vector registersare corrupted when returning to the caller. The vulnerable code is used onlyon newer PowerPC processors supporting the PowerISA 2.07 instructions.The consequences of this kind of internal application state corruption canbe various – from no consequences, if the calling application does notdepend on the contents of non-volatile XMM registers at all, to the worstconsequences, where the attacker could get complete control of the applicationprocess. However unless the compiler uses the vector registers for storingpointers, the most likely consequence, if any, would be an incorrect resultof some application dependent calculations or a crash leading to a denial ofservice.The POLY1305 MAC algorithm is most frequently used as part of theCHACHA20-POLY1305 AEAD (authenticated encryption with associated data)algorithm. The most common usage of this AEAD cipher is with TLS protocolversions 1.2 and 1.3. If this cipher is enabled on the server a maliciousclient can influence whether this AEAD cipher is used. This implies thatTLS server applications using OpenSSL can be potentially impacted. Howeverwe are currently not aware of any concrete application that would be affectedby this issue therefore we consider this a Low severity security issue.

• Vulnerability: CVE-2013-2765

  – CVSS Score: 5

  – Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

• Vulnerability: CVE-2011-2688

  – CVSS Score: 7.5

  – Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

• Vulnerability: CVE-2009-3767

  – CVSS Score: 4.3

  – Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other versions, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

• Vulnerability: CVE-2007-4723

  – CVSS Score: 7.5

- Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- **Vulnerability: CVE-2013-0941**

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- **Vulnerability: CVE-2013-0942**

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- **Vulnerability: CVE-2024-38476**

  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- **Vulnerability: CVE-2024-40898**

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- **Vulnerability: CVE-2023-2975**

  - CVSS Score: N/A
  - Description: Issue summary: The AES-SIV cipher implementation contains a bug that causesit to ignore empty associated data entries which are unauthenticated asa consequence.Impact summary: Applications that use the AES-SIV algorithm and want toauthenticate empty data entries as associated data can be mislead by removingadding or reordering such empty entries as these are ignored by the OpenSSLimplementation. We are currently unaware of any such applications.The AES-SIV algorithm allows for authentication of multiple associateddata entries along with the encryption. To authenticate empty data theapplication has to call EVP_EncryptUpdate() (or EVP_CipherUpdate()) withNULL pointer as the output buffer and 0 as the input buffer length.The AES-SIV implementation in OpenSSL just returns success for such a callinstead of performing the associated data authentication operation.The empty data thus will not be authenticated.As this issue does not affect non-empty associated data authentication andwe expect it to be rare for an application to use empty associated dataentries this is qualified as Low severity issue.

- Vulnerability: CVE-2023-5363
  - CVSS Score: N/A
  - Description: Issue summary: A bug has been identified in the processing of key
    andinitialisation vector (IV) lengths. This can lead to potential
    truncationor overruns during the initialisation of some symmetric
    ciphers.Impact summary: A truncation in the IV can result in
    non-uniqueness,which could result in loss of confidentiality for some
    cipher modes.When calling EVP_EncryptInit_ex2(), EVP_DecryptInit_ex2()
    orEVP_CipherInit_ex2() the provided OSSL_PARAM array is processed
    afterthe key and IV have been established. Any alterations to the
    key length,via the "keylen" parameter or the IV length, via the
    "ivlen" parameter,within the OSSL_PARAM array will not take effect
    as intended, potentiallycausing truncation or overreading of these
    values. The following ciphersand cipher modes are impacted: RC2,
    RC4, RC5, CCM, GCM and OCB.For the CCM, GCM and OCB cipher modes,
    truncation of the IV can result inloss of confidentiality. For
    example, when following NIST's SP 800-38Dsection 8.2.1 guidance for
    constructing a deterministic IV for AES inGCM mode, truncation of the
    counter portion could lead to IV reuse.Both truncations and overruns
    of the key and overruns of the IV willproduce incorrect results and
    could, in some cases, trigger a memoryexception. However, these
    issues are not currently assessed as securitycritical.Changing the
    key and/or IV lengths is not considered to be a common operationand
    the vulnerable API was recently introduced. Furthermore it is
    likely thatapplication developers will have spotted this problem
    during testing sincedecryption would fail unless both peers in
    the communication were similarlyvulnerable. For these reasons
    we expect the probability of an application beingvulnerable to
    this to be quite low. However if an application is vulnerable
    thenthis issue is considered very serious. For these reasons we have
    assessed thisissue as Moderate severity overall.The OpenSSL SSL/TLS
    implementation is not affected by this issue.The OpenSSL 3.0 and 3.1
    FIPS providers are not affected by this becausethe issue lies outside
    of the FIPS provider boundary.OpenSSL 3.1 and 3.0 are vulnerable to
    this issue.
- Vulnerability: CVE-2009-2299
  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module
    before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before
    3.1.1-11637, a module for the Apache HTTP Server, allows remote
    attackers to cause a denial of service (memory consumption) via an
    HTTP request with a large Content-Length value but no POST data.
- Vulnerability: CVE-2024-27316
  - CVSS Score: N/A
  - Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered
    in nghttp2 in order to generate an informative HTTP 413 response.
    If a client does not stop sending headers, this leads to memory
    exhaustion.
- Vulnerability: CVE-2013-2765
  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server
    allows remote attackers to cause a denial of service (NULL pointer
    dereference, process crash, and disk consumption) via a POST request
    with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2024-4577

  - CVSS Score: N/A
  - Description: In PHP versions8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in command line given toWin32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc.

- Vulnerability: CVE-2013-4365

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2009-1390

  - CVSS Score: 6.8
  - Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2) GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS certificate in the chain is accepted instead of verifying the entire chain, which allows remote attackers to spoof trusted servers via a man-in-the-middle attack.

- Vulnerability: CVE-2007-3205

  - CVSS Score: 5
  - Description: The parse_str function in (1) PHP, (2) Hardened-PHP, and (3) Suhosin, when called without a second parameter, might allow remote attackers to overwrite arbitrary variables by specifying variable names and values in the string to be parsed. NOTE: it is not clear whether this is a design limitation of the function or a bug in PHP, although it is likely to be regarded as a bug in Hardened-PHP and Suhosin.

- Vulnerability: CVE-2024-5458

  - CVSS Score: N/A
  - Description: In PHP versions8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, due to a code logic error, filtering functions such as filter_var when validating URLs(FILTER_VALIDATE_URL) for certain types of URLs the function will result in invalid user information (username + password part of URLs) being treated as valid user information. This may lead to the downstream code accepting invalid URLs as valid and parsing them incorrectly.

- Vulnerability: CVE-2023-5678

  - CVSS Score: N/A

– Description: Issue summary: Generating excessively long X9.42 DH keys or checkingexcessively long X9.42 DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_generate_key() togenerate an X9.42 DH key may experience long delays. Likewise, applicationsthat use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check()to check an X9.42 DH key or X9.42 DH parameters may experience long delays.Where the key or parameters that are being checked have been obtained froman untrusted source this may lead to a Denial of Service.While DH_check() performs all the necessary checks (as of CVE-2023-3817),DH_check_pub_key() doesn't make any of these checks, and is thereforevulnerable for excessively large P and Q parameters.Likewise, while DH_generate_key() performs a check for an excessively largeP, it doesn't check for an excessively large Q.An application that calls DH_generate_key() or DH_check_pub_key() andsupplies a key or parameters obtained from an untrusted source could bevulnerable to a Denial of Service attack.DH_generate_key() and DH_check_pub_key() are also called by a number ofother OpenSSL functions. An application calling any of those otherfunctions may similarly be affected. The other functions affected by thisare DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate().Also vulnerable are the OpenSSL pkey command line application when using the"-pubcheck" option, as well as the OpenSSL genpkey command line application.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2009-3766

  – CVSS Score: 6.8
  – Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when OpenSSL is used, does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

- Vulnerability: CVE-2024-38477

  – CVSS Score: N/A
  – Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-38474

  – CVSS Score: N/A
  – Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2009-3765

  – CVSS Score: 6.8

- Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2019-0190

  - CVSS Score: 5

  - Description: A bug exists in the way mod_ssl handled client renegotiations. A remote attacker could send a carefully crafted request that would cause mod_ssl to enter a loop leading to a denial of service. This bug can be only triggered with Apache HTTP Server version 2.4.37 when using OpenSSL version 1.1.1 or later, due to an interaction in changes to handling of renegotiation attempts.

- Vulnerability: CVE-2009-0796

  - CVSS Score: 2.6

  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2024-0727

  - CVSS Score: N/A

  - Description: Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSLto crash leading to a potential Denial of Service attackImpact summary: Applications loading files in the PKCS12 format from untrustedsources might terminate abruptly.A file in PKCS12 format can contain certificates and keys and may come from anuntrusted source. The PKCS12 specification allows certain fields to be NULL, butOpenSSL does not correctly check for this case. This can lead to a NULL pointerdereference that results in OpenSSL crashing. If an application processes PKCS12files from an untrusted source using the OpenSSL APIs then that application willbe vulnerable to this issue.OpenSSL APIs that are vulnerable to this are: PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a similar issue in SMIME_write_PKCS7(). However since thisfunction is related to writing data we do not consider it security significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.

- Vulnerability: CVE-2012-3526

  - CVSS Score: 5

  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2013-2220

  - CVSS Score: 7.5

  - Description: Buffer overflow in the radius_get_vendor_attr function in the Radius extension before 1.2.7 for PHP allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a large Vendor Specific Attributes (VSA) length value.

- Vulnerability: CVE-2012-4360

  – CVSS Score: 4.3
  – Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2011-1176

  – CVSS Score: 4.3
  – Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2012-4001

  – CVSS Score: 5
  – Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2023-3817

  – CVSS Score: N/A
  – Description: Issue summary: Checking excessively long DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH key or DH parameters may experience longdelays. Where the key or parameters that are being checked have been obtainedfrom an untrusted source this may lead to a Denial of Service.The function DH_check() performs various checks on DH parameters. After fixingCVE-2023-3446 it was discovered that a large q parameter value can also triggeran overly long computation during some of these checks. A correct q value,if present, cannot be larger than the modulus p parameter, thus it isunnecessary to perform these checks if q is larger than p.An application that calls DH_check() and supplies a key or parameters obtainedfrom an untrusted source could be vulnerable to a Denial of Service attack.The function DH_check() is itself called by a number of other OpenSSL functions.An application calling any of those other functions may similarly be affected.The other functions affected by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable are the OpenSSL dhparam and pkeyparam command line applicationswhen using the "-check" option.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2023-4807

  – CVSS Score: N/A

- Description: Issue summary: The POLY1305 MAC (message authentication code)
                  implementationcontains a bug that might corrupt the internal state
                  of applications on theWindows 64 platform when running on newer
                  X86_64 processors supporting theAVX512-IFMA instructions.Impact
                  summary: If in an application that uses the OpenSSL library an
                  attackercan influence whether the POLY1305 MAC algorithm is used,
                  the applicationstate might be corrupted with various application
                  dependent consequences.The POLY1305 MAC (message authentication
                  code) implementation in OpenSSL doesnot save the contents of
                  non-volatile XMM registers on Windows 64 platformwhen calculating
                  the MAC of data larger than 64 bytes. Before returning tothe
                  caller all the XMM registers are set to zero rather than restoring
                  theirprevious content. The vulnerable code is used only on newer
                  x86_64 processorssupporting the AVX512-IFMA instructions.The
                  consequences of this kind of internal application state corruption
                  canbe various - from no consequences, if the calling application
                  does notdepend on the contents of non-volatile XMM registers at
                  all, to the worstconsequences, where the attacker could get complete
                  control of the applicationprocess. However given the contents of
                  the registers are just zeroized sothe attacker cannot put arbitrary
                  values inside, the most likely consequence,if any, would be an
                  incorrect result of some application dependentcalculations or a crash
                  leading to a denial of service.The POLY1305 MAC algorithm is most
                  frequently used as part of theCHACHA20-POLY1305 AEAD (authenticated
                  encryption with associated data)algorithm. The most common usage
                  of this AEAD cipher is with TLS protocolversions 1.2 and 1.3 and
                  a malicious client can influence whether this AEADcipher is used
                  by the server. This implies that server applications usingOpenSSL
                  can be potentially impacted. However we are currently not aware
                  ofany concrete application that would be affected by this issue
                  therefore weconsider this a Low severity security issue.As a
                  workaround the AVX512-IFMA instructions support can be disabled
                  atruntime by setting the environment variable OPENSSL_ia32cap:
                  OPENSSL_ia32cap=:~0x200000The FIPS provider is not affected by this
                  issue.
- Vulnerability: CVE-2023-6129

    - CVSS Score: N/A

- Description: Issue summary: The POLY1305 MAC (message authentication code) implementationcontains a bug that might corrupt the internal state of applications runningon PowerPC CPU based platforms if the CPU provides vector instructions.Impact summary: If an attacker can influence whether the POLY1305 MACalgorithm is used, the application state might be corrupted with variousapplication dependent consequences.The POLY1305 MAC (message authentication code) implementation in OpenSSL forPowerPC CPUs restores the contents of vector registers in a different orderthan they are saved. Thus the contents of some of these vector registersare corrupted when returning to the caller. The vulnerable code is used onlyon newer PowerPC processors supporting the PowerISA 2.07 instructions.The consequences of this kind of internal application state corruption canbe various – from no consequences, if the calling application does notdepend on the contents of non-volatile XMM registers at all, to the worstconsequences, where the attacker could get complete control of the applicationprocess. However unless the compiler uses the vector registers for storingpointers, the most likely consequence, if any, would be an incorrect resultof some application dependent calculations or a crash leading to a denial ofservice.The POLY1305 MAC algorithm is most frequently used as part of theCHACHA20-POLY1305 AEAD (authenticated encryption with associated data)algorithm. The most common usage of this AEAD cipher is with TLS protocolversions 1.2 and 1.3. If this cipher is enabled on the server a maliciousclient can influence whether this AEAD cipher is used. This implies thatTLS server applications using OpenSSL can be potentially impacted. Howeverwe are currently not aware of any concrete application that would be affectedby this issue therefore we consider this a Low severity security issue.

- Vulnerability: CVE-2024-2408

  - CVSS Score: N/A
  - Description: The openssl_private_decrypt function in PHP, when using PKCS1 padding (OPENSSL_PKCS1_PADDING, which is the default), is vulnerable to the Marvin Attack unless it is used with an OpenSSL version that includes the changes from this pull request: https://github.com/openssl/openssl/pull/13817 (rsa_pkcs1_implicit_rejection). These changes are part of OpenSSL 3.2 and have also been backported to stable versions of various Linux distributions, as well as to the PHP builds provided for Windows since the previous release. All distributors and builders should ensure that this version is used to prevent PHP from being vulnerable.PHP Windows builds for the versions8.1.29,8.2.20 and8.3.8 and above include OpenSSL patches that fix the vulnerability.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.
- Vulnerability: CVE-2009-3767

  - CVSS Score: 4.3

- Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other versions, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2024-38476

  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-40898

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2024-5585

  - CVSS Score: N/A
  - Description: In PHP versions8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, the fix forCVE-2024-1874 does not work if the command name includes trailing spaces. Original issue:when using proc_open() command with array syntax, due to insufficient escaping, if the arguments of the executed command are controlled by a malicious user, the user can supply arguments that would execute arbitrary commands in Windows shell.

- **Vulnerability: CVE-2023-2975**

  - CVSS Score: N/A
  - Description: Issue summary: The AES-SIV cipher implementation contains a bug that causesit to ignore empty associated data entries which are unauthenticated asa consequence.Impact summary: Applications that use the AES-SIV algorithm and want toauthenticate empty data entries as associated data can be mislead by removingadding or reordering such empty entries as these are ignored by the OpenSSLimplementation. We are currently unaware of any such applications.The AES-SIV algorithm allows for authentication of multiple associateddata entries along with the encryption. To authenticate empty data theapplication has to call EVP_EncryptUpdate() (or EVP_CipherUpdate()) withNULL pointer as the output buffer and 0 as the input buffer length.The AES-SIV implementation in OpenSSL just returns success for such a callinstead of performing the associated data authentication operation.The empty data thus will not be authenticated.As this issue does not affect non-empty associated data authentication andwe expect it to be rare for an application to use empty associated dataentries this is qualified as Low severity issue.

- **Vulnerability: CVE-2023-5363**

  - CVSS Score: N/A
  - Description: Issue summary: A bug has been identified in the processing of key andinitialisation vector (IV) lengths. This can lead to potential truncationor overruns during the initialisation of some symmetric ciphers.Impact summary: A truncation in the IV can result in non-uniqueness,which could result in loss of confidentiality for some cipher modes.When calling EVP_EncryptInit_ex2(), EVP_DecryptInit_ex2() orEVP_CipherInit_ex2() the provided OSSL_PARAM array is processed afterthe key and IV have been established. Any alterations to the key length,via the "keylen" parameter or the IV length, via the "ivlen" parameter,within the OSSL_PARAM array will not take effect as intended, potentiallycausing truncation or overreading of these values. The following ciphersand cipher modes are impacted: RC2, RC4, RC5, CCM, GCM and OCB.For the CCM, GCM and OCB cipher modes, truncation of the IV can result inloss of confidentiality. For example, when following NIST's SP 800-38Dsection 8.2.1 guidance for constructing a deterministic IV for AES inGCM mode, truncation of the counter portion could lead to IV reuse.Both truncations and overruns of the key and overruns of the IV willproduce incorrect results and could, in some cases, trigger a memoryexception. However, these issues are not currently assessed as securitycritical.Changing the key and/or IV lengths is not considered to be a common operationand the vulnerable API was recently introduced. Furthermore it is likely thatapplication developers will have spotted this problem during testing sincedecryption would fail unless both peers in the communication were similarlyvulnerable. For these reasons we expect the probability of an application beingvulnerable to this to be quite low. However if an application is vulnerable thenthis issue is considered very serious. For these reasons we have assessed thisissue as Moderate severity overall.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this becausethe issue lies outside of the FIPS provider boundary.OpenSSL 3.1 and 3.0 are vulnerable to this issue.

11.21 IP Address: 159.149.130.139

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 1

- High Vulnerabilities: 7

- Medium Vulnerabilities: 18

- Low Vulnerabilities: 5

- Total Vulnerabilities: 31

Services Running on IP Address

- Service: OpenSSH

    - Port: 22
    - Version: 8.7
    - Location:

- Service: Apache httpd

    - Port: 80
    - Version: 2.4.62
    - Location: /

- Service: Apache httpd

    - Port: 443
    - Version: 2.4.62
    - Location: /

Vulnerabilities Found

- Vulnerability: CVE-2016-20012

    - CVSS Score: 4.3
    - Description: OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product

- Vulnerability: CVE-2021-36368

    - CVSS Score: 2.6
    - Description: An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is "this is not an authentication bypass, since nothing is being bypassed.

- Vulnerability: CVE-2008-3844

– CVSS Score: 9.3

– Description: Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, as signed in August 2008 using a legitimate Red Hat GPG key, contain an externally introduced modification (Trojan Horse) that allows the package authors to have an unknown impact. NOTE: since the malicious packages were not distributed from any official Red Hat sources, the scope of this issue is restricted to users who may have obtained these packages through unofficial distribution points. As of 20080827, no unofficial distributions of this software are known.

• Vulnerability: CVE-2023-51767

– CVSS Score: N/A

– Description: OpenSSH through 9.6, when common types of DRAM are used, might allow row hammer attacks (for authentication bypass) because the integer value of authenticated in mm_answer_authpassword does not resist flips of a single bit. NOTE: this is applicable to a certain threat model of attacker-victim co-location in which the attacker has user privileges.

• Vulnerability: CVE-2023-48795

– CVSS Score: N/A

– Description: The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.

• Vulnerability: CVE-2023-38408

– CVSS Score: N/A

- Description: The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009.

- Vulnerability: CVE-2007-2768

  - CVSS Score: 4.3
  - Description: OpenSSH, when using OPIE (One-Time Passwords in Everything) for PAM, allows remote attackers to determine the existence of certain user accounts, which displays a different response if the user account exists and is configured to use one-time passwords (OTP), a similar issue to CVE-2007-2243.

- Vulnerability: CVE-2021-41617

  - CVSS Score: 4.4
  - Description: sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

- Vulnerability: CVE-2023-51385

  - CVSS Score: N/A
  - Description: In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.

- Vulnerability: CVE-2024-6387

  - CVSS Score: N/A
  - Description: A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period.

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2012-4001

  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2013-2220

  - CVSS Score: 7.5
  - Description: Buffer overflow in the radius_get_vendor_attr function in the Radius extension before 1.2.7 for PHP allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a large Vendor Specific Attributes (VSA) length value.

- Vulnerability: CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2009-0796

  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2024-4577

– CVSS Score: N/A

– Description: In PHP versions8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in command line given toWin32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc.

- Vulnerability: CVE-2012-3526

  – CVSS Score: 5

  – Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2013-2765

  – CVSS Score: 5

  – Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2013-4365

  – CVSS Score: 7.5

  – Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2012-4360

  – CVSS Score: 4.3

  – Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2007-3205

  – CVSS Score: 5

  – Description: The parse_str function in (1) PHP, (2) Hardened-PHP, and (3) Suhosin, when called without a second parameter, might allow remote attackers to overwrite arbitrary variables by specifying variable names and values in the string to be parsed. NOTE: it is not clear whether this is a design limitation of the function or a bug in PHP, although it is likely to be regarded as a bug in Hardened-PHP and Suhosin.

- Vulnerability: CVE-2024-5458

  – CVSS Score: N/A

  – Description: In PHP versions8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, due to a code logic error, filtering functions such as filter_var when validating URLs(FILTER_VALIDATE_URL) for certain types of URLs the function will result in invalid user information (username + password part of URLs) being treated as valid user information. This may lead to the downstream code accepting invalid URLs as valid and parsing them incorrectly.

- Vulnerability: CVE-2013-0941

  – CVSS Score: 2.1
  – Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  – CVSS Score: 4.3
  – Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2009-2299

  – CVSS Score: 5
  – Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2013-2765

  – CVSS Score: 5
  – Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2011-1176

  – CVSS Score: 4.3
  – Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2011-2688

  – CVSS Score: 7.5
  – Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2009-0796

  – CVSS Score: 2.6
  – Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2007-4723

– CVSS Score: 7.5

– Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

• Vulnerability: CVE-2012-4001

– CVSS Score: 5

– Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

• Vulnerability: CVE-2013-4365

– CVSS Score: 7.5

– Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

• Vulnerability: CVE-2012-3526

– CVSS Score: 5

– Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

• Vulnerability: CVE-2012-4360

– CVSS Score: 4.3

– Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

11.22   IP Address: 159.149.145.2

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 1

- High Vulnerabilities: 4

- Medium Vulnerabilities: 16

- Low Vulnerabilities: 1

- Total Vulnerabilities: 22

Services Running on IP Address

- Service: OpenSSH

    – Port: 22
    – Version: 8.0
    – Location:

- Service: nginx

    – Port: 80
    – Version: 1.14.1
    – Location: /

- Service: nginx

    – Port: 443
    – Version: 1.14.1
    – Location: /

Vulnerabilities Found

- Vulnerability: CVE-2019-16905

    – CVSS Score: 4.4
    – Description: OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an
                    experimental key type, has a pre-authentication integer overflow if a
                    client or server is configured to use a crafted XMSS key. This leads
                    to memory corruption and local code execution because of an error
                    in the XMSS key parsing algorithm. NOTE: the XMSS implementation is
                    considered experimental in all released OpenSSH versions, and there
                    is no supported way to enable it when building portable OpenSSH.

- Vulnerability: CVE-2016-20012

    – CVSS Score: 4.3
    – Description: OpenSSH through 8.7 allows remote attackers, who have a suspicion
                    that a certain combination of username and public key is known to
                    an SSH server, to test whether this suspicion is correct. This
                    occurs because a challenge is sent only when that combination could
                    be valid for a login session. NOTE: the vendor does not recognize
                    user enumeration as a vulnerability for this product

- Vulnerability: CVE-2021-36368

    – CVSS Score: 2.6

- Description: An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is "this is not an authentication bypass, since nothing is being bypassed.

- Vulnerability: CVE-2020-14145

  - CVSS Score: 4.3
  - Description: The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.

- Vulnerability: CVE-2023-51767

  - CVSS Score: N/A
  - Description: OpenSSH through 9.6, when common types of DRAM are used, might allow row hammer attacks (for authentication bypass) because the integer value of authenticated in mm_answer_authpassword does not resist flips of a single bit. NOTE: this is applicable to a certain threat model of attacker-victim co-location in which the attacker has user privileges.

- Vulnerability: CVE-2020-15778

  - CVSS Score: 6.8
  - Description: scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."

- Vulnerability: CVE-2023-48795

  - CVSS Score: N/A

- Description: The SSH transport protocol with certain OpenSSH extensions,
  found in OpenSSH before 9.6 and other products, allows remote
  attackers to bypass integrity checks such that some packets are
  omitted (from the extension negotiation message), and a client and
  server may consequently end up with a connection for which some
  security features have been downgraded or disabled, aka a Terrapin
  attack. This occurs because the SSH Binary Packet Protocol (BPP),
  implemented by these extensions, mishandles the handshake phase
  and mishandles use of sequence numbers. For example, there is an
  effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with
  Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com
  and (if CBC is used) the -etm@openssh.com MAC algorithms. This also
  affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear
  through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80,
  AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh
  before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway
  before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch
  before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through
  23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0,
  ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before
  2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0,
  ConnectBot SSH library before 2.2.22, Apache MINA sshd through
  2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2
  6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before
  11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before
  5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2,
  Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY
  through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2
  module before 1.15.0 for Node.js, the thrussh library before 0.35.1
  for Rust, and the Russh crate before 0.40.2 for Rust.

- Vulnerability: CVE-2023-38408

  - CVSS Score: N/A
  - Description: The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an
    insufficiently trustworthy search path, leading to remote code
    execution if an agent is forwarded to an attacker-controlled
    system. (Code in /usr/lib is not necessarily safe for loading into
    ssh-agent.) NOTE: this issue exists because of an incomplete fix for
    CVE-2016-10009.

- Vulnerability: CVE-2007-2768

  - CVSS Score: 4.3
  - Description: OpenSSH, when using OPIE (One-Time Passwords in Everything) for PAM,
    allows remote attackers to determine the existence of certain user
    accounts, which displays a different response if the user account
    exists and is configured to use one-time passwords (OTP), a similar
    issue to CVE-2007-2243.

- Vulnerability: CVE-2021-41617

  - CVSS Score: 4.4
  - Description: sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default
    configurations are used, allows privilege escalation because
    supplemental groups are not initialized as expected. Helper programs
    for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run
    with privileges associated with group memberships of the sshd
    process, if the configuration specifies running the command as a
    different user.

- Vulnerability: CVE-2023-51385

- CVSS Score: N/A
- Description: In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.

- Vulnerability: CVE-2008-3844

  - CVSS Score: 9.3
  - Description: Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, as signed in August 2008 using a legitimate Red Hat GPG key, contain an externally introduced modification (Trojan Horse) that allows the package authors to have an unknown impact. NOTE: since the malicious packages were not distributed from any official Red Hat sources, the scope of this issue is restricted to users who may have obtained these packages through unofficial distribution points. As of 20080827, no unofficial distributions of this software are known.

- Vulnerability: CVE-2023-44487

  - CVSS Score: N/A
  - Description: The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

- Vulnerability: CVE-2019-9516

  - CVSS Score: 6.8
  - Description: Some HTTP/2 implementations are vulnerable to a header leak, potentially leading to a denial of service. The attacker sends a stream of headers with a 0-length header name and 0-length header value, optionally Huffman encoded into 1-byte or greater headers. Some implementations allocate memory for these headers and keep the allocation alive until the session dies. This can consume excess memory.

- Vulnerability: CVE-2019-9513

  - CVSS Score: 7.8
  - Description: Some HTTP/2 implementations are vulnerable to resource loops, potentially leading to a denial of service. The attacker creates multiple request streams and continually shuffles the priority of the streams in a way that causes substantial churn to the priority tree. This can consume excess CPU.

- Vulnerability: CVE-2019-9511

  - CVSS Score: 7.8
  - Description: Some HTTP/2 implementations are vulnerable to window size manipulation and stream prioritization manipulation, potentially leading to a denial of service. The attacker requests a large amount of data from a specified resource over multiple streams. They manipulate window size and stream priority to force the server to queue the data in 1-byte chunks. Depending on how efficiently this data is queued, this can consume excess CPU, memory, or both.

- Vulnerability: CVE-2021-23017

  - CVSS Score: 6.8

– Description: A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting in worker process crash or potential other impact.

- Vulnerability: CVE-2021-3618

  – CVSS Score: 5.8

  – Description: ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MiTM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer.

- Vulnerability: CVE-2019-20372

  – CVSS Score: 4.3

  – Description: NGINX before 1.17.7, with certain error_page configurations, allows HTTP request smuggling, as demonstrated by the ability of an attacker to read unauthorized web pages in environments where NGINX is being fronted by a load balancer.

- Vulnerability: CVE-2018-16845

  – CVSS Score: 5.8

  – Description: nginx before versions 1.15.6, 1.14.1 has a vulnerability in the ngx_http_mp4_module, which might allow an attacker to cause infinite loop in a worker process, cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted mp4 file. The issue only affects nginx if it is built with the ngx_http_mp4_module (the module is not built by default) and the .mp4. directive is used in the configuration file. Further, the attack is only possible if an attacker is able to trigger processing of a specially crafted mp4 file with the ngx_http_mp4_module.

- Vulnerability: CVE-2023-44487

  – CVSS Score: N/A

  – Description: The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

- Vulnerability: CVE-2019-9516

  – CVSS Score: 6.8

  – Description: Some HTTP/2 implementations are vulnerable to a header leak, potentially leading to a denial of service. The attacker sends a stream of headers with a 0-length header name and 0-length header value, optionally Huffman encoded into 1-byte or greater headers. Some implementations allocate memory for these headers and keep the allocation alive until the session dies. This can consume excess memory.

- Vulnerability: CVE-2019-9513

  – CVSS Score: 7.8

- Description: Some HTTP/2 implementations are vulnerable to resource loops, potentially leading to a denial of service. The attacker creates multiple request streams and continually shuffles the priority of the streams in a way that causes substantial churn to the priority tree. This can consume excess CPU.

- Vulnerability: CVE-2019-9511

  - CVSS Score: 7.8
  - Description: Some HTTP/2 implementations are vulnerable to window size manipulation and stream prioritization manipulation, potentially leading to a denial of service. The attacker requests a large amount of data from a specified resource over multiple streams. They manipulate window size and stream priority to force the server to queue the data in 1-byte chunks. Depending on how efficiently this data is queued, this can consume excess CPU, memory, or both.

- Vulnerability: CVE-2021-23017

  - CVSS Score: 6.8
  - Description: A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting in worker process crash or potential other impact.

- Vulnerability: CVE-2021-3618

  - CVSS Score: 5.8
  - Description: ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MiTM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer.

- Vulnerability: CVE-2019-20372

  - CVSS Score: 4.3
  - Description: NGINX before 1.17.7, with certain error_page configurations, allows HTTP request smuggling, as demonstrated by the ability of an attacker to read unauthorized web pages in environments where NGINX is being fronted by a load balancer.

- Vulnerability: CVE-2018-16845

  - CVSS Score: 5.8
  - Description: nginx before versions 1.15.6, 1.14.1 has a vulnerability in the ngx_http_mp4_module, which might allow an attacker to cause infinite loop in a worker process, cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted mp4 file. The issue only affects nginx if it is built with the ngx_http_mp4_module (the module is not built by default) and the .mp4. directive is used in the configuration file. Further, the attack is only possible if an attacker is able to trigger processing of a specially crafted mp4 file with the ngx_http_mp4_module.

11.23 IP Address: 159.149.47.69

- Organization: UNI-Milano
- Operating System: N/A
- Critical Vulnerabilities: 1
- High Vulnerabilities: 4
- Medium Vulnerabilities: 16
- Low Vulnerabilities: 1
- Total Vulnerabilities: 22

Services Running on IP Address

- Service: OpenSSH
  - Port: 22
  - Version: 8.0
  - Location:
- Service: nginx
  - Port: 443
  - Version: 1.14.1
  - Location: /

Vulnerabilities Found

- Vulnerability: CVE-2019-16905
  - CVSS Score: 4.4
  - Description: OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.
- Vulnerability: CVE-2016-20012
  - CVSS Score: 4.3
  - Description: OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product
- Vulnerability: CVE-2021-36368
  - CVSS Score: 2.6
  - Description: An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is "this is not an authentication bypass, since nothing is being bypassed.

908

- Vulnerability: CVE-2020-14145

  - CVSS Score: 4.3
  - Description: The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.

- Vulnerability: CVE-2023-51767

  - CVSS Score: N/A
  - Description: OpenSSH through 9.6, when common types of DRAM are used, might allow row hammer attacks (for authentication bypass) because the integer value of authenticated in mm_answer_authpassword does not resist flips of a single bit. NOTE: this is applicable to a certain threat model of attacker-victim co-location in which the attacker has user privileges.

- Vulnerability: CVE-2020-15778

  - CVSS Score: 6.8
  - Description: scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."

- Vulnerability: CVE-2023-48795

  - CVSS Score: N/A

- Description: The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.

- Vulnerability: CVE-2023-38408

  - CVSS Score: N/A
  - Description: The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009.

- Vulnerability: CVE-2007-2768

  - CVSS Score: 4.3
  - Description: OpenSSH, when using OPIE (One-Time Passwords in Everything) for PAM, allows remote attackers to determine the existence of certain user accounts, which displays a different response if the user account exists and is configured to use one-time passwords (OTP), a similar issue to CVE-2007-2243.

- Vulnerability: CVE-2021-41617

  - CVSS Score: 4.4
  - Description: sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

- Vulnerability: CVE-2023-51385

- CVSS Score: N/A
- Description: In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.

- Vulnerability: CVE-2008-3844

  - CVSS Score: 9.3
  - Description: Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, as signed in August 2008 using a legitimate Red Hat GPG key, contain an externally introduced modification (Trojan Horse) that allows the package authors to have an unknown impact. NOTE: since the malicious packages were not distributed from any official Red Hat sources, the scope of this issue is restricted to users who may have obtained these packages through unofficial distribution points. As of 20080827, no unofficial distributions of this software are known.

- Vulnerability: CVE-2023-44487

  - CVSS Score: N/A
  - Description: The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

- Vulnerability: CVE-2019-9516

  - CVSS Score: 6.8
  - Description: Some HTTP/2 implementations are vulnerable to a header leak, potentially leading to a denial of service. The attacker sends a stream of headers with a 0-length header name and 0-length header value, optionally Huffman encoded into 1-byte or greater headers. Some implementations allocate memory for these headers and keep the allocation alive until the session dies. This can consume excess memory.

- Vulnerability: CVE-2019-9513

  - CVSS Score: 7.8
  - Description: Some HTTP/2 implementations are vulnerable to resource loops, potentially leading to a denial of service. The attacker creates multiple request streams and continually shuffles the priority of the streams in a way that causes substantial churn to the priority tree. This can consume excess CPU.

- Vulnerability: CVE-2019-9511

  - CVSS Score: 7.8
  - Description: Some HTTP/2 implementations are vulnerable to window size manipulation and stream prioritization manipulation, potentially leading to a denial of service. The attacker requests a large amount of data from a specified resource over multiple streams. They manipulate window size and stream priority to force the server to queue the data in 1-byte chunks. Depending on how efficiently this data is queued, this can consume excess CPU, memory, or both.

- Vulnerability: CVE-2021-23017

  - CVSS Score: 6.8

- Description: A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting in worker process crash or potential other impact.

- Vulnerability: CVE-2021-3618

  - CVSS Score: 5.8
  - Description: ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MiTM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer.

- Vulnerability: CVE-2019-20372

  - CVSS Score: 4.3
  - Description: NGINX before 1.17.7, with certain error_page configurations, allows HTTP request smuggling, as demonstrated by the ability of an attacker to read unauthorized web pages in environments where NGINX is being fronted by a load balancer.

- Vulnerability: CVE-2018-16845

  - CVSS Score: 5.8
  - Description: nginx before versions 1.15.6, 1.14.1 has a vulnerability in the ngx_http_mp4_module, which might allow an attacker to cause infinite loop in a worker process, cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted mp4 file. The issue only affects nginx if it is built with the ngx_http_mp4_module (the module is not built by default) and the .mp4. directive is used in the configuration file. Further, the attack is only possible if an attacker is able to trigger processing of a specially crafted mp4 file with the ngx_http_mp4_module.

- Vulnerability: CVE-2023-44487

  - CVSS Score: N/A
  - Description: The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

- Vulnerability: CVE-2019-9516

  - CVSS Score: 6.8
  - Description: Some HTTP/2 implementations are vulnerable to a header leak, potentially leading to a denial of service. The attacker sends a stream of headers with a 0-length header name and 0-length header value, optionally Huffman encoded into 1-byte or greater headers. Some implementations allocate memory for these headers and keep the allocation alive until the session dies. This can consume excess memory.

- Vulnerability: CVE-2019-9513

  - CVSS Score: 7.8

– Description: Some HTTP/2 implementations are vulnerable to resource loops, potentially leading to a denial of service. The attacker creates multiple request streams and continually shuffles the priority of the streams in a way that causes substantial churn to the priority tree. This can consume excess CPU.

- Vulnerability: CVE-2019-9511

    – CVSS Score: 7.8
    – Description: Some HTTP/2 implementations are vulnerable to window size manipulation and stream prioritization manipulation, potentially leading to a denial of service. The attacker requests a large amount of data from a specified resource over multiple streams. They manipulate window size and stream priority to force the server to queue the data in 1-byte chunks. Depending on how efficiently this data is queued, this can consume excess CPU, memory, or both.

- Vulnerability: CVE-2021-23017

    – CVSS Score: 6.8
    – Description: A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting in worker process crash or potential other impact.

- Vulnerability: CVE-2021-3618

    – CVSS Score: 5.8
    – Description: ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MiTM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer.

- Vulnerability: CVE-2019-20372

    – CVSS Score: 4.3
    – Description: NGINX before 1.17.7, with certain error_page configurations, allows HTTP request smuggling, as demonstrated by the ability of an attacker to read unauthorized web pages in environments where NGINX is being fronted by a load balancer.

- Vulnerability: CVE-2018-16845

    – CVSS Score: 5.8
    – Description: nginx before versions 1.15.6, 1.14.1 has a vulnerability in the ngx_http_mp4_module, which might allow an attacker to cause infinite loop in a worker process, cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted mp4 file. The issue only affects nginx if it is built with the ngx_http_mp4_module (the module is not built by default) and the .mp4. directive is used in the configuration file. Further, the attack is only possible if an attacker is able to trigger processing of a specially crafted mp4 file with the ngx_http_mp4_module.

11.24 IP Address: 159.149.53.242

- Organization: UNI-Milano

- Operating System: Windows

- Critical Vulnerabilities: 1

- High Vulnerabilities: 1

- Medium Vulnerabilities: 4

- Low Vulnerabilities: 0

- Total Vulnerabilities: 6

Services Running on IP Address

- Service: Microsoft IIS httpd

  - Port: 80
  - Version: 6.0
  - Location: http://studenti.divsi.unimi.it/Default.htm

Vulnerabilities Found

- Vulnerability: CVE-2009-4444

  - CVSS Score: 6
  - Description: Microsoft Internet Information Services (IIS) 5.x and 6.x uses only the portion of a filename before a ; (semicolon) character to determine the file extension, which allows remote attackers to bypass intended extension restrictions of third-party upload applications via a filename with a (1) .asp, (2) .cer, or (3) .asa first extension, followed by a semicolon and a safe extension, as demonstrated by the use of asp.dll to handle a .asp;.jpg file.

- Vulnerability: CVE-2009-4445

  - CVSS Score: 6
  - Description: Microsoft Internet Information Services (IIS), when used in conjunction with unspecified third-party upload applications, allows remote attackers to create empty files with arbitrary extensions via a filename containing an initial extension followed by a : (colon) and a safe extension, as demonstrated by an upload of a .asp:.jpg file that results in creation of an empty .asp file, related to support for the NTFS Alternate Data Streams (ADS) filename syntax. NOTE: it could be argued that this is a vulnerability in the third-party product, not IIS, because the third-party product should be applying its extension restrictions to the portion of the filename before the colon.

- Vulnerability: CVE-2005-2089

  - CVSS Score: 4.3
  - Description: Microsoft IIS 5.0 and 6.0 allows remote attackers to poison the web cache, bypass web application firewall protection, and conduct XSS attacks via an HTTP request with both a "Transfer-Encoding: chunked" header and a Content-Length header, which causes IIS to incorrectly handle and forward the body of the request in a way that causes the receiving server to process it as a separate HTTP request, aka "HTTP Request Smuggling."

- Vulnerability: CVE-2009-1535

  - CVSS Score: 7.5
  - Description: The WebDAV extension in Microsoft Internet Information Services (IIS) 5.1 and 6.0 allows remote attackers to bypass URI-based protection mechanisms, and list folders or read, create, or modify files, via a %c0%af (Unicode / character) at an arbitrary position in the URI, as demonstrated by inserting %c0%af into a "/protected/" initial pathname component to bypass the password protection on the protected\{} folder, aka "IIS 5.1 and 6.0 WebDAV Authentication Bypass Vulnerability," a different vulnerability than CVE-2009-1122.

- Vulnerability: CVE-2009-2521

  - CVSS Score: 5
  - Description: Stack consumption vulnerability in the FTP Service in Microsoft Internet Information Services (IIS) 5.0 through 7.0 allows remote authenticated users to cause a denial of service (daemon crash) via a list (ls) -R command containing a wildcard that references a subdirectory, followed by a .. (dot dot), aka "IIS FTP Service DoS Vulnerability."

- Vulnerability: CVE-2008-1446

  - CVSS Score: 9
  - Description: Integer overflow in the Internet Printing Protocol (IPP) ISAPI extension in Microsoft Internet Information Services (IIS) 5.0 through 7.0 on Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, and Server 2008 allows remote authenticated users to execute arbitrary code via an HTTP POST request that triggers an outbound IPP connection from a web server to a machine operated by the attacker, aka "Integer Overflow in IPP Service Vulnerability."

11.25 IP Address: 159.149.53.244

- Organization: UNI-Milano

- Operating System: Windows

- Critical Vulnerabilities: 1

- High Vulnerabilities: 1

- Medium Vulnerabilities: 4

- Low Vulnerabilities: 0

- Total Vulnerabilities: 6

Services Running on IP Address

- Service: Microsoft IIS httpd

  - Port: 80
  - Version: 6.0
  - Location: http://159.149.53.244/Default.htm

Vulnerabilities Found

- Vulnerability: CVE-2009-4444

  - CVSS Score: 6
  - Description: Microsoft Internet Information Services (IIS) 5.x and 6.x uses only the portion of a filename before a ; (semicolon) character to determine the file extension, which allows remote attackers to bypass intended extension restrictions of third-party upload applications via a filename with a (1) .asp, (2) .cer, or (3) .asa first extension, followed by a semicolon and a safe extension, as demonstrated by the use of asp.dll to handle a .asp;.jpg file.

- Vulnerability: CVE-2009-4445

  - CVSS Score: 6
  - Description: Microsoft Internet Information Services (IIS), when used in conjunction with unspecified third-party upload applications, allows remote attackers to create empty files with arbitrary extensions via a filename containing an initial extension followed by a : (colon) and a safe extension, as demonstrated by an upload of a .asp:.jpg file that results in creation of an empty .asp file, related to support for the NTFS Alternate Data Streams (ADS) filename syntax. NOTE: it could be argued that this is a vulnerability in the third-party product, not IIS, because the third-party product should be applying its extension restrictions to the portion of the filename before the colon.

- Vulnerability: CVE-2005-2089

  - CVSS Score: 4.3
  - Description: Microsoft IIS 5.0 and 6.0 allows remote attackers to poison the web cache, bypass web application firewall protection, and conduct XSS attacks via an HTTP request with both a "Transfer-Encoding: chunked" header and a Content-Length header, which causes IIS to incorrectly handle and forward the body of the request in a way that causes the receiving server to process it as a separate HTTP request, aka "HTTP Request Smuggling."

- Vulnerability: CVE-2009-1535

  – CVSS Score: 7.5
  – Description: The WebDAV extension in Microsoft Internet Information Services (IIS)
                5.1 and 6.0 allows remote attackers to bypass URI-based protection
                mechanisms, and list folders or read, create, or modify files,
                via a %c0%af (Unicode / character) at an arbitrary position in
                the URI, as demonstrated by inserting %c0%af into a "/protected/"
                initial pathname component to bypass the password protection on
                the protected\{} folder, aka "IIS 5.1 and 6.0 WebDAV Authentication
                Bypass Vulnerability," a different vulnerability than CVE-2009-1122.

- Vulnerability: CVE-2009-2521

  – CVSS Score: 5
  – Description: Stack consumption vulnerability in the FTP Service in Microsoft
                Internet Information Services (IIS) 5.0 through 7.0 allows remote
                authenticated users to cause a denial of service (daemon crash)
                via a list (ls) -R command containing a wildcard that references a
                subdirectory, followed by a .. (dot dot), aka "IIS FTP Service DoS
                Vulnerability."

- Vulnerability: CVE-2008-1446

  – CVSS Score: 9
  – Description: Integer overflow in the Internet Printing Protocol (IPP) ISAPI
                extension in Microsoft Internet Information Services (IIS) 5.0
                through 7.0 on Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1
                and SP2, and Server 2008 allows remote authenticated users to execute
                arbitrary code via an HTTP POST request that triggers an outbound IPP
                connection from a web server to a machine operated by the attacker,
                aka "Integer Overflow in IPP Service Vulnerability."

11.26 IP Address: 185.221.216.115

- Organization: Global Managed Hosting Inc.

- Operating System: N/A

- Critical Vulnerabilities: 1

- High Vulnerabilities: 0

- Medium Vulnerabilities: 11

- Low Vulnerabilities: 2

- Total Vulnerabilities: 14

Services Running on IP Address

- Service: OpenSSH

  – Port: 22
  – Version: 7.4
  – Location:

- Service: N/A

  – Port: 53
  – Version: N/A
  – Location:

- Service: N/A

  – Port: 53
  – Version: N/A
  – Location:

- Service: Apache httpd

  – Port: 80
  – Version: N/A
  – Location: /

- Service: N/A

  – Port: 110
  – Version: N/A
  – Location:

- Service: N/A

  – Port: 143
  – Version: N/A
  – Location:

- Service: Apache httpd

  – Port: 443
  – Version: N/A
  – Location: /

- Service: Exim smtpd

- Port: 587
- Version: 4.97.1
- Location:

- Service: N/A
  - Port: 993
  - Version: N/A
  - Location:

- Service: N/A
  - Port: 995
  - Version: N/A
  - Location:

- Service: N/A
  - Port: 2079
  - Version: N/A
  - Location: https://cpanel.system.com:2080/

- Service: N/A
  - Port: 2082
  - Version: N/A
  - Location: https://185.221.216.115:2083/

- Service: cPanel
  - Port: 2083
  - Version: N/A
  - Location: /

- Service: N/A
  - Port: 2086
  - Version: N/A
  - Location: https://cpanel.system.com:2087/

- Service: N/A
  - Port: 2087
  - Version: N/A
  - Location:

- Service: MariaDB
  - Port: 3306
  - Version: N/A
  - Location:

Vulnerabilities Found

- Vulnerability: CVE-2008-3844

  – CVSS Score: 9.3

  – Description: Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, as signed in August 2008 using a legitimate Red Hat GPG key, contain an externally introduced modification (Trojan Horse) that allows the package authors to have an unknown impact. NOTE: since the malicious packages were not distributed from any official Red Hat sources, the scope of this issue is restricted to users who may have obtained these packages through unofficial distribution points. As of 20080827, no unofficial distributions of this software are known.

- Vulnerability: CVE-2019-6110

  – CVSS Score: 4

  – Description: In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.

- Vulnerability: CVE-2016-20012

  – CVSS Score: 4.3

  – Description: OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product

- Vulnerability: CVE-2018-15919

  – CVSS Score: 5

  – Description: Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'

- Vulnerability: CVE-2018-15473

  – CVSS Score: 5

  – Description: OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.

- Vulnerability: CVE-2021-36368

  – CVSS Score: 2.6

  – Description: An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is "this is not an authentication bypass, since nothing is being bypassed.

- Vulnerability: CVE-2017-15906

- CVSS Score: 5
- Description: The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.

- Vulnerability: CVE-2018-20685

  - CVSS Score: 2.6
  - Description: In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.

- Vulnerability: CVE-2020-14145

  - CVSS Score: 4.3
  - Description: The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.

- Vulnerability: CVE-2023-51767

  - CVSS Score: N/A
  - Description: OpenSSH through 9.6, when common types of DRAM are used, might allow row hammer attacks (for authentication bypass) because the integer value of authenticated in mm_answer_authpassword does not resist flips of a single bit. NOTE: this is applicable to a certain threat model of attacker-victim co-location in which the attacker has user privileges.

- Vulnerability: CVE-2020-15778

  - CVSS Score: 6.8
  - Description: scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."

- Vulnerability: CVE-2023-48795

  - CVSS Score: N/A

- Description: The SSH transport protocol with certain OpenSSH extensions,
              found in OpenSSH before 9.6 and other products, allows remote
              attackers to bypass integrity checks such that some packets are
              omitted (from the extension negotiation message), and a client and
              server may consequently end up with a connection for which some
              security features have been downgraded or disabled, aka a Terrapin
              attack. This occurs because the SSH Binary Packet Protocol (BPP),
              implemented by these extensions, mishandles the handshake phase
              and mishandles use of sequence numbers. For example, there is an
              effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with
              Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com
              and (if CBC is used) the -etm@openssh.com MAC algorithms. This also
              affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear
              through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80,
              AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh
              before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway
              before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch
              before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through
              23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0,
              ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before
              2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0,
              ConnectBot SSH library before 2.2.22, Apache MINA sshd through
              2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2
              6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before
              11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before
              5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2,
              Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY
              through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2
              module before 1.15.0 for Node.js, the thrussh library before 0.35.1
              for Rust, and the Russh crate before 0.40.2 for Rust.

- Vulnerability: CVE-2023-38408

  - CVSS Score: N/A
  - Description: The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an
              insufficiently trustworthy search path, leading to remote code
              execution if an agent is forwarded to an attacker-controlled
              system. (Code in /usr/lib is not necessarily safe for loading into
              ssh-agent.) NOTE: this issue exists because of an incomplete fix for
              CVE-2016-10009.

- Vulnerability: CVE-2007-2768

  - CVSS Score: 4.3
  - Description: OpenSSH, when using OPIE (One-Time Passwords in Everything) for PAM,
              allows remote attackers to determine the existence of certain user
              accounts, which displays a different response if the user account
              exists and is configured to use one-time passwords (OTP), a similar
              issue to CVE-2007-2243.

- Vulnerability: CVE-2021-41617

  - CVSS Score: 4.4
  - Description: sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default
              configurations are used, allows privilege escalation because
              supplemental groups are not initialized as expected. Helper programs
              for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run
              with privileges associated with group memberships of the sshd
              process, if the configuration specifies running the command as a
              different user.

- Vulnerability: CVE-2019-6111

- CVSS Score: 5.8
- Description: An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).

- Vulnerability: CVE-2023-51385

  - CVSS Score: N/A
  - Description: In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.

- Vulnerability: CVE-2019-6109

  - CVSS Score: 4
  - Description: An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.

11.27 IP Address: 159.149.147.136

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 1

- High Vulnerabilities: 0

- Medium Vulnerabilities: 11

- Low Vulnerabilities: 2

- Total Vulnerabilities: 14

Services Running on IP Address

- Service: OpenSSH

  - Port: 22
  - Version: 7.4
  - Location:

Vulnerabilities Found

- Vulnerability: CVE-2008-3844

  - CVSS Score: 9.3
  - Description: Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, as signed in August 2008 using a legitimate Red Hat GPG key, contain an externally introduced modification (Trojan Horse) that allows the package authors to have an unknown impact. NOTE: since the malicious packages were not distributed from any official Red Hat sources, the scope of this issue is restricted to users who may have obtained these packages through unofficial distribution points. As of 20080827, no unofficial distributions of this software are known.

- Vulnerability: CVE-2019-6110

  - CVSS Score: 4
  - Description: In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.

- Vulnerability: CVE-2016-20012

  - CVSS Score: 4.3
  - Description: OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product

- Vulnerability: CVE-2018-15919

  - CVSS Score: 5
  - Description: Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'

- Vulnerability: CVE-2018-15473

  – CVSS Score: 5
  – Description: OpenSSH through 7.7 is prone to a user enumeration vulnerability
                  due to not delaying bailout for an invalid authenticating user
                  until after the packet containing the request has been fully parsed,
                  related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.

- Vulnerability: CVE-2021-36368

  – CVSS Score: 2.6
  – Description: An issue was discovered in OpenSSH before 8.9. If a client is
                  using public-key authentication with agent forwarding but without
                  -oLogLevel=verbose, and an attacker has silently modified the
                  server to support the None authentication option, then the user
                  cannot determine whether FIDO authentication is going to confirm
                  that the user wishes to connect to that server, or that the user
                  wishes to allow that server to connect to a different server on
                  the user's behalf. NOTE: the vendor's position is "this is not an
                  authentication bypass, since nothing is being bypassed.

- Vulnerability: CVE-2017-15906

  – CVSS Score: 5
  – Description: The process_open function in sftp-server.c in OpenSSH before 7.6 does
                  not properly prevent write operations in readonly mode, which allows
                  attackers to create zero-length files.

- Vulnerability: CVE-2018-20685

  – CVSS Score: 2.6
  – Description: In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers
                  to bypass intended access restrictions via the filename of . or
                  an empty filename. The impact is modifying the permissions of the
                  target directory on the client side.

- Vulnerability: CVE-2020-14145

  – CVSS Score: 4.3
  – Description: The client side in OpenSSH 5.7 through 8.4 has an Observable
                  Discrepancy leading to an information leak in the algorithm
                  negotiation. This allows man-in-the-middle attackers to target
                  initial connection attempts (where no host key for the server has
                  been cached by the client). NOTE: some reports state that 8.5 and
                  8.6 are also affected.

- Vulnerability: CVE-2023-51767

  – CVSS Score: N/A
  – Description: OpenSSH through 9.6, when common types of DRAM are used, might allow
                  row hammer attacks (for authentication bypass) because the integer
                  value of authenticated in mm_answer_authpassword does not resist
                  flips of a single bit. NOTE: this is applicable to a certain threat
                  model of attacker-victim co-location in which the attacker has user
                  privileges.

- Vulnerability: CVE-2020-15778

  – CVSS Score: 6.8

- Description: scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."

- Vulnerability: CVE-2023-48795

  - CVSS Score: N/A

  - Description: The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.

- Vulnerability: CVE-2023-38408

  - CVSS Score: N/A

  - Description: The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009.

- Vulnerability: CVE-2007-2768

  - CVSS Score: 4.3

  - Description: OpenSSH, when using OPIE (One-Time Passwords in Everything) for PAM, allows remote attackers to determine the existence of certain user accounts, which displays a different response if the user account exists and is configured to use one-time passwords (OTP), a similar issue to CVE-2007-2243.

- Vulnerability: CVE-2021-41617

- CVSS Score: 4.4
- Description: sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

- Vulnerability: CVE-2019-6111

  - CVSS Score: 5.8
  - Description: An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).

- Vulnerability: CVE-2023-51385

  - CVSS Score: N/A
  - Description: In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.

- Vulnerability: CVE-2019-6109

  - CVSS Score: 4
  - Description: An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.

11.28 IP Address: 159.149.130.182

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 1

- High Vulnerabilities: 0

- Medium Vulnerabilities: 7

- Low Vulnerabilities: 0

- Total Vulnerabilities: 8

Services Running on IP Address

- Service: OpenSSH

    - Port: 22
    - Version: 9.6
    - Location:

- Service: N/A

    - Port: 80
    - Version: N/A
    - Location: https://grew.di.unimi.it/

- Service: nginx

    - Port: 443
    - Version: 1.27.0
    - Location: /

Vulnerabilities Found

- Vulnerability: CVE-2007-2768

    - CVSS Score: 4.3
    - Description: OpenSSH, when using OPIE (One-Time Passwords in Everything) for PAM, allows remote attackers to determine the existence of certain user accounts, which displays a different response if the user account exists and is configured to use one-time passwords (OTP), a similar issue to CVE-2007-2243.

- Vulnerability: CVE-2008-3844

    - CVSS Score: 9.3
    - Description: Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, as signed in August 2008 using a legitimate Red Hat GPG key, contain an externally introduced modification (Trojan Horse) that allows the package authors to have an unknown impact. NOTE: since the malicious packages were not distributed from any official Red Hat sources, the scope of this issue is restricted to users who may have obtained these packages through unofficial distribution points. As of 20080827, no unofficial distributions of this software are known.

- Vulnerability: CVE-2024-6387

    - CVSS Score: N/A

– Description: A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period.

- Vulnerability: CVE-2023-51767

  – CVSS Score: N/A

  – Description: OpenSSH through 9.6, when common types of DRAM are used, might allow row hammer attacks (for authentication bypass) because the integer value of authenticated in mm_answer_authpassword does not resist flips of a single bit. NOTE: this is applicable to a certain threat model of attacker-victim co-location in which the attacker has user privileges.

- Vulnerability: CVE-2019-11358

  – CVSS Score: 4.3

  – Description: jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.

- Vulnerability: CVE-2020-7656

  – CVSS Score: 4.3

  – Description: jquery prior to 1.9.0 allows Cross-site Scripting attacks via the load method. The load method fails to recognize and remove "<script>" HTML tags that contain a whitespace character, i.e: "</script >", which results in the enclosed script logic to be executed.

- Vulnerability: CVE-2015-9251

  – CVSS Score: 4.3

  – Description: jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.

- Vulnerability: CVE-2012-6708

  – CVSS Score: 4.3

  – Description: jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

- Vulnerability: CVE-2020-11022

  – CVSS Score: 4.3

  – Description: In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources – even after sanitizing it – to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

- Vulnerability: CVE-2020-11023

  – CVSS Score: 4.3

  – Description: In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources – even after sanitizing it – to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

11.29   IP Address: 92.42.111.202

- Organization: Communication and Digital Media of Eastern Mediterranean P.C.

- Operating System: N/A

- Critical Vulnerabilities: 1

- High Vulnerabilities: 0

- Medium Vulnerabilities: 6

- Low Vulnerabilities: 1

- Total Vulnerabilities: 8

Services Running on IP Address

- Service: N/A

    - Port: 53
    - Version: N/A
    - Location:

- Service: N/A

    - Port: 53
    - Version: N/A
    - Location:

- Service: Apache httpd

    - Port: 80
    - Version: N/A
    - Location: https://m-logos.gr/

- Service: N/A

    - Port: 143
    - Version: N/A
    - Location:

- Service: Apache httpd

    - Port: 443
    - Version: N/A
    - Location: /

- Service: Exim smtpd

    - Port: 465
    - Version: 4.97.1
    - Location:

- Service: Exim smtpd

    - Port: 587
    - Version: 4.97.1
    - Location:

- Service: N/A

- Port: 993
- Version: N/A
- Location:

• Service: N/A

- Port: 995
- Version: N/A
- Location:

• Service: N/A

- Port: 2082
- Version: N/A
- Location: https://electra.media42.eu:2083/

• Service: N/A

- Port: 2083
- Version: N/A
- Location: https://electra.media42.eu:2083

• Service: N/A

- Port: 2086
- Version: N/A
- Location: https://electra.media42.eu:2087/

• Service: N/A

- Port: 2087
- Version: N/A
- Location:

• Service: N/A

- Port: 2096
- Version: N/A
- Location: https://electra.media42.eu:2096

• Service: OpenSSH

- Port: 8816
- Version: 8.0
- Location:

Vulnerabilities Found

• Vulnerability: CVE-2019-16905

- CVSS Score: 4.4
- Description: OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.

- Vulnerability: CVE-2016-20012

  - CVSS Score: 4.3
  - Description: OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product

- Vulnerability: CVE-2021-36368

  - CVSS Score: 2.6
  - Description: An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is "this is not an authentication bypass, since nothing is being bypassed.

- Vulnerability: CVE-2020-14145

  - CVSS Score: 4.3
  - Description: The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.

- Vulnerability: CVE-2023-51767

  - CVSS Score: N/A
  - Description: OpenSSH through 9.6, when common types of DRAM are used, might allow row hammer attacks (for authentication bypass) because the integer value of authenticated in mm_answer_authpassword does not resist flips of a single bit. NOTE: this is applicable to a certain threat model of attacker-victim co-location in which the attacker has user privileges.

- Vulnerability: CVE-2020-15778

  - CVSS Score: 6.8
  - Description: scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."

- Vulnerability: CVE-2023-48795

  - CVSS Score: N/A

- Description: The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.

- **Vulnerability:** CVE-2023-38408

  - CVSS Score: N/A
  - Description: The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009.

- **Vulnerability:** CVE-2007-2768

  - CVSS Score: 4.3
  - Description: OpenSSH, when using OPIE (One-Time Passwords in Everything) for PAM, allows remote attackers to determine the existence of certain user accounts, which displays a different response if the user account exists and is configured to use one-time passwords (OTP), a similar issue to CVE-2007-2243.

- **Vulnerability:** CVE-2021-41617

  - CVSS Score: 4.4
  - Description: sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

- **Vulnerability:** CVE-2023-51385

– CVSS Score: N/A

– Description: In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.

- Vulnerability: CVE-2008-3844

    – CVSS Score: 9.3

    – Description: Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, as signed in August 2008 using a legitimate Red Hat GPG key, contain an externally introduced modification (Trojan Horse) that allows the package authors to have an unknown impact. NOTE: since the malicious packages were not distributed from any official Red Hat sources, the scope of this issue is restricted to users who may have obtained these packages through unofficial distribution points. As of 20080827, no unofficial distributions of this software are known.

11.30   IP Address: 159.149.145.130

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 1

- High Vulnerabilities: 0

- Medium Vulnerabilities: 3

- Low Vulnerabilities: 0

- Total Vulnerabilities: 4

Services Running on IP Address

- Service: OpenSSH

    – Port: 22
    – Version: 8.9p1 Ubuntu-3ubuntu0.10
    – Location:

- Service: N/A

    – Port: 80
    – Version: N/A
    – Location: https://159.149.145.130/

- Service: nginx

    – Port: 443
    – Version: 1.19.0
    – Location: /

- Service: OpenSSH

    – Port: 2222
    – Version: 9.3
    – Location:

Vulnerabilities Found

- Vulnerability: CVE-2023-44487

    – CVSS Score: N/A
    – Description: The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

- Vulnerability: CVE-2021-23017

    – CVSS Score: 6.8
    – Description: A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting in worker process crash or potential other impact.

- Vulnerability: CVE-2021-3618

    – CVSS Score: 5.8

- Description: ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MiTM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer.

- Vulnerability: CVE-2008-3844

  - CVSS Score: 9.3
  - Description: Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, as signed in August 2008 using a legitimate Red Hat GPG key, contain an externally introduced modification (Trojan Horse) that allows the package authors to have an unknown impact. NOTE: since the malicious packages were not distributed from any official Red Hat sources, the scope of this issue is restricted to users who may have obtained these packages through unofficial distribution points. As of 20080827, no unofficial distributions of this software are known.

- Vulnerability: CVE-2023-51767

  - CVSS Score: N/A
  - Description: OpenSSH through 9.6, when common types of DRAM are used, might allow row hammer attacks (for authentication bypass) because the integer value of authenticated in mm_answer_authpassword does not resist flips of a single bit. NOTE: this is applicable to a certain threat model of attacker-victim co-location in which the attacker has user privileges.

- Vulnerability: CVE-2023-48795

  - CVSS Score: N/A

- Description: The SSH transport protocol with certain OpenSSH extensions,
  found in OpenSSH before 9.6 and other products, allows remote
  attackers to bypass integrity checks such that some packets are
  omitted (from the extension negotiation message), and a client and
  server may consequently end up with a connection for which some
  security features have been downgraded or disabled, aka a Terrapin
  attack. This occurs because the SSH Binary Packet Protocol (BPP),
  implemented by these extensions, mishandles the handshake phase
  and mishandles use of sequence numbers. For example, there is an
  effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with
  Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com
  and (if CBC is used) the -etm@openssh.com MAC algorithms. This also
  affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear
  through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80,
  AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh
  before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway
  before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch
  before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through
  23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0,
  ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before
  2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0,
  ConnectBot SSH library before 2.2.22, Apache MINA sshd through
  2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2
  6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before
  11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before
  5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2,
  Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY
  through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2
  module before 1.15.0 for Node.js, the thrussh library before 0.35.1
  for Rust, and the Russh crate before 0.40.2 for Rust.

- Vulnerability: CVE-2023-38408

  - CVSS Score: N/A
  - Description: The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an
    insufficiently trustworthy search path, leading to remote code
    execution if an agent is forwarded to an attacker-controlled
    system. (Code in /usr/lib is not necessarily safe for loading into
    ssh-agent.) NOTE: this issue exists because of an incomplete fix for
    CVE-2016-10009.

- Vulnerability: CVE-2007-2768

  - CVSS Score: 4.3
  - Description: OpenSSH, when using OPIE (One-Time Passwords in Everything) for PAM,
    allows remote attackers to determine the existence of certain user
    accounts, which displays a different response if the user account
    exists and is configured to use one-time passwords (OTP), a similar
    issue to CVE-2007-2243.

- Vulnerability: CVE-2023-51384

  - CVSS Score: N/A
  - Description: In ssh-agent in OpenSSH before 9.6, certain destination constraints
    can be incompletely applied. When destination constraints are
    specified during addition of PKCS#11-hosted private keys, these
    constraints are only applied to the first key, even if a PKCS#11
    token returns multiple keys.

- Vulnerability: CVE-2023-51385

  - CVSS Score: N/A

- Description: In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.

- Vulnerability: CVE-2024-6387

  - CVSS Score: N/A
  - Description: A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period.

11.31 IP Address: 159.149.129.213

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 1

- High Vulnerabilities: 0

- Medium Vulnerabilities: 1

- Low Vulnerabilities: 0

- Total Vulnerabilities: 2

Services Running on IP Address

- Service: OpenSSH

    - Port: 22
    - Version: 9.3
    - Location:

- Service: nginx

    - Port: 80
    - Version: 1.24.0
    - Location: https://logic-ai.ricerca.di.unimi.it/

- Service: nginx

    - Port: 443
    - Version: 1.24.0
    - Location: /

Vulnerabilities Found

- Vulnerability: CVE-2008-3844

    - CVSS Score: 9.3
    - Description: Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, as signed in August 2008 using a legitimate Red Hat GPG key, contain an externally introduced modification (Trojan Horse) that allows the package authors to have an unknown impact. NOTE: since the malicious packages were not distributed from any official Red Hat sources, the scope of this issue is restricted to users who may have obtained these packages through unofficial distribution points. As of 20080827, no unofficial distributions of this software are known.

- Vulnerability: CVE-2023-51767

    - CVSS Score: N/A
    - Description: OpenSSH through 9.6, when common types of DRAM are used, might allow row hammer attacks (for authentication bypass) because the integer value of authenticated in mm_answer_authpassword does not resist flips of a single bit. NOTE: this is applicable to a certain threat model of attacker-victim co-location in which the attacker has user privileges.

- Vulnerability: CVE-2023-48795

    - CVSS Score: N/A

- Description: The SSH transport protocol with certain OpenSSH extensions,
  found in OpenSSH before 9.6 and other products, allows remote
  attackers to bypass integrity checks such that some packets are
  omitted (from the extension negotiation message), and a client and
  server may consequently end up with a connection for which some
  security features have been downgraded or disabled, aka a Terrapin
  attack. This occurs because the SSH Binary Packet Protocol (BPP),
  implemented by these extensions, mishandles the handshake phase
  and mishandles use of sequence numbers. For example, there is an
  effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with
  Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com
  and (if CBC is used) the -etm@openssh.com MAC algorithms. This also
  affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear
  through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80,
  AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh
  before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway
  before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch
  before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through
  23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0,
  ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before
  2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0,
  ConnectBot SSH library before 2.2.22, Apache MINA sshd through
  2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2
  6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before
  11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before
  5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2,
  Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY
  through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2
  module before 1.15.0 for Node.js, the thrussh library before 0.35.1
  for Rust, and the Russh crate before 0.40.2 for Rust.

- Vulnerability: CVE-2023-38408

  - CVSS Score: N/A
  - Description: The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an
    insufficiently trustworthy search path, leading to remote code
    execution if an agent is forwarded to an attacker-controlled
    system. (Code in /usr/lib is not necessarily safe for loading into
    ssh-agent.) NOTE: this issue exists because of an incomplete fix for
    CVE-2016-10009.

- Vulnerability: CVE-2007-2768

  - CVSS Score: 4.3
  - Description: OpenSSH, when using OPIE (One-Time Passwords in Everything) for PAM,
    allows remote attackers to determine the existence of certain user
    accounts, which displays a different response if the user account
    exists and is configured to use one-time passwords (OTP), a similar
    issue to CVE-2007-2243.

- Vulnerability: CVE-2023-51384

  - CVSS Score: N/A
  - Description: In ssh-agent in OpenSSH before 9.6, certain destination constraints
    can be incompletely applied. When destination constraints are
    specified during addition of PKCS#11-hosted private keys, these
    constraints are only applied to the first key, even if a PKCS#11
    token returns multiple keys.

- Vulnerability: CVE-2023-51385

  - CVSS Score: N/A

– Description: In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.

- Vulnerability: CVE-2024-6387

  – CVSS Score: N/A

  – Description: A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period.

11.32 IP Address: 159.149.15.69

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 25

- Medium Vulnerabilities: 79

- Low Vulnerabilities: 7

- Total Vulnerabilities: 111

Services Running on IP Address

- Service: Apache httpd

    – Port: 80
    – Version: 2.4.41
    – Location: https://infermieristica.ctu.unimi.it/

- Service: Apache httpd

    – Port: 443
    – Version: 2.4.41
    – Location: /

Vulnerabilities Found

- Vulnerability: CVE-2024-27316

    – CVSS Score: N/A
    – Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

- Vulnerability: CVE-2013-2765

    – CVSS Score: 5
    – Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2020-1934

    – CVSS Score: 5
    – Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

- Vulnerability: CVE-2022-36760

    – CVSS Score: N/A
    – Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2020-35452

- CVSS Score: 6.8
- Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

- Vulnerability: CVE-2022-29404

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2023-27522

  - CVSS Score: N/A
  - Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.Special characters in the origin response header can truncate/split the response forwarded to the client.

- Vulnerability: CVE-2009-0796

  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2013-4365

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2022-22720

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2021-30641

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.39 to 2.4.46 Unexpected matching behavior with 'MergeSlashes OFF'

- Vulnerability: CVE-2022-28330

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2020-11993

  - CVSS Score: 4.3

- Description: Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug
    was enabled for the HTTP/2 module and on certain traffic edge
    patterns, logging statements were made on the wrong connection,
    causing concurrent use of memory pools. Configuring the LogLevel of
    mod_http2 above "info" will mitigate this vulnerability for unpatched
    servers.

- Vulnerability: CVE-2021-32791

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the
    Apache 2.x HTTP server that functions as an OpenID Connect Relying
    Party, authenticating users against an OpenID Connect Provider.
    In mod_auth_openidc before version 2.4.9, the AES GCM encryption in
    mod_auth_openidc uses a static IV and AAD. It is important to fix
    because this creates a static nonce and since aes-gcm is a stream
    cipher, this can lead to known cryptographic issues, since the same
    key is being reused. From 2.4.9 onwards this has been patched to use
    dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2021-32792

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the
    Apache 2.x HTTP server that functions as an OpenID Connect Relying
    Party, authenticating users against an OpenID Connect Provider. In
    mod_auth_openidc before version 2.4.9, there is an XSS vulnerability
    in when using 'OIDCPreservePost On'.

- Vulnerability: CVE-2023-31122

  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP
    Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2024-38476

  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are
    vulnerably to information disclosure, SSRF or local script execution
    viabackend applications whose response headers are malicious or
    exploitable.Users are recommended to upgrade to version 2.4.60, which
    fixes this issue.

- Vulnerability: CVE-2024-38477

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59
    and earlier allows an attacker to crash the server via a malicious
    request.Users are recommended to upgrade to version 2.4.60, which
    fixes this issue.

- Vulnerability: CVE-2024-38474

  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server
    2.4.59 and earlier allows attacker to execute scripts indirectories
    permitted by the configuration but not directly reachable by anyURL
    or source disclosure of scripts meant to only to be executed as
    CGI.Users are recommended to upgrade to version 2.4.60, which fixes
    this issue.Some RewriteRules that capture and substitute unsafely
    will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2022-22721

  - CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2006-20001

  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2021-33193

  - CVSS Score: 5
  - Description: A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2019-17567

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

- Vulnerability: CVE-2012-3526

  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2022-31813

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

- Vulnerability: CVE-2012-4001

  - CVSS Score: 5

– Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2022-37436

  – CVSS Score: N/A
  – Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2012-4360

  – CVSS Score: 4.3
  – Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2021-40438

  – CVSS Score: 6.8
  – Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2011-1176

  – CVSS Score: 4.3
  – Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2021-36160

  – CVSS Score: 5
  – Description: A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS). This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48 (inclusive).

- Vulnerability: CVE-2022-23943

  – CVSS Score: 7.5
  – Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

- Vulnerability: CVE-2020-1927

  – CVSS Score: 5.8
  – Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.

- Vulnerability: CVE-2011-2688

  – CVSS Score: 7.5

- Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2021-34798

  - CVSS Score: 5
  - Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2023-25690

  - CVSS Score: N/A
  - Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2021-32786

  - CVSS Score: 5.8
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, 'oidc_validate_redirect_url()' does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring 'mod_auth_openidc' to only allow redirection whose destination matches a given regular expression.

- Vulnerability: CVE-2021-32785

  - CVSS Score: 4.3

– Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache ('OIDCCacheEncrypt off', 'OIDCSessionType server-cache', 'OIDCCacheType redis'), 'mod_auth_openidc' wrongly performed argument interpolation before passing Redis requests to 'hiredis', which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the 'hiredis' API. As a workaround, this vulnerability can be mitigated by setting 'OIDCCacheEncrypt' to 'on', as cache keys are cryptographically hashed before use when this option is enabled.

• Vulnerability: CVE-2020-9490

  – CVSS Score: 5

  – Description: Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.

• Vulnerability: CVE-2021-44224

  – CVSS Score: 6.4

  – Description: A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).

• Vulnerability: CVE-2007-4723

  – CVSS Score: 7.5

  – Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

• Vulnerability: CVE-2020-11984

  – CVSS Score: 7.5

  – Description: Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE

• Vulnerability: CVE-2021-44790

  – CVSS Score: 7.5

  – Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

• Vulnerability: CVE-2013-0942

- CVSS Score: 4.3
- Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication
  Agent 7.1 before 7.1.1 for Web for Internet Information Services,
  and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to
  inject arbitrary web script or HTML via unspecified vectors.

- **Vulnerability:** CVE-2021-26690

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted
    Cookie header handled by mod_session can cause a NULL pointer
    dereference and crash, leading to a possible Denial Of Service

- **Vulnerability:** CVE-2021-26691

  - CVSS Score: 7.5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted
    SessionHeader sent by an origin server could cause a heap overflow

- **Vulnerability:** CVE-2022-26377

  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request
    Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server
    allows an attacker to smuggle requests to the AJP server it forwards
    requests to. This issue affects Apache HTTP Server Apache HTTP
    Server 2.4 version 2.4.53 and prior versions.

- **Vulnerability:** CVE-2023-45802

  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a
    time window were the request's memory resources were not reclaimed
    immediately. Instead, de-allocation was deferred to connection
    close. A client could send new requests and resets, keeping the
    connection busy and open and causing the memory footprint to keep
    on growing. On connection close, all resources were reclaimed, but
    the process might run out of memory before that.This was found by
    the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset
    Exploit) with their own test client. During "normal" HTTP/2 use, the
    probability to hit this bug is very low. The kept memory would not
    become noticeable before the connection closes or times out.Users are
    recommended to upgrade to version 2.4.58, which fixes the issue.

- **Vulnerability:** CVE-2022-28614

  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier
    may read unintended memory if an attacker can cause the server to
    reflect very large input using ap_rwrite() or ap_rputs(), such as
    with mod_luas r:puts() function. Modules compiled and distributed
    separately from Apache HTTP Server that use the 'ap_rputs' function
    and may pass it a very large (INT_MAX or larger) string must be
    compiled against current headers to resolve the issue.

- **Vulnerability:** CVE-2020-13938

  - CVSS Score: 2.1
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users
    can stop httpd on Windows

- **Vulnerability:** CVE-2009-2299

- CVSS Score: 5
- Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- **Vulnerability:** CVE-2020-13950

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.41 to 2.4.46 mod_proxy_http can be made to crash (NULL pointer dereference) with specially crafted requests using both Content-Length and Transfer-Encoding headers, leading to a Denial of Service

- **Vulnerability:** CVE-2024-40898

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- **Vulnerability:** CVE-2021-39275

  - CVSS Score: 7.5
  - Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

- **Vulnerability:** CVE-2022-28615

  - CVSS Score: 6.4
  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- **Vulnerability:** CVE-2022-30556

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- **Vulnerability:** CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- **Vulnerability:** CVE-2023-5544

  - CVSS Score: N/A
  - Description: Wiki comments required additional sanitizing and access restrictions to prevent a stored XSS risk and potential IDOR risk.

- **Vulnerability:** CVE-2023-5545

- CVSS Score: N/A
- Description: H5P metadata automatically populated the author with the user's username, which could be sensitive information.

- **Vulnerability:** CVE-2023-5547

  - CVSS Score: N/A
  - Description: The course upload preview contained an XSS risk for users uploading unsafe data.

- **Vulnerability:** CVE-2023-5540

  - CVSS Score: N/A
  - Description: A remote code execution risk was identified in the IMSCP activity. By default this was only available to teachers and managers.

- **Vulnerability:** CVE-2023-5541

  - CVSS Score: N/A
  - Description: The CSV grade import method contained an XSS risk for users importing the spreadsheet, if it contained unsafe content.

- **Vulnerability:** CVE-2023-5548

  - CVSS Score: N/A
  - Description: Stronger revision number limitations were required on file serving endpoints to improve cache poisoning protection.

- **Vulnerability:** CVE-2023-5549

  - CVSS Score: N/A
  - Description: Insufficient web service capability checks made it possible to move categories a user had permission to manage, to a parent category they did not have the capability to manage.

- **Vulnerability:** CVE-2023-23921

  - CVSS Score: N/A
  - Description: The vulnerability was found Moodle which exists due to insufficient sanitization of user-supplied data in some returnurl parameters. A remote attacker can trick the victim to follow a specially crafted link and execute arbitrary HTML and script code in user's browser in context of vulnerable website. This flaw allows a remote attacker to perform cross-site scripting (XSS) attacks.

- **Vulnerability:** CVE-2021-32786

  - CVSS Score: 5.8
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, 'oidc_validate_redirect_url()' does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring 'mod_auth_openidc' to only allow redirection whose destination matches a given regular expression.

- **Vulnerability:** CVE-2022-40313

- CVSS Score: N/A
- Description: Recursive rendering of Mustache template helpers containing user input could, in some cases, result in an XSS risk or a page failing to load.

- **Vulnerability: CVE-2024-38276**

  - CVSS Score: N/A
  - Description: Incorrect CSRF token checks resulted in multiple CSRF risks.

- **Vulnerability: CVE-2021-40693**

  - CVSS Score: N/A
  - Description: An authentication bypass risk was identified in the external database authentication functionality, due to a type juggling vulnerability.

- **Vulnerability: CVE-2022-40316**

  - CVSS Score: N/A
  - Description: The H5P activity attempts report did not filter by groups, which in separate groups mode could reveal information to non-editing teachers about attempts/users in groups they should not have access to.

- **Vulnerability: CVE-2021-40695**

  - CVSS Score: N/A
  - Description: It was possible for a student to view their quiz grade before it had been released, using a quiz web service.

- **Vulnerability: CVE-2022-40314**

  - CVSS Score: N/A
  - Description: A remote code execution risk when restoring backup files originating from Moodle 1.9 was identified.

- **Vulnerability: CVE-2021-36568**

  - CVSS Score: N/A
  - Description: In certain Moodle products after creating a course, it is possible to add in a arbitrary "Topic" a resource, in this case a "Database" with the type "Text" where its values "Field name" and "Field description" are vulnerable to Cross Site Scripting Stored(XSS). This affects Moodle 3.11 and Moodle 3.10.4 and Moodle 3.9.7.

- **Vulnerability: CVE-2021-32791**

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

- **Vulnerability: CVE-2021-32792**

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using `OIDCPreservePost On`.

- Vulnerability: CVE-2024-38476
  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.
- Vulnerability: CVE-2024-27316
  - CVSS Score: N/A
  - Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.
- Vulnerability: CVE-2023-31122
  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.
- Vulnerability: CVE-2009-0796
  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.
- Vulnerability: CVE-2021-36160
  - CVSS Score: 5
  - Description: A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS). This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48 (inclusive).
- Vulnerability: CVE-2023-5539
  - CVSS Score: N/A
  - Description: A remote code execution risk was identified in the Lesson activity. By default this was only available to teachers and managers.
- Vulnerability: CVE-2023-23923
  - CVSS Score: N/A
  - Description: The vulnerability was found Moodle which exists due to insufficient limitations on the "start page" preference. A remote attacker can set that preference for another user. The vulnerability allows a remote attacker to gain unauthorized access to otherwise restricted functionality.
- Vulnerability: CVE-2011-2688
  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.
- Vulnerability: CVE-2022-0984
  - CVSS Score: 4

- Description: Users with the capability to configure badge criteria (teachers and managers by default) were able to configure course badges with profile field criteria, which should only be available for site badges.

• Vulnerability: CVE-2022-0985

  – CVSS Score: 4
  – Description: Insufficient capability checks could allow users with the moodle/site:uploadusers capability to delete users, without having the necessary moodle/user:delete capability.

• Vulnerability: CVE-2021-32785

  – CVSS Score: 4.3
  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache (`OIDCCacheEncrypt off`, `OIDCSessionType server-cache`, `OIDCCacheType redis`), `mod_auth_openidc` wrongly performed argument interpolation before passing Redis requests to `hiredis`, which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the `hiredis` API. As a workaround, this vulnerability can be mitigated by setting `OIDCCacheEncrypt` to `on`, as cache keys are cryptographically hashed before use when this option is enabled.

• Vulnerability: CVE-2020-9490

  – CVSS Score: 5
  – Description: Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.

• Vulnerability: CVE-2007-4723

  – CVSS Score: 7.5
  – Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

• Vulnerability: CVE-2022-0983

  – CVSS Score: 6.5
  – Description: An SQL injection risk was identified in Badges code relating to configuring criteria. Access to the relevant capability was limited to teachers and managers by default.

• Vulnerability: CVE-2021-44790

  – CVSS Score: 7.5

- Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

- Vulnerability: CVE-2022-37436

  - CVSS Score: N/A
  - Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2020-13938

  - CVSS Score: 2.1
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

- Vulnerability: CVE-2022-30600

  - CVSS Score: 7.5
  - Description: A flaw was found in moodle where logic used to count failed login attempts could result in the account lockout threshold being bypassed.

- Vulnerability: CVE-2020-35452

  - CVSS Score: 6.8
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

- Vulnerability: CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2021-43560

  - CVSS Score: 5
  - Description: A flaw was found in Moodle in versions 3.11 to 3.11.3, 3.10 to 3.10.7, 3.9 to 3.9.10 and earlier unsupported versions. Insufficient capability checks made it possible to fetch other users' calendar action events.

- Vulnerability: CVE-2020-1934

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

- Vulnerability: CVE-2022-36760

  - CVSS Score: N/A

- Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2021-36400

  - CVSS Score: N/A
  - Description: In Moodle, insufficient capability checks made it possible to remove other users' calendar URL subscriptions.

- Vulnerability: CVE-2023-28332

  - CVSS Score: N/A
  - Description: If the algebra filter was enabled but not functional (eg the necessary binaries were missing from the server), it presented an XSS risk.

- Vulnerability: CVE-2022-0333

  - CVSS Score: 5.5
  - Description: A flaw was found in Moodle in versions 3.11 to 3.11.4, 3.10 to 3.10.8, 3.9 to 3.9.11 and earlier unsupported versions. The calendar:manageentries capability allowed managers to access or modify any calendar event, but should have been restricted from accessing user level events.

- Vulnerability: CVE-2022-0332

  - CVSS Score: 7.5
  - Description: A flaw was found in Moodle in versions 3.11 to 3.11.4. An SQL injection risk was identified in the h5p activity web service responsible for fetching user attempt data.

- Vulnerability: CVE-2021-36402

  - CVSS Score: N/A
  - Description: In Moodle, Users' names required additional sanitizing in the account confirmation email, to prevent a self-registration phishing risk.

- Vulnerability: CVE-2022-0335

  - CVSS Score: 6.8
  - Description: A flaw was found in Moodle in versions 3.11 to 3.11.4, 3.10 to 3.10.8, 3.9 to 3.9.11 and earlier unsupported versions. The "delete badge alignment" functionality did not include the necessary token check to prevent a CSRF risk.

- Vulnerability: CVE-2023-1402

  - CVSS Score: N/A
  - Description: The course participation report required additional checks to prevent roles being displayed which the user did not have access to view.

- Vulnerability: CVE-2021-36403

  - CVSS Score: N/A
  - Description: In Moodle, in some circumstances, email notifications of messages could have the link back to the original message hidden by HTML, which may pose a phishing risk.

- Vulnerability: CVE-2013-4365

- CVSS Score: 7.5
- Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2021-40694

  - CVSS Score: N/A
  - Description: Insufficient escaping of the LaTeX preamble made it possible for site administrators to read files available to the HTTP server system account.

- Vulnerability: CVE-2021-33193

  - CVSS Score: 5
  - Description: A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.

- Vulnerability: CVE-2019-17567

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

- Vulnerability: CVE-2022-28330

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2022-31813

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

- Vulnerability: CVE-2021-36395

  - CVSS Score: N/A
  - Description: In Moodle, the file repository's URL parsing required additional recursion handling to mitigate the risk of recursion denial of service.

- Vulnerability: CVE-2022-40315

  - CVSS Score: N/A
  - Description: A limited SQL injection risk was identified in the "browse list of users" site administration page.

- Vulnerability: CVE-2012-4360

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2007-6538

  – CVSS Score: 7.5
  – Description: SQL injection vulnerability in ing/blocks/mrbs/code/web/view_entry.php
                 in the MRBS plugin for Moodle allows remote attackers to execute
                 arbitrary SQL commands via the id parameter.

- Vulnerability: CVE-2023-28329

  – CVSS Score: N/A
  – Description: Insufficient validation of profile field availability condition
                 resulted in an SQL injection risk (by default only available to
                 teachers and managers).

- Vulnerability: CVE-2022-40208

  – CVSS Score: N/A
  – Description: In Moodle, insufficient limitations in some quiz web services made it
                 possible for students to bypass sequential navigation during a quiz
                 attempt.

- Vulnerability: CVE-2021-26691

  – CVSS Score: 7.5
  – Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted
                 SessionHeader sent by an origin server could cause a heap overflow

- Vulnerability: CVE-2020-13950

  – CVSS Score: 5
  – Description: Apache HTTP Server versions 2.4.41 to 2.4.46 mod_proxy_http can be
                 made to crash (NULL pointer dereference) with specially crafted
                 requests using both Content-Length and Transfer-Encoding headers,
                 leading to a Denial of Service

- Vulnerability: CVE-2024-38477

  – CVSS Score: N/A
  – Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59
                 and earlier allows an attacker to crash the server via a malicious
                 request.Users are recommended to upgrade to version 2.4.60, which
                 fixes this issue.

- Vulnerability: CVE-2024-38474

  – CVSS Score: N/A
  – Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server
                 2.4.59 and earlier allows attacker to execute scripts indirectories
                 permitted by the configuration but not directly reachable by anyURL
                 or source disclosure of scripts meant to only to be executed as
                 CGI.Users are recommended to upgrade to version 2.4.60, which fixes
                 this issue.Some RewriteRules that capture and substitute unsafely
                 will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2021-39275

  – CVSS Score: 7.5
  – Description: ap_escape_quotes() may write beyond the end of a buffer when given
                 malicious input. No included modules pass untrusted data to these
                 functions, but third-party / external modules may. This issue
                 affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2022-2986

- CVSS Score: N/A
- Description: Enabling and disabling installed H5P libraries did not include the necessary token to prevent a CSRF risk.

- Vulnerability: CVE-2022-29404

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2023-28333

  - CVSS Score: N/A
  - Description: The Mustache pix helper contained a potential Mustache injection risk if combined with user input (note: This did not appear to be implemented/exploitable anywhere in the core Moodle LMS).

- Vulnerability: CVE-2021-36401

  - CVSS Score: N/A
  - Description: In Moodle, ID numbers exported in HTML data formats required additional sanitizing to prevent a local stored XSS risk.

- Vulnerability: CVE-2023-28331

  - CVSS Score: N/A
  - Description: Content output by the database auto-linking filter required additional sanitizing to prevent an XSS risk.

- Vulnerability: CVE-2023-28330

  - CVSS Score: N/A
  - Description: Insufficient sanitizing in backup resulted in an arbitrary file read risk. The capability to access this feature is only available to teachers, managers and admins by default.

- Vulnerability: CVE-2023-28336

  - CVSS Score: N/A
  - Description: Insufficient filtering of grade report history made it possible for teachers to access the names of users they could not otherwise access.

- Vulnerability: CVE-2020-11993

  - CVSS Score: 4.3
  - Description: Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2021-40691

  - CVSS Score: N/A
  - Description: A session hijack risk was identified in the Shibboleth authentication plugin.

- Vulnerability: CVE-2021-44224

  - CVSS Score: 6.4

- Description: A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).

- Vulnerability: CVE-2022-22721

  - CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2006-20001

  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2023-35133

  - CVSS Score: N/A
  - Description: An issue in the logic used to check 0.0.0.0 against the cURL blocked hosts lists resulted in an SSRF risk. This flaw affects Moodle versions 4.2, 4.1 to 4.1.3, 4.0 to 4.0.8, 3.11 to 3.11.14, 3.9 to 3.9.21 and earlier unsupported versions.

- Vulnerability: CVE-2023-35132

  - CVSS Score: N/A
  - Description: A limited SQL injection risk was identified on the Mnet SSO access control page. This flaw affects Moodle versions 4.2, 4.1 to 4.1.3, 4.0 to 4.0.8, 3.11 to 3.11.14, 3.9 to 3.9.21 and earlier unsupported versions.

- Vulnerability: CVE-2023-35131

  - CVSS Score: N/A
  - Description: Content on the groups page required additional sanitizing to prevent an XSS risk. This flaw affects Moodle versions 4.2, 4.1 to 4.1.3, 4.0 to 4.0.8 and 3.11 to 3.11.14.

- Vulnerability: CVE-2021-40438

  - CVSS Score: 6.8
  - Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2021-40692

  - CVSS Score: N/A
  - Description: Insufficient capability checks made it possible for teachers to download users outside of their courses.

- Vulnerability: CVE-2022-23943

  - CVSS Score: 7.5

- Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

- Vulnerability: CVE-2022-45149

  - CVSS Score: N/A
  - Description: A vulnerability was found in Moodle which exists due to insufficient validation of the HTTP request origin in course redirect URL. A user's CSRF token was unnecessarily included in the URL when being redirected to a course they have just restored. A remote attacker can trick the victim to visit a specially crafted web page and perform arbitrary actions on behalf of the victim on the vulnerable website. This flaw allows an attacker to perform cross-site request forgery attacks.

- Vulnerability: CVE-2021-3943

  - CVSS Score: 7.5
  - Description: A flaw was found in Moodle in versions 3.11 to 3.11.3, 3.10 to 3.10.7, 3.9 to 3.9.10 and earlier unsupported versions. A remote code execution risk when restoring backup files was identified.

- Vulnerability: CVE-2022-22720

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2021-34798

  - CVSS Score: 5
  - Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2023-25690

  - CVSS Score: N/A
  - Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2020-11984

  - CVSS Score: 7.5
  - Description: Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE

- Vulnerability: CVE-2010-4208

  - CVSS Score: 4.3

- Description: Cross-site scripting (XSS) vulnerability in the Flash component infrastructure in YUI 2.5.0 through 2.8.1, as used in Bugzilla, Moodle, and other products, allows remote attackers to inject arbitrary web script or HTML via vectors related to uploader/assets/uploader.swf.

- Vulnerability: CVE-2022-26377

  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2010-4207

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the Flash component infrastructure in YUI 2.4.0 through 2.8.1, as used in Bugzilla, Moodle, and other products, allows remote attackers to inject arbitrary web script or HTML via vectors related to charts/assets/charts.swf.

- Vulnerability: CVE-2021-26690

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service

- Vulnerability: CVE-2024-40898

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2022-35649

  - CVSS Score: N/A
  - Description: The vulnerability was found in Moodle, occurs due to improper input validation when parsing PostScript code. An omitted execution parameter results in a remote code execution risk for sites running GhostScript versions older than 9.50. Successful exploitation of this vulnerability may result in complete compromise of vulnerable system.

- Vulnerability: CVE-2023-27522

  - CVSS Score: N/A
  - Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.Special characters in the origin response header can truncate/split the response forwarded to the client.

- Vulnerability: CVE-2022-45151

  - CVSS Score: N/A

- Description: The stored-XSS vulnerability was discovered in Moodle which exists due to insufficient sanitization of user-supplied data in several "social" user profile fields. An attacker could inject and execute arbitrary HTML and script code in user's browser in context of vulnerable website.

- Vulnerability: CVE-2021-36397

  - CVSS Score: N/A
  - Description: In Moodle, insufficient capability checks meant message deletions were not limited to the current user.

- Vulnerability: CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2021-36392

  - CVSS Score: N/A
  - Description: In Moodle, an SQL injection risk was identified in the library fetching a user's enrolled courses.

- Vulnerability: CVE-2021-36393

  - CVSS Score: N/A
  - Description: In Moodle, an SQL injection risk was identified in the library fetching a user's recent courses.

- Vulnerability: CVE-2021-36394

  - CVSS Score: N/A
  - Description: In Moodle, a remote code execution risk was identified in the Shibboleth authentication plugin.

- Vulnerability: CVE-2022-45152

  - CVSS Score: N/A
  - Description: A blind Server-Side Request Forgery (SSRF) vulnerability was found in Moodle. This flaw exists due to insufficient validation of user-supplied input in LTI provider library. The library does not utilise Moodle's inbuilt cURL helper, which resulted in a blind SSRF risk. An attacker can send a specially crafted HTTP request and trick the application to initiate requests to arbitrary systems. This vulnerability allows a remote attacker to perform SSRF attacks.

- Vulnerability: CVE-2021-36396

  - CVSS Score: N/A
  - Description: In Moodle, insufficient redirect handling made it possible to blindly bypass cURL blocked hosts/allowed ports restrictions, resulting in a blind SSRF risk.

- Vulnerability: CVE-2022-45150

  - CVSS Score: N/A

– Description: A reflected cross-site scripting vulnerability was discovered in Moodle. This flaw exists due to insufficient sanitization of user-supplied data in policy tool. An attacker can trick the victim to open a specially crafted link that executes an arbitrary HTML and script code in user's browser in context of vulnerable website. This vulnerability may allow an attacker to perform cross-site scripting (XSS) attacks to gain access potentially sensitive information and modification of web pages.

- Vulnerability: CVE-2021-36398

  – CVSS Score: N/A

  – Description: In moodle, ID numbers displayed in the web service token list required additional sanitizing to prevent a stored XSS risk.

- Vulnerability: CVE-2021-36399

  – CVSS Score: N/A

  – Description: In Moodle, ID numbers displayed in the quiz override screens required additional sanitizing to prevent a stored XSS risk.

- Vulnerability: CVE-2021-30641

  – CVSS Score: 5

  – Description: Apache HTTP Server versions 2.4.39 to 2.4.46 Unexpected matching behavior with 'MergeSlashes OFF'

- Vulnerability: CVE-2012-3526

  – CVSS Score: 5

  – Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2009-2299

  – CVSS Score: 5

  – Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2023-30944

  – CVSS Score: N/A

  – Description: The vulnerability was found Moodle which exists due to insufficient sanitization of user-supplied data in external Wiki method for listing pages. A remote attacker can send a specially crafted request to the affected application and execute limited SQL commands within the application database.

- Vulnerability: CVE-2022-35653

  – CVSS Score: N/A

  – Description: A reflected XSS issue was identified in the LTI module of Moodle. The vulnerability exists due to insufficient sanitization of user-supplied data in the LTI module. A remote attacker can trick the victim to follow a specially crafted link and execute arbitrary HTML and script code in user's browser in context of vulnerable website to steal potentially sensitive information, change appearance of the web page, can perform phishing and drive-by-download attacks. This vulnerability does not impact authenticated users.

- Vulnerability: CVE-2022-35652

  – CVSS Score: N/A
  – Description: An open redirect issue was found in Moodle due to improper sanitization of user-supplied data in mobile auto-login feature. A remote attacker can create a link that leads to a trusted website, however, when clicked, it redirects the victims to arbitrary URL/domain. Successful exploitation of this vulnerability may allow a remote attacker to perform a phishing attack and steal potentially sensitive information.

- Vulnerability: CVE-2022-35651

  – CVSS Score: N/A
  – Description: A stored XSS and blind SSRF vulnerability was found in Moodle, occurs due to insufficient sanitization of user-supplied data in the SCORM track details. A remote attacker can trick the victim to follow a specially crafted link and execute arbitrary HTML and script code in user's browser in context of vulnerable website to steal potentially sensitive information, change appearance of the web page, can perform phishing and drive-by-download attacks.

- Vulnerability: CVE-2022-35650

  – CVSS Score: N/A
  – Description: The vulnerability was found in Moodle, occurs due to input validation error when importing lesson questions. This insufficient path checks results in arbitrary file read risk. This vulnerability allows a remote attacker to perform directory traversal attacks. The capability to access this feature is only available to teachers, managers and admins by default.

- Vulnerability: CVE-2020-1927

  – CVSS Score: 5.8
  – Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.

- Vulnerability: CVE-2012-4001

  – CVSS Score: 5
  – Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2022-0334

  – CVSS Score: 4
  – Description: A flaw was found in Moodle in versions 3.11 to 3.11.4, 3.10 to 3.10.8, 3.9 to 3.9.11 and earlier unsupported versions. Insufficient capability checks could lead to users accessing their grade report for courses where they did not have the required gradereport/user:view capability.

- Vulnerability: CVE-2021-43558

  – CVSS Score: 4.3

- Description: A flaw was found in Moodle in versions 3.11 to 3.11.3, 3.10 to 3.10.7, 3.9 to 3.9.10 and earlier unsupported versions. A URL parameter in the filetype site administrator tool required extra sanitizing to prevent a reflected XSS risk.

- Vulnerability: CVE-2021-43559

  - CVSS Score: 6.8
  - Description: A flaw was found in Moodle in versions 3.11 to 3.11.3, 3.10 to 3.10.7, 3.9 to 3.9.10 and earlier unsupported versions. The "delete related badge" functionality did not include the necessary token check to prevent a CSRF risk.

- Vulnerability: CVE-2023-5551

  - CVSS Score: N/A
  - Description: Separate Groups mode restrictions were not honoured in the forum summary report, which would display users from other groups.

- Vulnerability: CVE-2023-5550

  - CVSS Score: N/A
  - Description: In a shared hosting environment that has been misconfigured to allow access to other users' content, a Moodle user who also has direct access to the web server outside of the Moodle webroot could utilise a local file include to achieve remote code execution.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2022-30599

  - CVSS Score: 7.5
  - Description: A flaw was found in moodle where an SQL injection risk was identified in Badges code relating to configuring criteria.

- Vulnerability: CVE-2022-30598

  - CVSS Score: 4

- Description: A flaw was found in moodle where global search results could include author information on some activities where a user may not otherwise have access to it.

- Vulnerability: CVE-2022-30597

  - CVSS Score: 5

  - Description: A flaw was found in moodle where the description user field was not hidden when being set as a hidden user field.

- Vulnerability: CVE-2022-30596

  - CVSS Score: 3.5

  - Description: A flaw was found in moodle where ID numbers displayed when bulk allocating markers to assignments required additional sanitizing to prevent a stored XSS risk.

- Vulnerability: CVE-2023-45802

  - CVSS Score: N/A

  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5

  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- Vulnerability: CVE-2022-28615

  - CVSS Score: 6.4

  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- Vulnerability: CVE-2022-28614

  - CVSS Score: 5

  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

11.33 IP Address: 159.149.133.61

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 22

- Medium Vulnerabilities: 100

- Low Vulnerabilities: 8

- Total Vulnerabilities: 130

Services Running on IP Address

- Service: Apache httpd

  – Port: 80
  – Version: 2.4.29
  – Location: /

- Service: Apache httpd

  – Port: 443
  – Version: 2.4.29
  – Location: /

- Service: N/A

  – Port: 10001
  – Version: N/A
  – Location:

Vulnerabilities Found

- Vulnerability: CVE-2019-0220

  – CVSS Score: 5
  – Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38.
    When the path component of a request URL contains multiple
    consecutive slashes ('/'), directives such as LocationMatch and
    RewriteRule must account for duplicates in regular expressions while
    other aspects of the servers processing will implicitly collapse
    them.

- Vulnerability: CVE-2024-27316

  – CVSS Score: N/A
  – Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered
    in nghttp2 in order to generate an informative HTTP 413 response.
    If a client does not stop sending headers, this leads to memory
    exhaustion.

- Vulnerability: CVE-2011-2688

  – CVSS Score: 7.5
  – Description: SQL injection vulnerability in mysql/mysql-auth.pl in the
    mod_authnz_external module 3.2.5 and earlier for the Apache HTTP
    Server allows remote attackers to execute arbitrary SQL commands
    via the user field.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2020-1934

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

- Vulnerability: CVE-2018-17189

  - CVSS Score: 5
  - Description: In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 (mod_http2) connections.

- Vulnerability: CVE-2022-36760

  - CVSS Score: N/A
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2020-35452

  - CVSS Score: 6.8
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

- Vulnerability: CVE-2022-29404

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2021-33193

  - CVSS Score: 5
  - Description: A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.

- Vulnerability: CVE-2009-0796

  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2013-4365

  – CVSS Score: 7.5
  – Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2018-1333

  – CVSS Score: 5
  – Description: By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.18-2.4.30,2.4.33).

- Vulnerability: CVE-2022-22720

  – CVSS Score: 7.5
  – Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2018-11763

  – CVSS Score: 4.3
  – Description: In Apache HTTP Server 2.4.17 to 2.4.34, by sending continuous, large SETTINGS frames a client can occupy a connection, server thread and CPU time without any connection timeout coming to effect. This affects only HTTP/2 connections. A possible mitigation is to not enable the h2 protocol.

- Vulnerability: CVE-2022-28330

  – CVSS Score: 5
  – Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2020-11993

  – CVSS Score: 4.3
  – Description: Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2021-32791

  – CVSS Score: 4.3
  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2021-32792

- CVSS Score: 4.3
- Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using `OIDCPreservePost On`.

- **Vulnerability:** CVE-2023-31122

  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- **Vulnerability:** CVE-2019-9517

  - CVSS Score: 7.8
  - Description: Some HTTP/2 implementations are vulnerable to unconstrained interal data buffering, potentially leading to a denial of service. The attacker opens the HTTP/2 window so the peer can send without constraint; however, they leave the TCP window closed so the peer cannot actually write (many of) the bytes on the wire. The attacker then sends a stream of requests for a large response object. Depending on how the servers queue the responses, this can consume excess memory, CPU, or both.

- **Vulnerability:** CVE-2024-38476

  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- **Vulnerability:** CVE-2024-38477

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- **Vulnerability:** CVE-2024-38474

  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- **Vulnerability:** CVE-2019-0196

  - CVSS Score: 5
  - Description: A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.

- **Vulnerability:** CVE-2019-0211

- CVSS Score: 7.2
- Description: In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.

- Vulnerability: CVE-2022-22721

  - CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2006-20001

  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2019-10092

  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2019-17567

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

- Vulnerability: CVE-2017-15715

  - CVSS Score: 6.8
  - Description: In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.

- Vulnerability: CVE-2022-31813

  – CVSS Score: 7.5
  – Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-*
    headers to the origin server based on client side Connection
    header hop-by-hop mechanism. This may be used to bypass IP based
    authentication on the origin server/application.

- Vulnerability: CVE-2012-4001

  – CVSS Score: 5
  – Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server
    does not properly verify its host name, which allows remote attackers
    to trigger HTTP requests to arbitrary hosts via unspecified vectors,
    as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2019-10098

  – CVSS Score: 5.8
  – Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with
    mod_rewrite that were intended to be self-referential might be fooled
    by encoded newlines and redirect instead to an unexpected URL within
    the request URL.

- Vulnerability: CVE-2022-37436

  – CVSS Score: N/A
  – Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause
    the response headers to be truncated early, resulting in some headers
    being incorporated into the response body. If the later headers have
    any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2012-4360

  – CVSS Score: 4.3
  – Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module
    0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote
    attackers to inject arbitrary web script or HTML via unspecified
    vectors.

- Vulnerability: CVE-2021-40438

  – CVSS Score: 6.8
  – Description: A crafted request uri-path can cause mod_proxy to forward the request
    to an origin server choosen by the remote user. This issue affects
    Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2011-1176

  – CVSS Score: 4.3
  – Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk
    Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP
    Server does not properly handle certain configuration sections that
    specify NiceValue but not AssignUserID, which might allow remote
    attackers to gain privileges by leveraging the root uid and root gid
    of an mpm-itk process.

- Vulnerability: CVE-2022-23943

  – CVSS Score: 7.5
  – Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server
    allows an attacker to overwrite heap memory with possibly attacker
    provided data. This issue affects Apache HTTP Server 2.4 version
    2.4.52 and prior versions.

- Vulnerability: CVE-2020-1927

  - CVSS Score: 5.8
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.

- Vulnerability: CVE-2018-17199

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

- Vulnerability: CVE-2017-15710

  - CVSS Score: 5
  - Description: In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.

- Vulnerability: CVE-2018-1301

  - CVSS Score: 4.3
  - Description: A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.

- Vulnerability: CVE-2018-1302

  - CVSS Score: 4.3
  - Description: When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.

- Vulnerability: CVE-2018-1303

  - CVSS Score: 5
  - Description: A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache. The vulnerability is considered as low risk since mod_cache_socache is not widely used, mod_cache_disk is not concerned by this vulnerability.

- Vulnerability: CVE-2021-34798

  - CVSS Score: 5
  - Description: Malformed requests may cause the server to dereference a NULL
    pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2023-25690

  - CVSS Score: N/A
  - Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0
    through 2.4.55 allow a HTTP Request Smuggling attack.Configurations
    are affected when mod_proxy is enabled along with some form of
    RewriteRule or ProxyPassMatch in which a non-specific pattern
    matches some portion of the user-supplied request-target (URL)
    data and is then re-inserted into the proxied request-target using
    variable substitution. For example, something like:RewriteEngine
    onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1";
    [P]ProxyPassReverse /here/ http://example.com:8080/Request
    splitting/smuggling could result in bypass of access controls in the
    proxy server, proxying unintended URLs to existing origin servers,
    and cache poisoning. Users are recommended to update to at least
    version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2021-32786

  - CVSS Score: 5.8
  - Description: mod_auth_openidc is an authentication/authorization module for the
    Apache 2.x HTTP server that functions as an OpenID Connect Relying
    Party, authenticating users against an OpenID Connect Provider. In
    versions prior to 2.4.9, `oidc_validate_redirect_url()` does not parse
    URLs the same way as most browsers do. As a result, this function
    can be bypassed and leads to an Open Redirect vulnerability in the
    logout functionality. This bug has been fixed in version 2.4.9
    by replacing any backslash of the URL to redirect with slashes
    to address a particular breaking change between the different
    specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this
    vulnerability can be mitigated by configuring `mod_auth_openidc` to
    only allow redirection whose destination matches a given regular
    expression.

- Vulnerability: CVE-2021-32785

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the
    Apache 2.x HTTP server that functions as an OpenID Connect Relying
    Party, authenticating users against an OpenID Connect Provider. When
    mod_auth_openidc versions prior to 2.4.9 are configured to use an
    unencrypted Redis cache (`OIDCCacheEncrypt off`, `OIDCSessionType
    server-cache`, `OIDCCacheType redis`), `mod_auth_openidc` wrongly
    performed argument interpolation before passing Redis requests to
    `hiredis`, which would perform it again and lead to an uncontrolled
    format string bug. Initial assessment shows that this bug does
    not appear to allow gaining arbitrary code execution, but can
    reliably provoke a denial of service by repeatedly crashing the
    Apache workers. This bug has been corrected in version 2.4.9 by
    performing argument interpolation only once, using the `hiredis`
    API. As a workaround, this vulnerability can be mitigated by setting
    `OIDCCacheEncrypt` to `on`, as cache keys are cryptographically
    hashed before use when this option is enabled.

- Vulnerability: CVE-2020-9490

- CVSS Score: 5
- Description: Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.

- **Vulnerability:** CVE-2021-44224

  - CVSS Score: 6.4
  - Description: A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).

- **Vulnerability:** CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- **Vulnerability:** CVE-2021-44790

  - CVSS Score: 7.5
  - Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

- **Vulnerability:** CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- **Vulnerability:** CVE-2021-26690

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service

- **Vulnerability:** CVE-2021-26691

  - CVSS Score: 7.5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow

- **Vulnerability:** CVE-2022-26377

  - CVSS Score: 5

- Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2023-45802

  - CVSS Score: N/A

  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-28614

  - CVSS Score: 5

  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

- Vulnerability: CVE-2020-13938

  - CVSS Score: 2.1

  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

- Vulnerability: CVE-2019-10081

  - CVSS Score: 5

  - Description: HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example configured with "H2PushResource", could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client.

- Vulnerability: CVE-2018-1283

  - CVSS Score: 3.5

  - Description: In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to forward its session data to CGI applications (SessionEnv on, not the default), a remote user may influence their content by using a "Session" header. This comes from the "HTTP_SESSION" variable name used by mod_session to forward its data to CGIs, since the prefix "HTTP_" is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications.

- Vulnerability: CVE-2019-10082

  - CVSS Score: 6.4

– Description: In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.

• Vulnerability: CVE-2018-1312

  – CVSS Score: 6.8
  – Description: In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

• Vulnerability: CVE-2012-3526

  – CVSS Score: 5
  – Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

• Vulnerability: CVE-2024-40898

  – CVSS Score: N/A
  – Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

• Vulnerability: CVE-2019-0217

  – CVSS Score: 6
  – Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.

• Vulnerability: CVE-2009-2299

  – CVSS Score: 5
  – Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

• Vulnerability: CVE-2021-39275

  – CVSS Score: 7.5
  – Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

• Vulnerability: CVE-2022-28615

  – CVSS Score: 6.4
  – Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to
               applications calling r:wsread() that point past the end of the
               storage allocated for the buffer.

- Vulnerability: CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory
               area which could cause the process to crash. This issue affects
               Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2019-0220

  - CVSS Score: 5
  - Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38.
               When the path component of a request URL contains multiple
               consecutive slashes ('/'), directives such as LocationMatch and
               RewriteRule must account for duplicates in regular expressions while
               other aspects of the servers processing will implicitly collapse
               them.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the
               mod_authnz_external module 3.2.5 and earlier for the Apache HTTP
               Server allows remote attackers to execute arbitrary SQL commands
               via the user field.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server
               allows remote attackers to cause a denial of service (NULL pointer
               dereference, process crash, and disk consumption) via a POST request
               with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2018-14040

  - CVSS Score: 4.3
  - Description: In Bootstrap before 4.1.2, XSS is possible in the collapse
               data-parent attribute.

- Vulnerability: CVE-2018-17189

  - CVSS Score: 5
  - Description: In Apache HTTP server versions 2.4.37 and prior, by sending request
               bodies in a slow loris way to plain resources, the h2 stream for
               that request unnecessarily occupied a server thread cleaning up that
               incoming data. This affects only HTTP/2 (mod_http2) connections.

- Vulnerability: CVE-2018-14042

  - CVSS Score: 4.3
  - Description: In Bootstrap before 4.1.2, XSS is possible in the data-container
               property of tooltip.

- Vulnerability: CVE-2020-35452

  - CVSS Score: 6.8

- Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted
  Digest nonce can cause a stack overflow in mod_auth_digest. There
  is no report of this overflow being exploitable, nor the Apache HTTP
  Server team could create one, though some particular compiler and/or
  compilation option might make it possible, with limited consequences
  anyway due to the size (a single byte) and the value (zero byte) of
  the overflow

- Vulnerability: CVE-2016-10735

  - CVSS Score: 4.3
  - Description: In Bootstrap 3.x before 3.4.0 and 4.x-beta before 4.0.0-beta.2, XSS
    is possible in the data-target attribute, a different vulnerability
    than CVE-2018-14041.

- Vulnerability: CVE-2022-29404

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a
    lua script that calls r:parsebody(0) may cause a denial of service
    due to no default limit on possible input size.

- Vulnerability: CVE-2021-33193

  - CVSS Score: 5
  - Description: A crafted method sent through HTTP/2 will bypass validation and be
    forwarded by mod_proxy, which can lead to request splitting or cache
    poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.

- Vulnerability: CVE-2009-0796

  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in
    Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the
    Apache HTTP Server, when /perl-status is accessible, allows remote
    attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2013-4365

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function
    in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache
    HTTP Server allows remote attackers to have an unspecified impact via
    unknown vectors.

- Vulnerability: CVE-2018-1333

  - CVSS Score: 5
  - Description: By specially crafting HTTP/2 requests, workers would be allocated
    60 seconds longer than necessary, leading to worker exhaustion and
    a denial of service. Fixed in Apache HTTP Server 2.4.34 (Affected
    2.4.18-2.4.30,2.4.33).

- Vulnerability: CVE-2022-22720

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound
    connection when errors are encountered discarding the request body,
    exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2018-11763

  - CVSS Score: 4.3

– Description: In Apache HTTP Server 2.4.17 to 2.4.34, by sending continuous, large SETTINGS frames a client can occupy a connection, server thread and CPU time without any connection timeout coming to effect. This affects only HTTP/2 connections. A possible mitigation is to not enable the h2 protocol.

- Vulnerability: CVE-2022-28330

    – CVSS Score: 5

    – Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2020-11993

    – CVSS Score: 4.3

    – Description: Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2021-32791

    – CVSS Score: 4.3

    – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2021-32792

    – CVSS Score: 4.3

    – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.

- Vulnerability: CVE-2023-31122

    – CVSS Score: N/A

    – Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2019-9517

    – CVSS Score: 7.8

    – Description: Some HTTP/2 implementations are vulnerable to unconstrained interal data buffering, potentially leading to a denial of service. The attacker opens the HTTP/2 window so the peer can send without constraint; however, they leave the TCP window closed so the peer cannot actually write (many of) the bytes on the wire. The attacker then sends a stream of requests for a large response object. Depending on how the servers queue the responses, this can consume excess memory, CPU, or both.

- Vulnerability: CVE-2024-38476

- CVSS Score: N/A
- Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

• Vulnerability: CVE-2024-27316

- CVSS Score: N/A
- Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

• Vulnerability: CVE-2024-38474

- CVSS Score: N/A
- Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

• Vulnerability: CVE-2019-0196

- CVSS Score: 5
- Description: A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.

• Vulnerability: CVE-2019-0211

- CVSS Score: 7.2
- Description: In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.

• Vulnerability: CVE-2022-22721

- CVSS Score: 5.8
- Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

• Vulnerability: CVE-2006-20001

- CVSS Score: N/A
- Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

• Vulnerability: CVE-2019-10092

- CVSS Score: 4.3

- Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2019-8331

  - CVSS Score: 4.3
  - Description: In Bootstrap before 3.4.1 and 4.3.x before 4.3.1, XSS is possible in the tooltip or popover data-template attribute.

- Vulnerability: CVE-2017-15715

  - CVSS Score: 6.8
  - Description: In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.

- Vulnerability: CVE-2022-31813

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

- Vulnerability: CVE-2012-4001

  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2019-17567

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

- Vulnerability: CVE-2019-10098

  - CVSS Score: 5.8

- Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.

- **Vulnerability: CVE-2022-37436**

  - CVSS Score: N/A
  - Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- **Vulnerability: CVE-2012-4360**

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- **Vulnerability: CVE-2021-40438**

  - CVSS Score: 6.8
  - Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

- **Vulnerability: CVE-2011-1176**

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- **Vulnerability: CVE-2018-20677**

  - CVSS Score: 4.3
  - Description: In Bootstrap before 3.4.0, XSS is possible in the affix configuration target property.

- **Vulnerability: CVE-2022-23943**

  - CVSS Score: 7.5
  - Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

- **Vulnerability: CVE-2020-1927**

  - CVSS Score: 5.8
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.

- **Vulnerability: CVE-2020-1934**

  - CVSS Score: 5

– Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use
uninitialized memory when proxying to a malicious FTP server.

• Vulnerability: CVE-2018-17199

– CVSS Score: 5
– Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session
checks the session expiry time before decoding the session. This
causes session expiry time to be ignored for mod_session_cookie
sessions since the expiry time is loaded when the session is decoded.

• Vulnerability: CVE-2024-40898

– CVSS Score: N/A
– Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in
server/vhost context, allows to potentially leak NTML hashes to
a malicious server via SSRF and malicious requests.Users are
recommended to upgrade to version 2.4.62 which fixes this issue.

• Vulnerability: CVE-2017-15710

– CVSS Score: 5
– Description: In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to
2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig,
uses the Accept-Language header value to lookup the right charset
encoding when verifying the user's credentials. If the header value
is not present in the charset conversion table, a fallback mechanism
is used to truncate it to a two characters value to allow a quick
retry (for example, 'en-US' is truncated to 'en'). A header value of
less than two characters forces an out of bound write of one NUL byte
to a memory location that is not part of the string. In the worst
case, quite unlikely, the process would crash which could be used as
a Denial of Service attack. In the more likely case, this memory is
already reserved for future use and the issue has no effect at all.

• Vulnerability: CVE-2018-1301

– CVSS Score: 4.3
– Description: A specially crafted request could have crashed the Apache HTTP Server
prior to version 2.4.30, due to an out of bound access after a size
limit is reached by reading the HTTP header. This vulnerability
is considered very hard if not impossible to trigger in non-debug
mode (both log and build level), so it is classified as low risk for
common server usage.

• Vulnerability: CVE-2018-1302

– CVSS Score: 4.3
– Description: When an HTTP/2 stream was destroyed after being handled, the Apache
HTTP Server prior to version 2.4.30 could have written a NULL pointer
potentially to an already freed memory. The memory pools maintained
by the server make this vulnerability hard to trigger in usual
configurations, the reporter and the team could not reproduce it
outside debug builds, so it is classified as low risk.

• Vulnerability: CVE-2018-1303

– CVSS Score: 5
– Description: A specially crafted HTTP request header could have crashed the Apache
HTTP Server prior to version 2.4.30 due to an out of bound read while
preparing data to be cached in shared memory. It could be used as
a Denial of Service attack against users of mod_cache_socache. The
vulnerability is considered as low risk since mod_cache_socache is not
widely used, mod_cache_disk is not concerned by this vulnerability.

- Vulnerability: CVE-2022-36760

  – CVSS Score: N/A
  – Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2023-25690

  – CVSS Score: N/A
  – Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2021-32786

  – CVSS Score: 5.8
  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, 'oidc_validate_redirect_url()' does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring 'mod_auth_openidc' to only allow redirection whose destination matches a given regular expression.

- Vulnerability: CVE-2021-32785

  – CVSS Score: 4.3
  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache ('OIDCCacheEncrypt off', 'OIDCSessionType server-cache', 'OIDCCacheType redis'), 'mod_auth_openidc' wrongly performed argument interpolation before passing Redis requests to 'hiredis', which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the 'hiredis' API. As a workaround, this vulnerability can be mitigated by setting 'OIDCCacheEncrypt' to 'on', as cache keys are cryptographically hashed before use when this option is enabled.

- Vulnerability: CVE-2020-9490
  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2021-44224
  - CVSS Score: 6.4
  - Description: A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).

- Vulnerability: CVE-2021-34798
  - CVSS Score: 5
  - Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2021-44790
  - CVSS Score: 7.5
  - Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

- Vulnerability: CVE-2013-0942
  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2012-3526
  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2021-26690
  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service

- Vulnerability: CVE-2021-26691
  - CVSS Score: 7.5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow

- Vulnerability: CVE-2022-26377

  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2023-45802

  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- Vulnerability: CVE-2020-13938

  - CVSS Score: 2.1
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

- Vulnerability: CVE-2019-10081

  - CVSS Score: 5
  - Description: HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example configured with "H2PushResource", could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client.

- Vulnerability: CVE-2018-1283

  - CVSS Score: 3.5

- Description: In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to forward its session data to CGI applications (SessionEnv on, not the default), a remote user may influence their content by using a "Session" header. This comes from the "HTTP_SESSION" variable name used by mod_session to forward its data to CGIs, since the prefix "HTTP_" is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications.

- Vulnerability: CVE-2019-10082

  - CVSS Score: 6.4
  - Description: In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.

- Vulnerability: CVE-2018-1312

  - CVSS Score: 6.8
  - Description: In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

- Vulnerability: CVE-2018-20676

  - CVSS Score: 4.3
  - Description: In Bootstrap before 3.4.0, XSS is possible in the tooltip data-viewport attribute.

- Vulnerability: CVE-2024-38477

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2019-0217

  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2021-39275

  - CVSS Score: 7.5
  - Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2022-28615

  – CVSS Score: 6.4
  – Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- Vulnerability: CVE-2022-28614

  – CVSS Score: 5
  – Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

- Vulnerability: CVE-2022-22719

  – CVSS Score: 5
  – Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

11.34 IP Address: 18.200.39.12

- Organization: Amazon Data Services Ireland Limited

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 22

- Medium Vulnerabilities: 94

- Low Vulnerabilities: 8

- Total Vulnerabilities: 124

Services Running on IP Address

- Service: Apache httpd

  – Port: 80
  – Version: 2.4.29
  – Location: /

- Service: Apache httpd

  – Port: 443
  – Version: 2.4.29
  – Location: /

Vulnerabilities Found

- Vulnerability: CVE-2019-0220

  – CVSS Score: 5
  – Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38.
    When the path component of a request URL contains multiple
    consecutive slashes ('/'), directives such as LocationMatch and
    RewriteRule must account for duplicates in regular expressions while
    other aspects of the servers processing will implicitly collapse
    them.

- Vulnerability: CVE-2024-27316

  – CVSS Score: N/A
  – Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered
    in nghttp2 in order to generate an informative HTTP 413 response.
    If a client does not stop sending headers, this leads to memory
    exhaustion.

- Vulnerability: CVE-2011-2688

  – CVSS Score: 7.5
  – Description: SQL injection vulnerability in mysql/mysql-auth.pl in the
    mod_authnz_external module 3.2.5 and earlier for the Apache HTTP
    Server allows remote attackers to execute arbitrary SQL commands
    via the user field.

- Vulnerability: CVE-2013-2765

  – CVSS Score: 5
  – Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server
    allows remote attackers to cause a denial of service (NULL pointer
    dereference, process crash, and disk consumption) via a POST request
    with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2020-1934

  – CVSS Score: 5
  – Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

- Vulnerability: CVE-2018-17189

  – CVSS Score: 5
  – Description: In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 (mod_http2) connections.

- Vulnerability: CVE-2022-36760

  – CVSS Score: N/A
  – Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2020-35452

  – CVSS Score: 6.8
  – Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

- Vulnerability: CVE-2022-29404

  – CVSS Score: 5
  – Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2021-33193

  – CVSS Score: 5
  – Description: A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.

- Vulnerability: CVE-2009-0796

  – CVSS Score: 2.6
  – Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2013-4365

  – CVSS Score: 7.5
  – Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2018-1333

  - CVSS Score: 5
  - Description: By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.18-2.4.30,2.4.33).

- Vulnerability: CVE-2022-22720

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2018-11763

  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.17 to 2.4.34, by sending continuous, large SETTINGS frames a client can occupy a connection, server thread and CPU time without any connection timeout coming to effect. This affects only HTTP/2 connections. A possible mitigation is to not enable the h2 protocol.

- Vulnerability: CVE-2022-28330

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2020-11993

  - CVSS Score: 4.3
  - Description: Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2021-32791

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2021-32792

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.

- Vulnerability: CVE-2023-31122

- CVSS Score: N/A
- Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

• Vulnerability: CVE-2019-9517

- CVSS Score: 7.8
- Description: Some HTTP/2 implementations are vulnerable to unconstrained interal data buffering, potentially leading to a denial of service. The attacker opens the HTTP/2 window so the peer can send without constraint; however, they leave the TCP window closed so the peer cannot actually write (many of) the bytes on the wire. The attacker then sends a stream of requests for a large response object. Depending on how the servers queue the responses, this can consume excess memory, CPU, or both.

• Vulnerability: CVE-2024-38476

- CVSS Score: N/A
- Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

• Vulnerability: CVE-2024-38477

- CVSS Score: N/A
- Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

• Vulnerability: CVE-2024-38474

- CVSS Score: N/A
- Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

• Vulnerability: CVE-2019-0196

- CVSS Score: 5
- Description: A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.

• Vulnerability: CVE-2019-0211

- CVSS Score: 7.2
- Description: In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.

• Vulnerability: CVE-2022-22721

- CVSS Score: 5.8
- Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2006-20001

  - CVSS Score: N/A

  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2019-10092

  - CVSS Score: 4.3

  - Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1

  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2019-17567

  - CVSS Score: 5

  - Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

- Vulnerability: CVE-2017-15715

  - CVSS Score: 6.8

  - Description: In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.

- Vulnerability: CVE-2022-31813

  - CVSS Score: 7.5

  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

- Vulnerability: CVE-2012-4001

  – CVSS Score: 5
  – Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server
    does not properly verify its host name, which allows remote attackers
    to trigger HTTP requests to arbitrary hosts via unspecified vectors,
    as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2019-10098

  – CVSS Score: 5.8
  – Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with
    mod_rewrite that were intended to be self-referential might be fooled
    by encoded newlines and redirect instead to an unexpected URL within
    the request URL.

- Vulnerability: CVE-2022-37436

  – CVSS Score: N/A
  – Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause
    the response headers to be truncated early, resulting in some headers
    being incorporated into the response body. If the later headers have
    any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2012-4360

  – CVSS Score: 4.3
  – Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module
    0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote
    attackers to inject arbitrary web script or HTML via unspecified
    vectors.

- Vulnerability: CVE-2021-40438

  – CVSS Score: 6.8
  – Description: A crafted request uri-path can cause mod_proxy to forward the request
    to an origin server choosen by the remote user. This issue affects
    Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2011-1176

  – CVSS Score: 4.3
  – Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk
    Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP
    Server does not properly handle certain configuration sections that
    specify NiceValue but not AssignUserID, which might allow remote
    attackers to gain privileges by leveraging the root uid and root gid
    of an mpm-itk process.

- Vulnerability: CVE-2022-23943

  – CVSS Score: 7.5
  – Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server
    allows an attacker to overwrite heap memory with possibly attacker
    provided data. This issue affects Apache HTTP Server 2.4 version
    2.4.52 and prior versions.

- Vulnerability: CVE-2020-1927

  – CVSS Score: 5.8
  – Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with
    mod_rewrite that were intended to be self-referential might be fooled
    by encoded newlines and redirect instead to an an unexpected URL
    within the request URL.

- Vulnerability: CVE-2018-17199

  – CVSS Score: 5
  – Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

- Vulnerability: CVE-2017-15710

  – CVSS Score: 5
  – Description: In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.

- Vulnerability: CVE-2018-1301

  – CVSS Score: 4.3
  – Description: A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.

- Vulnerability: CVE-2018-1302

  – CVSS Score: 4.3
  – Description: When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.

- Vulnerability: CVE-2018-1303

  – CVSS Score: 5
  – Description: A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache. The vulnerability is considered as low risk since mod_cache_socache is not widely used, mod_cache_disk is not concerned by this vulnerability.

- Vulnerability: CVE-2021-34798

  – CVSS Score: 5
  – Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2023-25690

– CVSS Score: N/A

  – Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2021-32786

  – CVSS Score: 5.8

  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, 'oidc_validate_redirect_url()' does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring 'mod_auth_openidc' to only allow redirection whose destination matches a given regular expression.

- Vulnerability: CVE-2021-32785

  – CVSS Score: 4.3

  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache ('OIDCCacheEncrypt off', 'OIDCSessionType server-cache', 'OIDCCacheType redis'), 'mod_auth_openidc' wrongly performed argument interpolation before passing Redis requests to 'hiredis', which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the 'hiredis' API. As a workaround, this vulnerability can be mitigated by setting 'OIDCCacheEncrypt' to 'on', as cache keys are cryptographically hashed before use when this option is enabled.

- Vulnerability: CVE-2020-9490

  – CVSS Score: 5

  – Description: Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2021-44224

  - CVSS Score: 6.4
  - Description: A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).

- Vulnerability: CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2021-44790

  - CVSS Score: 7.5
  - Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2021-26690

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service

- Vulnerability: CVE-2021-26691

  - CVSS Score: 7.5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow

- Vulnerability: CVE-2022-26377

  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2023-45802

  - CVSS Score: N/A

- Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that. This was found by the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out. Users are recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-28614

  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

- Vulnerability: CVE-2020-13938

  - CVSS Score: 2.1
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

- Vulnerability: CVE-2019-10081

  - CVSS Score: 5
  - Description: HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example configured with "H2PushResource", could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client.

- Vulnerability: CVE-2018-1283

  - CVSS Score: 3.5
  - Description: In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to forward its session data to CGI applications (SessionEnv on, not the default), a remote user may influence their content by using a "Session" header. This comes from the "HTTP_SESSION" variable name used by mod_session to forward its data to CGIs, since the prefix "HTTP_" is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications.

- Vulnerability: CVE-2019-10082

  - CVSS Score: 6.4
  - Description: In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.

- Vulnerability: CVE-2018-1312

  - CVSS Score: 6.8

– Description: In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest
                  authentication challenge, the nonce sent to prevent reply attacks
                  was not correctly generated using a pseudo-random seed. In a cluster
                  of servers using a common Digest authentication configuration, HTTP
                  requests could be replayed across servers by an attacker without
                  detection.

- Vulnerability: CVE-2012-3526

  – CVSS Score: 5
  – Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the
                  Apache HTTP Server allows remote attackers to cause a denial of
                  service (server or application crash) via multiple X-Forwarded-For
                  headers in a request.

- Vulnerability: CVE-2024-40898

  – CVSS Score: N/A
  – Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in
                  server/vhost context, allows to potentially leak NTML hashes to
                  a malicious server via SSRF and malicious requests.Users are
                  recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2019-0217

  – CVSS Score: 6
  – Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition
                  in mod_auth_digest when running in a threaded server could allow a
                  user with valid credentials to authenticate using another username,
                  bypassing configured access control restrictions.

- Vulnerability: CVE-2009-2299

  – CVSS Score: 5
  – Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module
                  before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before
                  3.1.1-11637, a module for the Apache HTTP Server, allows remote
                  attackers to cause a denial of service (memory consumption) via an
                  HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2021-39275

  – CVSS Score: 7.5
  – Description: ap_escape_quotes() may write beyond the end of a buffer when given
                  malicious input. No included modules pass untrusted data to these
                  functions, but third-party / external modules may. This issue
                  affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2022-28615

  – CVSS Score: 6.4
  – Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose
                  information due to a read beyond bounds in ap_strcmp_match() when
                  provided with an extremely large input buffer. While no code
                  distributed with the server can be coerced into such a call,
                  third-party modules or lua scripts that use ap_strcmp_match() may
                  hypothetically be affected.

- Vulnerability: CVE-2022-30556

  – CVSS Score: 5
  – Description: Apache HTTP Server 2.4.53 and earlier may return lengths to
                  applications calling r:wsread() that point past the end of the
                  storage allocated for the buffer.

- Vulnerability: CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2019-0220

  - CVSS Score: 5
  - Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.

- Vulnerability: CVE-2024-27316

  - CVSS Score: N/A
  - Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2020-1934

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

- Vulnerability: CVE-2018-17189

  - CVSS Score: 5
  - Description: In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 (mod_http2) connections.

- Vulnerability: CVE-2022-36760

  - CVSS Score: N/A
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2020-35452
  - CVSS Score: 6.8
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

- Vulnerability: CVE-2022-29404
  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2021-33193
  - CVSS Score: 5
  - Description: A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.

- Vulnerability: CVE-2009-0796
  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2013-4365
  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2018-1333
  - CVSS Score: 5
  - Description: By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.18-2.4.30,2.4.33).

- Vulnerability: CVE-2022-22720
  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2018-11763
  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.17 to 2.4.34, by sending continuous, large SETTINGS frames a client can occupy a connection, server thread and CPU time without any connection timeout coming to effect. This affects only HTTP/2 connections. A possible mitigation is to not enable the h2 protocol.

- Vulnerability: CVE-2022-28330

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2020-11993

  - CVSS Score: 4.3
  - Description: Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2021-32791

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2021-32792

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.

- Vulnerability: CVE-2023-31122

  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2019-9517

  - CVSS Score: 7.8
  - Description: Some HTTP/2 implementations are vulnerable to unconstrained interal data buffering, potentially leading to a denial of service. The attacker opens the HTTP/2 window so the peer can send without constraint; however, they leave the TCP window closed so the peer cannot actually write (many of) the bytes on the wire. The attacker then sends a stream of requests for a large response object. Depending on how the servers queue the responses, this can consume excess memory, CPU, or both.

- Vulnerability: CVE-2024-38476

  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-38477

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59
                 and earlier allows an attacker to crash the server via a malicious
                 request.Users are recommended to upgrade to version 2.4.60, which
                 fixes this issue.

- Vulnerability: CVE-2024-38474

  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server
                 2.4.59 and earlier allows attacker to execute scripts indirectories
                 permitted by the configuration but not directly reachable by anyURL
                 or source disclosure of scripts meant to only to be executed as
                 CGI.Users are recommended to upgrade to version 2.4.60, which fixes
                 this issue.Some RewriteRules that capture and substitute unsafely
                 will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2019-0196

  - CVSS Score: 5
  - Description: A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38.
                 Using fuzzed network input, the http/2 request handling could be
                 made to access freed memory in string comparison when determining the
                 method of a request and thus process the request incorrectly.

- Vulnerability: CVE-2019-0211

  - CVSS Score: 7.2
  - Description: In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event,
                 worker or prefork, code executing in less-privileged child processes
                 or threads (including scripts executed by an in-process scripting
                 interpreter) could execute arbitrary code with the privileges of
                 the parent process (usually root) by manipulating the scoreboard.
                 Non-Unix systems are not affected.

- Vulnerability: CVE-2022-22721

  - CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than
                 350MB (defaults to 1M) on 32 bit systems an integer overflow happens
                 which later causes out of bounds writes. This issue affects Apache
                 HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2006-20001

  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or
                 write of a single zero byte, in a pool (heap) memory location beyond
                 the header value sent. This could cause the process to crash.This
                 issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2019-10092

  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting
                 issue was reported affecting the mod_proxy error page. An attacker
                 could cause the link on the error page to be malformed and instead
                 point to a page of their choice. This would only be exploitable
                 where a server was set up with proxying enabled but was misconfigured
                 in such a way that the Proxy Error page was displayed.

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2019-17567

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

- Vulnerability: CVE-2017-15715

  - CVSS Score: 6.8
  - Description: In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.

- Vulnerability: CVE-2022-31813

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

- Vulnerability: CVE-2012-4001

  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2019-10098

  - CVSS Score: 5.8
  - Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.

- Vulnerability: CVE-2022-37436

  - CVSS Score: N/A
  - Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2012-4360
  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
- Vulnerability: CVE-2021-40438
  - CVSS Score: 6.8
  - Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.
- Vulnerability: CVE-2011-1176
  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.
- Vulnerability: CVE-2022-23943
  - CVSS Score: 7.5
  - Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.
- Vulnerability: CVE-2020-1927
  - CVSS Score: 5.8
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.
- Vulnerability: CVE-2018-17199
  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.
- Vulnerability: CVE-2017-15710
  - CVSS Score: 5
  - Description: In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.

1008

- Vulnerability: CVE-2018-1301

  – CVSS Score: 4.3
  – Description: A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.

- Vulnerability: CVE-2018-1302

  – CVSS Score: 4.3
  – Description: When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.

- Vulnerability: CVE-2018-1303

  – CVSS Score: 5
  – Description: A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache. The vulnerability is considered as low risk since mod_cache_socache is not widely used, mod_cache_disk is not concerned by this vulnerability.

- Vulnerability: CVE-2021-34798

  – CVSS Score: 5
  – Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2023-25690

  – CVSS Score: N/A
  – Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2021-32786

  – CVSS Score: 5.8

- Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, `oidc_validate_redirect_url()` does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring `mod_auth_openidc` to only allow redirection whose destination matches a given regular expression.

- Vulnerability: CVE-2021-32785

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache (`OIDCCacheEncrypt off`, `OIDCSessionType server-cache`, `OIDCCacheType redis`), `mod_auth_openidc` wrongly performed argument interpolation before passing Redis requests to `hiredis`, which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the `hiredis` API. As a workaround, this vulnerability can be mitigated by setting `OIDCCacheEncrypt` to `on`, as cache keys are cryptographically hashed before use when this option is enabled.

- Vulnerability: CVE-2020-9490

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2021-44224

  - CVSS Score: 6.4
  - Description: A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).

- Vulnerability: CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2021-44790
  - CVSS Score: 7.5
  - Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.
- Vulnerability: CVE-2013-0942
  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
- Vulnerability: CVE-2021-26690
  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service
- Vulnerability: CVE-2021-26691
  - CVSS Score: 7.5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow
- Vulnerability: CVE-2022-26377
  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.
- Vulnerability: CVE-2023-45802
  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.
- Vulnerability: CVE-2022-28614
  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

- Vulnerability: CVE-2020-13938

  - CVSS Score: 2.1
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

- Vulnerability: CVE-2019-10081

  - CVSS Score: 5
  - Description: HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example configured with "H2PushResource", could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client.

- Vulnerability: CVE-2018-1283

  - CVSS Score: 3.5
  - Description: In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to forward its session data to CGI applications (SessionEnv on, not the default), a remote user may influence their content by using a "Session" header. This comes from the "HTTP_SESSION" variable name used by mod_session to forward its data to CGIs, since the prefix "HTTP_" is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications.

- Vulnerability: CVE-2019-10082

  - CVSS Score: 6.4
  - Description: In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.

- Vulnerability: CVE-2018-1312

  - CVSS Score: 6.8
  - Description: In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

- Vulnerability: CVE-2012-3526

  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2024-40898

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2019-0217

  - CVSS Score: 6

- Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.

- **Vulnerability: CVE-2009-2299**

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- **Vulnerability: CVE-2021-39275**

  - CVSS Score: 7.5
  - Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

- **Vulnerability: CVE-2022-28615**

  - CVSS Score: 6.4
  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- **Vulnerability: CVE-2022-30556**

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- **Vulnerability: CVE-2022-22719**

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

11.35 IP Address: 159.149.130.90

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 20

- Medium Vulnerabilities: 70

- Low Vulnerabilities: 6

- Total Vulnerabilities: 96

Services Running on IP Address

- Service: OpenSSH

  - Port: 22
  - Version: 8.2p1 Ubuntu-4ubuntu0.11
  - Location:

- Service: Postfix smtpd

  - Port: 25
  - Version: N/A
  - Location:

- Service: Apache httpd

  - Port: 80
  - Version: 2.4.41
  - Location: /

- Service: Apache httpd

  - Port: 443
  - Version: 2.4.41
  - Location: /

Vulnerabilities Found

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server
                   allows remote attackers to cause a denial of service (NULL pointer
                   dereference, process crash, and disk consumption) via a POST request
                   with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2020-1934

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use
                   uninitialized memory when proxying to a malicious FTP server.

- Vulnerability: CVE-2022-36760

  - CVSS Score: N/A

- Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- **Vulnerability: CVE-2020-35452**

  - CVSS Score: 6.8
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

- **Vulnerability: CVE-2022-29404**

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- **Vulnerability: CVE-2023-27522**

  - CVSS Score: N/A
  - Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.Special characters in the origin response header can truncate/split the response forwarded to the client.

- **Vulnerability: CVE-2009-0796**

  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- **Vulnerability: CVE-2013-4365**

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- **Vulnerability: CVE-2022-22720**

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- **Vulnerability: CVE-2021-30641**

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.39 to 2.4.46 Unexpected matching behavior with 'MergeSlashes OFF'

- **Vulnerability: CVE-2022-28330**

  - CVSS Score: 5

- Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2020-11993

  - CVSS Score: 4.3
  - Description: Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2021-32791

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2021-32792

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.

- Vulnerability: CVE-2023-31122

  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2024-38476

  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-27316

  - CVSS Score: N/A
  - Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

- Vulnerability: CVE-2024-38474

  - CVSS Score: N/A

- Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server
  2.4.59 and earlier allows attacker to execute scripts indirectories
  permitted by the configuration but not directly reachable by anyURL
  or source disclosure of scripts meant to only to be executed as
  CGI.Users are recommended to upgrade to version 2.4.60, which fixes
  this issue.Some RewriteRules that capture and substitute unsafely
  will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2022-22721

  – CVSS Score: 5.8

  – Description: If LimitXMLRequestBody is set to allow request bodies larger than
    350MB (defaults to 1M) on 32 bit systems an integer overflow happens
    which later causes out of bounds writes. This issue affects Apache
    HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2006-20001

  – CVSS Score: N/A

  – Description: A carefully crafted If: request header can cause a memory read, or
    write of a single zero byte, in a pool (heap) memory location beyond
    the header value sent. This could cause the process to crash.This
    issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2021-33193

  – CVSS Score: 5

  – Description: A crafted method sent through HTTP/2 will bypass validation and be
    forwarded by mod_proxy, which can lead to request splitting or cache
    poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.

- Vulnerability: CVE-2013-0941

  – CVSS Score: 2.1

  – Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5
    for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM
    Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows
    use an improper encryption algorithm and a weak key for maintaining
    the stored data of the node secret for the SecurID Authentication
    API, which allows local users to obtain sensitive information via
    cryptographic attacks on this data.

- Vulnerability: CVE-2019-17567

  – CVSS Score: 5

  – Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel
    configured on an URL that is not necessarily Upgraded by the origin
    server was tunneling the whole connection regardless, thus allowing
    for subsequent requests on the same connection to pass through
    with no HTTP validation, authentication or authorization possibly
    configured.

- Vulnerability: CVE-2012-3526

  – CVSS Score: 5

  – Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the
    Apache HTTP Server allows remote attackers to cause a denial of
    service (server or application crash) via multiple X-Forwarded-For
    headers in a request.

- Vulnerability: CVE-2022-31813

  – CVSS Score: 7.5

- Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-*
                headers to the origin server based on client side Connection
                header hop-by-hop mechanism. This may be used to bypass IP based
                authentication on the origin server/application.

• Vulnerability: CVE-2012-4001

  − CVSS Score: 5
  − Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server
                  does not properly verify its host name, which allows remote attackers
                  to trigger HTTP requests to arbitrary hosts via unspecified vectors,
                  as demonstrated by requests to intranet servers.

• Vulnerability: CVE-2022-37436

  − CVSS Score: N/A
  − Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause
                  the response headers to be truncated early, resulting in some headers
                  being incorporated into the response body. If the later headers have
                  any security purpose, they will not be interpreted by the client.

• Vulnerability: CVE-2012-4360

  − CVSS Score: 4.3
  − Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module
                  0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote
                  attackers to inject arbitrary web script or HTML via unspecified
                  vectors.

• Vulnerability: CVE-2020-11022

  − CVSS Score: 4.3
  − Description: In jQuery versions greater than or equal to 1.2 and before 3.5.0,
                  passing HTML from untrusted sources - even after sanitizing it - to
                  one of jQuery's DOM manipulation methods (i.e. .html(), .append(),
                  and others) may execute untrusted code. This problem is patched in
                  jQuery 3.5.0.

• Vulnerability: CVE-2020-11023

  − CVSS Score: 4.3
  − Description: In jQuery versions greater than or equal to 1.0.3 and before 3.5.0,
                  passing HTML containing <option> elements from untrusted sources
                  - even after sanitizing it - to one of jQuery's DOM manipulation
                  methods (i.e. .html(), .append(), and others) may execute untrusted
                  code. This problem is patched in jQuery 3.5.0.

• Vulnerability: CVE-2021-40438

  − CVSS Score: 6.8
  − Description: A crafted request uri-path can cause mod_proxy to forward the request
                  to an origin server choosen by the remote user. This issue affects
                  Apache HTTP Server 2.4.48 and earlier.

• Vulnerability: CVE-2011-1176

  − CVSS Score: 4.3
  − Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk
                  Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP
                  Server does not properly handle certain configuration sections that
                  specify NiceValue but not AssignUserID, which might allow remote
                  attackers to gain privileges by leveraging the root uid and root gid
                  of an mpm-itk process.

- Vulnerability: CVE-2021-36160
  - CVSS Score: 5
  - Description: A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS). This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48 (inclusive).
- Vulnerability: CVE-2022-23943
  - CVSS Score: 7.5
  - Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.
- Vulnerability: CVE-2020-1927
  - CVSS Score: 5.8
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.
- Vulnerability: CVE-2024-40898
  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.
- Vulnerability: CVE-2011-2688
  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.
- Vulnerability: CVE-2021-34798
  - CVSS Score: 5
  - Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.
- Vulnerability: CVE-2023-25690
  - CVSS Score: N/A
  - Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.
- Vulnerability: CVE-2021-32786

- CVSS Score: 5.8
- Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, `oidc_validate_redirect_url()` does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring `mod_auth_openidc` to only allow redirection whose destination matches a given regular expression.

- Vulnerability: CVE-2021-32785

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache (`OIDCCacheEncrypt off`, `OIDCSessionType server-cache`, `OIDCCacheType redis`), `mod_auth_openidc` wrongly performed argument interpolation before passing Redis requests to `hiredis`, which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the `hiredis` API. As a workaround, this vulnerability can be mitigated by setting `OIDCCacheEncrypt` to `on`, as cache keys are cryptographically hashed before use when this option is enabled.

- Vulnerability: CVE-2020-9490

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2021-44224

  - CVSS Score: 6.4
  - Description: A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).

- Vulnerability: CVE-2007-4723

  - CVSS Score: 7.5

- Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2020-11984

  - CVSS Score: 7.5
  - Description: Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE

- Vulnerability: CVE-2021-44790

  - CVSS Score: 7.5
  - Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2021-26690

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service

- Vulnerability: CVE-2021-26691

  - CVSS Score: 7.5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow

- Vulnerability: CVE-2022-26377

  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2023-45802

  - CVSS Score: N/A

- Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-28614

  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

- Vulnerability: CVE-2020-13938

  - CVSS Score: 2.1
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2020-13950

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.41 to 2.4.46 mod_proxy_http can be made to crash (NULL pointer dereference) with specially crafted requests using both Content-Length and Transfer-Encoding headers, leading to a Denial of Service

- Vulnerability: CVE-2024-38477

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2021-39275

  - CVSS Score: 7.5
  - Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2022-28615
  - CVSS Score: 6.4
  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.
- Vulnerability: CVE-2022-30556
  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.
- Vulnerability: CVE-2022-22719
  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.
- Vulnerability: CVE-2013-2765
  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.
- Vulnerability: CVE-2020-1934
  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.
- Vulnerability: CVE-2022-36760
  - CVSS Score: N/A
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.
- Vulnerability: CVE-2020-35452
  - CVSS Score: 6.8
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow
- Vulnerability: CVE-2022-29404
  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2023-27522

  – CVSS Score: N/A
  – Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.Special characters in the origin response header can truncate/split the response forwarded to the client.

- Vulnerability: CVE-2009-0796

  – CVSS Score: 2.6
  – Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2013-4365

  – CVSS Score: 7.5
  – Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2022-22720

  – CVSS Score: 7.5
  – Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2021-30641

  – CVSS Score: 5
  – Description: Apache HTTP Server versions 2.4.39 to 2.4.46 Unexpected matching behavior with 'MergeSlashes OFF'

- Vulnerability: CVE-2022-28330

  – CVSS Score: 5
  – Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2020-11993

  – CVSS Score: 4.3
  – Description: Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2021-32791

  – CVSS Score: 4.3
  – Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2021-32792

  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.

- Vulnerability: CVE-2023-31122

  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2024-38476

  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-27316

  - CVSS Score: N/A
  - Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

- Vulnerability: CVE-2024-38474

  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2022-22721

  - CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2006-20001

  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2021-33193

  - CVSS Score: 5

- Description: A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.

- **Vulnerability: CVE-2013-0941**

  – CVSS Score: 2.1
  – Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- **Vulnerability: CVE-2019-17567**

  – CVSS Score: 5
  – Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

- **Vulnerability: CVE-2012-3526**

  – CVSS Score: 5
  – Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- **Vulnerability: CVE-2022-31813**

  – CVSS Score: 7.5
  – Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

- **Vulnerability: CVE-2012-4001**

  – CVSS Score: 5
  – Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- **Vulnerability: CVE-2022-37436**

  – CVSS Score: N/A
  – Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- **Vulnerability: CVE-2012-4360**

  – CVSS Score: 4.3
  – Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2020-11022

  – CVSS Score: 4.3
  – Description: In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

- Vulnerability: CVE-2020-11023

  – CVSS Score: 4.3
  – Description: In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

- Vulnerability: CVE-2021-40438

  – CVSS Score: 6.8
  – Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2011-1176

  – CVSS Score: 4.3
  – Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2021-36160

  – CVSS Score: 5
  – Description: A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS). This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48 (inclusive).

- Vulnerability: CVE-2022-23943

  – CVSS Score: 7.5
  – Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

- Vulnerability: CVE-2020-1927

  – CVSS Score: 5.8
  – Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.

- Vulnerability: CVE-2024-40898

  – CVSS Score: N/A

- Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- **Vulnerability:** CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- **Vulnerability:** CVE-2021-34798

  - CVSS Score: 5
  - Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- **Vulnerability:** CVE-2023-25690

  - CVSS Score: N/A
  - Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- **Vulnerability:** CVE-2021-32786

  - CVSS Score: 5.8
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, 'oidc_validate_redirect_url()' does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring 'mod_auth_openidc' to only allow redirection whose destination matches a given regular expression.

- **Vulnerability:** CVE-2021-32785

  - CVSS Score: 4.3

– Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache (‘OIDCCacheEncrypt off‘, ‘OIDCSessionType server-cache‘, ‘OIDCCacheType redis‘), ‘mod_auth_openidc‘ wrongly performed argument interpolation before passing Redis requests to ‘hiredis‘, which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the ‘hiredis‘ API. As a workaround, this vulnerability can be mitigated by setting ‘OIDCCacheEncrypt‘ to ‘on‘, as cache keys are cryptographically hashed before use when this option is enabled.

• Vulnerability: CVE-2020-9490

   – CVSS Score: 5

   – Description: Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.

• Vulnerability: CVE-2021-44224

   – CVSS Score: 6.4

   – Description: A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).

• Vulnerability: CVE-2007-4723

   – CVSS Score: 7.5

   – Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

• Vulnerability: CVE-2020-11984

   – CVSS Score: 7.5

   – Description: Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE

• Vulnerability: CVE-2021-44790

   – CVSS Score: 7.5

   – Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

• Vulnerability: CVE-2013-0942

- CVSS Score: 4.3
- Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2021-26690

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service

- Vulnerability: CVE-2021-26691

  - CVSS Score: 7.5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow

- Vulnerability: CVE-2022-26377

  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2023-45802

  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-28614

  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

- Vulnerability: CVE-2020-13938

  - CVSS Score: 2.1
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

- Vulnerability: CVE-2009-2299

- CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2020-13950

  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.41 to 2.4.46 mod_proxy_http can be made to crash (NULL pointer dereference) with specially crafted requests using both Content-Length and Transfer-Encoding headers, leading to a Denial of Service

- Vulnerability: CVE-2024-38477

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2021-39275

  - CVSS Score: 7.5
  - Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2022-28615

  - CVSS Score: 6.4
  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- Vulnerability: CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

11.36   IP Address: 159.149.129.249

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 19

- Medium Vulnerabilities: 47

- Low Vulnerabilities: 6

- Total Vulnerabilities: 72

Services Running on IP Address

- Service: OpenSSH

  - Port: 22
  - Version: 8.9p1 Ubuntu-3ubuntu0.10
  - Location:

- Service: Apache httpd

  - Port: 80
  - Version: 2.4.52
  - Location: https://tutoraggio.di.unimi.it

- Service: Apache httpd

  - Port: 443
  - Version: 2.4.52
  - Location: /

- Service: Apache httpd

  - Port: 8080
  - Version: 2.4.52
  - Location: /

Vulnerabilities Found

- Vulnerability: CVE-2024-27316

  - CVSS Score: N/A
  - Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered
                  in nghttp2 in order to generate an informative HTTP 413 response.
                  If a client does not stop sending headers, this leads to memory
                  exhaustion.
- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server
                  allows remote attackers to cause a denial of service (NULL pointer
                  dereference, process crash, and disk consumption) via a POST request
                  with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2022-36760

  - CVSS Score: N/A

- Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-29404

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2023-27522

  - CVSS Score: N/A
  - Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.Special characters in the origin response header can truncate/split the response forwarded to the client.

- Vulnerability: CVE-2013-4365

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2022-22720

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2022-28330

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2023-31122

  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2024-38476

  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-38477

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-38474
  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2022-22721
  - CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2006-20001
  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2009-0796
  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2012-3526
  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2022-31813
  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

- Vulnerability: CVE-2012-4001
  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2022-37436
  - CVSS Score: N/A

– Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause
                the response headers to be truncated early, resulting in some headers
                being incorporated into the response body. If the later headers have
                any security purpose, they will not be interpreted by the client.

• Vulnerability: CVE-2012-4360

  – CVSS Score: 4.3
  – Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module
                  0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote
                  attackers to inject arbitrary web script or HTML via unspecified
                  vectors.

• Vulnerability: CVE-2011-1176

  – CVSS Score: 4.3
  – Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk
                  Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP
                  Server does not properly handle certain configuration sections that
                  specify NiceValue but not AssignUserID, which might allow remote
                  attackers to gain privileges by leveraging the root uid and root gid
                  of an mpm-itk process.

• Vulnerability: CVE-2022-23943

  – CVSS Score: 7.5
  – Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server
                  allows an attacker to overwrite heap memory with possibly attacker
                  provided data. This issue affects Apache HTTP Server 2.4 version
                  2.4.52 and prior versions.

• Vulnerability: CVE-2011-2688

  – CVSS Score: 7.5
  – Description: SQL injection vulnerability in mysql/mysql-auth.pl in the
                  mod_authnz_external module 3.2.5 and earlier for the Apache HTTP
                  Server allows remote attackers to execute arbitrary SQL commands
                  via the user field.

• Vulnerability: CVE-2023-25690

  – CVSS Score: N/A
  – Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0
                  through 2.4.55 allow a HTTP Request Smuggling attack.Configurations
                  are affected when mod_proxy is enabled along with some form of
                  RewriteRule or ProxyPassMatch in which a non-specific pattern
                  matches some portion of the user-supplied request-target (URL)
                  data and is then re-inserted into the proxied request-target using
                  variable substitution. For example, something like:RewriteEngine
                  onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1";
                  [P]ProxyPassReverse /here/ http://example.com:8080/Request
                  splitting/smuggling could result in bypass of access controls in the
                  proxy server, proxying unintended URLs to existing origin servers,
                  and cache poisoning. Users are recommended to update to at least
                  version 2.4.56 of Apache HTTP Server.

• Vulnerability: CVE-2007-4723

  – CVSS Score: 7.5

- Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- **Vulnerability:** CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- **Vulnerability:** CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- **Vulnerability:** CVE-2022-26377

  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- **Vulnerability:** CVE-2023-45802

  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

- **Vulnerability:** CVE-2022-28614

  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2024-40898

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2022-28615

  - CVSS Score: 6.4
  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- Vulnerability: CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2022-36760

  - CVSS Score: N/A
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-29404

  - CVSS Score: 5

- Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2023-27522

  - CVSS Score: N/A
  - Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.Special characters in the origin response header can truncate/split the response forwarded to the client.

- Vulnerability: CVE-2013-4365

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2024-38276

  - CVSS Score: N/A
  - Description: Incorrect CSRF token checks resulted in multiple CSRF risks.

- Vulnerability: CVE-2022-22720

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2022-28330

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2023-31122

  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2024-38476

  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-27316

  - CVSS Score: N/A
  - Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

- Vulnerability: CVE-2024-38474

  - CVSS Score: N/A

– Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server
2.4.59 and earlier allows attacker to execute scripts indirectories
permitted by the configuration but not directly reachable by anyURL
or source disclosure of scripts meant to only to be executed as
CGI.Users are recommended to upgrade to version 2.4.60, which fixes
this issue.Some RewriteRules that capture and substitute unsafely
will now fail unless rewrite flag "UnsafeAllow3F" is specified.

• Vulnerability: CVE-2022-22721

– CVSS Score: 5.8

– Description: If LimitXMLRequestBody is set to allow request bodies larger than
350MB (defaults to 1M) on 32 bit systems an integer overflow happens
which later causes out of bounds writes. This issue affects Apache
HTTP Server 2.4.52 and earlier.

• Vulnerability: CVE-2006-20001

– CVSS Score: N/A

– Description: A carefully crafted If: request header can cause a memory read, or
write of a single zero byte, in a pool (heap) memory location beyond
the header value sent. This could cause the process to crash.This
issue affects Apache HTTP Server 2.4.54 and earlier.

• Vulnerability: CVE-2009-0796

– CVSS Score: 2.6

– Description: Cross-site scripting (XSS) vulnerability in Status.pm in
Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the
Apache HTTP Server, when /perl-status is accessible, allows remote
attackers to inject arbitrary web script or HTML via the URI.

• Vulnerability: CVE-2024-34008

– CVSS Score: N/A

– Description: Actions in the admin management of analytics models did not include
the necessary token to prevent a CSRF risk.

• Vulnerability: CVE-2012-3526

– CVSS Score: 5

– Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the
Apache HTTP Server allows remote attackers to cause a denial of
service (server or application crash) via multiple X-Forwarded-For
headers in a request.

• Vulnerability: CVE-2022-31813

– CVSS Score: 7.5

– Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-*
headers to the origin server based on client side Connection
header hop-by-hop mechanism. This may be used to bypass IP based
authentication on the origin server/application.

• Vulnerability: CVE-2012-4001

– CVSS Score: 5

– Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server
does not properly verify its host name, which allows remote attackers
to trigger HTTP requests to arbitrary hosts via unspecified vectors,
as demonstrated by requests to intranet servers.

• Vulnerability: CVE-2022-37436

- CVSS Score: N/A
- Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- **Vulnerability: CVE-2012-4360**

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- **Vulnerability: CVE-2011-1176**

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- **Vulnerability: CVE-2022-23943**

  - CVSS Score: 7.5
  - Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

- **Vulnerability: CVE-2024-40898**

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- **Vulnerability: CVE-2013-0942**

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- **Vulnerability: CVE-2007-6538**

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in ing/blocks/mrbs/code/web/view_entry.php in the MRBS plugin for Moodle allows remote attackers to execute arbitrary SQL commands via the id parameter.

- **Vulnerability: CVE-2011-2688**

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2023-46858

  - CVSS Score: N/A
  - Description: Moodle 4.3 allows /grade/report/grader/index.php?searchvalue=
    reflected XSS when logged in as a teacher. NOTE: the Moodle Security
    FAQ link states "Some forms of rich content [are] used by teachers to
    enhance their courses ... admins and teachers can post XSS-capable
    content, but students can not."

- Vulnerability: CVE-2023-25690

  - CVSS Score: N/A
  - Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0
    through 2.4.55 allow a HTTP Request Smuggling attack.Configurations
    are affected when mod_proxy is enabled along with some form of
    RewriteRule or ProxyPassMatch in which a non-specific pattern
    matches some portion of the user-supplied request-target (URL)
    data and is then re-inserted into the proxied request-target using
    variable substitution. For example, something like:RewriteEngine
    onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1";
    [P]ProxyPassReverse /here/ http://example.com:8080/Request
    splitting/smuggling could result in bypass of access controls in the
    proxy server, proxying unintended URLs to existing origin servers,
    and cache poisoning. Users are recommended to update to at least
    version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel
    4.3.4a, when the Apache HTTP Server is used, allows remote attackers
    to bypass authentication via directory traversal sequences in a URI
    that ends with the name of a publicly available page, as demonstrated
    by a "/...../" sequence and an account_manage.php/login.php final
    component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5
    for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM
    Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows
    use an improper encryption algorithm and a weak key for maintaining
    the stored data of the node secret for the SecurID Authentication
    API, which allows local users to obtain sensitive information via
    cryptographic attacks on this data.

- Vulnerability: CVE-2010-4208

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the Flash component
    infrastructure in YUI 2.5.0 through 2.8.1, as used in Bugzilla,
    Moodle, and other products, allows remote attackers to
    inject arbitrary web script or HTML via vectors related to
    uploader/assets/uploader.swf.

- Vulnerability: CVE-2022-26377

  - CVSS Score: 5

- Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2010-4207

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the Flash component infrastructure in YUI 2.4.0 through 2.8.1, as used in Bugzilla, Moodle, and other products, allows remote attackers to inject arbitrary web script or HTML via vectors related to charts/assets/charts.swf.

- Vulnerability: CVE-2023-45802

  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2024-38477

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2022-28615

  - CVSS Score: 6.4
  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- Vulnerability: CVE-2022-28614

  – CVSS Score: 5

  – Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

- Vulnerability: CVE-2022-22719

  – CVSS Score: 5

  – Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2024-27316

  – CVSS Score: N/A

  – Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

- Vulnerability: CVE-2013-2765

  – CVSS Score: 5

  – Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2022-36760

  – CVSS Score: N/A

  – Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-29404

  – CVSS Score: 5

  – Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2023-27522

  – CVSS Score: N/A

  – Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.Special characters in the origin response header can truncate/split the response forwarded to the client.

- Vulnerability: CVE-2013-4365

  – CVSS Score: 7.5

       – Description: Heap-based buffer overflow in the fcgid_header_bucket_read function
                 in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache
                 HTTP Server allows remote attackers to have an unspecified impact via
                 unknown vectors.

- Vulnerability: CVE-2022-22720

  – CVSS Score: 7.5

  – Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound
    connection when errors are encountered discarding the request body,
    exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2022-28330

  – CVSS Score: 5

  – Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond
    bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2023-31122

  – CVSS Score: N/A

  – Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP
    Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2024-38476

  – CVSS Score: N/A

  – Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are
    vulnerably to information disclosure, SSRF or local script execution
    viabackend applications whose response headers are malicious or
    exploitable.Users are recommended to upgrade to version 2.4.60, which
    fixes this issue.

- Vulnerability: CVE-2024-38477

  – CVSS Score: N/A

  – Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59
    and earlier allows an attacker to crash the server via a malicious
    request.Users are recommended to upgrade to version 2.4.60, which
    fixes this issue.

- Vulnerability: CVE-2024-38474

  – CVSS Score: N/A

  – Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server
    2.4.59 and earlier allows attacker to execute scripts indirectories
    permitted by the configuration but not directly reachable by anyURL
    or source disclosure of scripts meant to only to be executed as
    CGI.Users are recommended to upgrade to version 2.4.60, which fixes
    this issue.Some RewriteRules that capture and substitute unsafely
    will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2022-22721

  – CVSS Score: 5.8

  – Description: If LimitXMLRequestBody is set to allow request bodies larger than
    350MB (defaults to 1M) on 32 bit systems an integer overflow happens
    which later causes out of bounds writes. This issue affects Apache
    HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2006-20001

  – CVSS Score: N/A

- Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2009-0796

  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2012-3526

  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2022-31813

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

- Vulnerability: CVE-2012-4001

  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2022-37436

  - CVSS Score: N/A
  - Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2012-4360

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2022-23943

  – CVSS Score: 7.5
  – Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

- Vulnerability: CVE-2011-2688

  – CVSS Score: 7.5
  – Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2023-25690

  – CVSS Score: N/A
  – Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2007-4723

  – CVSS Score: 7.5
  – Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2013-0941

  – CVSS Score: 2.1
  – Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  – CVSS Score: 4.3
  – Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2022-26377

  – CVSS Score: 5

  – Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2023-45802

  – CVSS Score: N/A

  – Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-28614

  – CVSS Score: 5

  – Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

- Vulnerability: CVE-2009-2299

  – CVSS Score: 5

  – Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2024-40898

  – CVSS Score: N/A

  – Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2022-28615

  – CVSS Score: 6.4

  – Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to
                  applications calling r:wsread() that point past the end of the
                  storage allocated for the buffer.

- Vulnerability: CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory
                  area which could cause the process to crash. This issue affects
                  Apache HTTP Server 2.4.52 and earlier.

11.37 IP Address: 159.149.15.70

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 13

- Medium Vulnerabilities: 32

- Low Vulnerabilities: 4

- Total Vulnerabilities: 49

Services Running on IP Address

- Service: Apache httpd

    – Port: 80
    – Version: 2.4.52
    – Location: https://infermieristica.ctu.unimi.it/

- Service: Apache httpd

    – Port: 443
    – Version: 2.4.52
    – Location: /

Vulnerabilities Found

- Vulnerability: CVE-2024-27316

    – CVSS Score: N/A
    – Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

- Vulnerability: CVE-2013-2765

    – CVSS Score: 5
    – Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2022-36760

    – CVSS Score: N/A
    – Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-29404

    – CVSS Score: 5
    – Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2023-27522
  - CVSS Score: N/A
  - Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.Special characters in the origin response header can truncate/split the response forwarded to the client.
- Vulnerability: CVE-2013-4365
  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.
- Vulnerability: CVE-2022-22720
  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling
- Vulnerability: CVE-2022-28330
  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.
- Vulnerability: CVE-2023-31122
  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.
- Vulnerability: CVE-2024-38476
  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.
- Vulnerability: CVE-2024-38477
  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.
- Vulnerability: CVE-2024-38474
  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.
- Vulnerability: CVE-2022-22721

- CVSS Score: 5.8
- Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

• Vulnerability: CVE-2006-20001

- CVSS Score: N/A
- Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

• Vulnerability: CVE-2009-0796

- CVSS Score: 2.6
- Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

• Vulnerability: CVE-2012-3526

- CVSS Score: 5
- Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

• Vulnerability: CVE-2022-31813

- CVSS Score: 7.5
- Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

• Vulnerability: CVE-2012-4001

- CVSS Score: 5
- Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

• Vulnerability: CVE-2022-37436

- CVSS Score: N/A
- Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

• Vulnerability: CVE-2012-4360

- CVSS Score: 4.3
- Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

• Vulnerability: CVE-2011-1176

- CVSS Score: 4.3
- Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- **Vulnerability: CVE-2022-23943**

  - CVSS Score: 7.5
  - Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

- **Vulnerability: CVE-2011-2688**

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- **Vulnerability: CVE-2023-25690**

  - CVSS Score: N/A
  - Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- **Vulnerability: CVE-2007-4723**

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- **Vulnerability: CVE-2013-0941**

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  – CVSS Score: 4.3

  – Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication
                 Agent 7.1 before 7.1.1 for Web for Internet Information Services,
                 and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to
                 inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2022-26377

  – CVSS Score: 5

  – Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request
                 Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server
                 allows an attacker to smuggle requests to the AJP server it forwards
                 requests to. This issue affects Apache HTTP Server Apache HTTP
                 Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2023-45802

  – CVSS Score: N/A

  – Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a
                 time window were the request's memory resources were not reclaimed
                 immediately. Instead, de-allocation was deferred to connection
                 close. A client could send new requests and resets, keeping the
                 connection busy and open and causing the memory footprint to keep
                 on growing. On connection close, all resources were reclaimed, but
                 the process might run out of memory before that.This was found by
                 the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset
                 Exploit) with their own test client. During "normal" HTTP/2 use, the
                 probability to hit this bug is very low. The kept memory would not
                 become noticeable before the connection closes or times out.Users are
                 recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-28614

  – CVSS Score: 5

  – Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier
                 may read unintended memory if an attacker can cause the server to
                 reflect very large input using ap_rwrite() or ap_rputs(), such as
                 with mod_luas r:puts() function. Modules compiled and distributed
                 separately from Apache HTTP Server that use the 'ap_rputs' function
                 and may pass it a very large (INT_MAX or larger) string must be
                 compiled against current headers to resolve the issue.

- Vulnerability: CVE-2009-2299

  – CVSS Score: 5

  – Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module
                 before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before
                 3.1.1-11637, a module for the Apache HTTP Server, allows remote
                 attackers to cause a denial of service (memory consumption) via an
                 HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2024-40898

  – CVSS Score: N/A

  – Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in
                 server/vhost context, allows to potentially leak NTML hashes to
                 a malicious server via SSRF and malicious requests.Users are
                 recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2022-28615

- CVSS Score: 6.4
- Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- Vulnerability: CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2023-5544

  - CVSS Score: N/A
  - Description: Wiki comments required additional sanitizing and access restrictions to prevent a stored XSS risk and potential IDOR risk.

- Vulnerability: CVE-2023-5545

  - CVSS Score: N/A
  - Description: H5P metadata automatically populated the author with the user's username, which could be sensitive information.

- Vulnerability: CVE-2023-5546

  - CVSS Score: N/A
  - Description: ID numbers displayed in the quiz grading report required additional sanitizing to prevent a stored XSS risk.

- Vulnerability: CVE-2023-5547

  - CVSS Score: N/A
  - Description: The course upload preview contained an XSS risk for users uploading unsafe data.

- Vulnerability: CVE-2023-5540

  - CVSS Score: N/A
  - Description: A remote code execution risk was identified in the IMSCP activity. By default this was only available to teachers and managers.

- Vulnerability: CVE-2023-5541

  - CVSS Score: N/A
  - Description: The CSV grade import method contained an XSS risk for users importing the spreadsheet, if it contained unsafe content.

- Vulnerability: CVE-2023-5543

  - CVSS Score: N/A
  - Description: When duplicating a BigBlueButton activity, the original meeting ID was also duplicated instead of using a new ID for the new activity. This could provide unintended access to the original meeting.

- Vulnerability: CVE-2013-2765
  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2023-5548
  - CVSS Score: N/A
  - Description: Stronger revision number limitations were required on file serving endpoints to improve cache poisoning protection.

- Vulnerability: CVE-2023-5549
  - CVSS Score: N/A
  - Description: Insufficient web service capability checks made it possible to move categories a user had permission to manage, to a parent category they did not have the capability to manage.

- Vulnerability: CVE-2023-23921
  - CVSS Score: N/A
  - Description: The vulnerability was found Moodle which exists due to insufficient sanitization of user-supplied data in some returnurl parameters. A remote attacker can trick the victim to follow a specially crafted link and execute arbitrary HTML and script code in user's browser in context of vulnerable website. This flaw allows a remote attacker to perform cross-site scripting (XSS) attacks.

- Vulnerability: CVE-2022-29404
  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2023-27522
  - CVSS Score: N/A
  - Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.Special characters in the origin response header can truncate/split the response forwarded to the client.

- Vulnerability: CVE-2013-4365
  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2023-28333
  - CVSS Score: N/A
  - Description: The Mustache pix helper contained a potential Mustache injection risk if combined with user input (note: This did not appear to be implemented/exploitable anywhere in the core Moodle LMS).

- Vulnerability: CVE-2023-28332
  - CVSS Score: N/A

- Description: If the algebra filter was enabled but not functional (eg the necessary binaries were missing from the server), it presented an XSS risk.

- Vulnerability: CVE-2024-38276

  - CVSS Score: N/A
  - Description: Incorrect CSRF token checks resulted in multiple CSRF risks.

- Vulnerability: CVE-2023-28330

  - CVSS Score: N/A
  - Description: Insufficient sanitizing in backup resulted in an arbitrary file read risk. The capability to access this feature is only available to teachers, managers and admins by default.

- Vulnerability: CVE-2023-28331

  - CVSS Score: N/A
  - Description: Content output by the database auto-linking filter required additional sanitizing to prevent an XSS risk.

- Vulnerability: CVE-2023-28335

  - CVSS Score: N/A
  - Description: The link to reset all templates of a database activity did not include the necessary token to prevent a CSRF risk.

- Vulnerability: CVE-2023-28334

  - CVSS Score: N/A
  - Description: Authenticated users were able to enumerate other users' names via the learning plans page.

- Vulnerability: CVE-2024-38476

  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2023-30944

  - CVSS Score: N/A
  - Description: The vulnerability was found Moodle which exists due to insufficient sanitization of user-supplied data in external Wiki method for listing pages. A remote attacker can send a specially crafted request to the affected application and execute limited SQL commands within the application database.

- Vulnerability: CVE-2024-38474

  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2023-30943

- CVSS Score: N/A
- Description: The vulnerability was found Moodle which exists because the application allows a user to control path of the older to create in TinyMCE loaders. A remote user can send a specially crafted HTTP request and create arbitrary folders on the system.

- **Vulnerability:** CVE-2023-28336

  - CVSS Score: N/A
  - Description: Insufficient filtering of grade report history made it possible for teachers to access the names of users they could not otherwise access.

- **Vulnerability:** CVE-2009-0796

  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- **Vulnerability:** CVE-2024-34008

  - CVSS Score: N/A
  - Description: Actions in the admin management of analytics models did not include the necessary token to prevent a CSRF risk.

- **Vulnerability:** CVE-2022-28330

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- **Vulnerability:** CVE-2022-31813

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

- **Vulnerability:** CVE-2012-4001

  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- **Vulnerability:** CVE-2023-35133

  - CVSS Score: N/A
  - Description: An issue in the logic used to check 0.0.0.0 against the cURL blocked hosts lists resulted in an SSRF risk. This flaw affects Moodle versions 4.2, 4.1 to 4.1.3, 4.0 to 4.0.8, 3.11 to 3.11.14, 3.9 to 3.9.21 and earlier unsupported versions.

- **Vulnerability:** CVE-2023-35132

  - CVSS Score: N/A
  - Description: A limited SQL injection risk was identified on the Mnet SSO access control page. This flaw affects Moodle versions 4.2, 4.1 to 4.1.3, 4.0 to 4.0.8, 3.11 to 3.11.14, 3.9 to 3.9.21 and earlier unsupported versions.

- Vulnerability: CVE-2023-35131
  - CVSS Score: N/A
  - Description: Content on the groups page required additional sanitizing to prevent an XSS risk. This flaw affects Moodle versions 4.2, 4.1 to 4.1.3, 4.0 to 4.0.8 and 3.11 to 3.11.14.
- Vulnerability: CVE-2023-1402
  - CVSS Score: N/A
  - Description: The course participation report required additional checks to prevent roles being displayed which the user did not have access to view.
- Vulnerability: CVE-2022-22721
  - CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.
- Vulnerability: CVE-2012-4360
  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
- Vulnerability: CVE-2011-1176
  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.
- Vulnerability: CVE-2022-23943
  - CVSS Score: 7.5
  - Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.
- Vulnerability: CVE-2023-5539
  - CVSS Score: N/A
  - Description: A remote code execution risk was identified in the Lesson activity. By default this was only available to teachers and managers.
- Vulnerability: CVE-2023-23923
  - CVSS Score: N/A
  - Description: The vulnerability was found Moodle which exists due to insufficient limitations on the "start page" preference. A remote attacker can set that preference for another user. The vulnerability allows a remote attacker to gain unauthorized access to otherwise restricted functionality.
- Vulnerability: CVE-2023-5551

- CVSS Score: N/A
  - Description: Separate Groups mode restrictions were not honoured in the forum summary report, which would display users from other groups.

- Vulnerability: CVE-2023-5550

  - CVSS Score: N/A
  - Description: In a shared hosting environment that has been misconfigured to allow access to other users' content, a Moodle user who also has direct access to the web server outside of the Moodle webroot could utilise a local file include to achieve remote code execution.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2007-6538

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in ing/blocks/mrbs/code/web/view_entry.php in the MRBS plugin for Moodle allows remote attackers to execute arbitrary SQL commands via the id parameter.

- Vulnerability: CVE-2023-23922

  - CVSS Score: N/A
  - Description: The vulnerability was found Moodle which exists due to insufficient sanitization of user-supplied data in blog search. A remote attacker can trick the victim to follow a specially crafted link and execute arbitrary HTML and script code in user's browser in context of vulnerable website. This flaw allows a remote attacker to perform cross-site scripting (XSS) attacks.

- Vulnerability: CVE-2022-22720

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2023-28329

  - CVSS Score: N/A
  - Description: Insufficient validation of profile field availability condition resulted in an SQL injection risk (by default only available to teachers and managers).

- Vulnerability: CVE-2023-25690

  - CVSS Score: N/A

- Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2010-4208

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the Flash component infrastructure in YUI 2.5.0 through 2.8.1, as used in Bugzilla, Moodle, and other products, allows remote attackers to inject arbitrary web script or HTML via vectors related to uploader/assets/uploader.swf.

- Vulnerability: CVE-2022-37436

  - CVSS Score: N/A
  - Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2024-38477

  - CVSS Score: N/A

- Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-27316

  - CVSS Score: N/A
  - Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

- Vulnerability: CVE-2022-26377

  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2010-4207

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the Flash component infrastructure in YUI 2.4.0 through 2.8.1, as used in Bugzilla, Moodle, and other products, allows remote attackers to inject arbitrary web script or HTML via vectors related to charts/assets/charts.swf.

- Vulnerability: CVE-2023-45802

  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-28614

  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

- Vulnerability: CVE-2006-20001

  - CVSS Score: N/A

- Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- Vulnerability: CVE-2012-3526

  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2024-40898

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2022-28615

  - CVSS Score: 6.4
  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- Vulnerability: CVE-2023-31122

  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2022-36760

  - CVSS Score: N/A
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-22719

– CVSS Score: 5

– Description: A carefully crafted request body can cause a read to a random memory
                 area which could cause the process to crash. This issue affects
                 Apache HTTP Server 2.4.52 and earlier.

11.38 IP Address: 35.185.199.199

- Organization: Google LLC

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 13

- Medium Vulnerabilities: 31

- Low Vulnerabilities: 4

- Total Vulnerabilities: 48

Services Running on IP Address

- Service: OpenSSH

  – Port: 22
  – Version: 8.9p1 Ubuntu-3ubuntu0.10
  – Location:

- Service: Apache httpd

  – Port: 80
  – Version: 2.4.52
  – Location: https://givingtrax.com/

- Service: Apache httpd

  – Port: 443
  – Version: 2.4.52
  – Location: https://www.givingtrax.com/

Vulnerabilities Found

- Vulnerability: CVE-2024-27316

  – CVSS Score: N/A
  – Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

- Vulnerability: CVE-2013-2765

  – CVSS Score: 5
  – Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2022-36760

  – CVSS Score: N/A
  – Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-29404

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2023-27522

  - CVSS Score: N/A
  - Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.Special characters in the origin response header can truncate/split the response forwarded to the client.

- Vulnerability: CVE-2013-4365

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2022-22720

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2022-28330

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2023-31122

  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2024-38476

  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-38477

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-38474

  - CVSS Score: N/A

– Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server
2.4.59 and earlier allows attacker to execute scripts indirectories
permitted by the configuration but not directly reachable by anyURL
or source disclosure of scripts meant to only to be executed as
CGI.Users are recommended to upgrade to version 2.4.60, which fixes
this issue.Some RewriteRules that capture and substitute unsafely
will now fail unless rewrite flag "UnsafeAllow3F" is specified.

• Vulnerability: CVE-2022-22721

– CVSS Score: 5.8
– Description: If LimitXMLRequestBody is set to allow request bodies larger than
350MB (defaults to 1M) on 32 bit systems an integer overflow happens
which later causes out of bounds writes. This issue affects Apache
HTTP Server 2.4.52 and earlier.

• Vulnerability: CVE-2006-20001

– CVSS Score: N/A
– Description: A carefully crafted If: request header can cause a memory read, or
write of a single zero byte, in a pool (heap) memory location beyond
the header value sent. This could cause the process to crash.This
issue affects Apache HTTP Server 2.4.54 and earlier.

• Vulnerability: CVE-2009-0796

– CVSS Score: 2.6
– Description: Cross-site scripting (XSS) vulnerability in Status.pm in
Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the
Apache HTTP Server, when /perl-status is accessible, allows remote
attackers to inject arbitrary web script or HTML via the URI.

• Vulnerability: CVE-2012-3526

– CVSS Score: 5
– Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the
Apache HTTP Server allows remote attackers to cause a denial of
service (server or application crash) via multiple X-Forwarded-For
headers in a request.

• Vulnerability: CVE-2022-31813

– CVSS Score: 7.5
– Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-*
headers to the origin server based on client side Connection
header hop-by-hop mechanism. This may be used to bypass IP based
authentication on the origin server/application.

• Vulnerability: CVE-2012-4001

– CVSS Score: 5
– Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server
does not properly verify its host name, which allows remote attackers
to trigger HTTP requests to arbitrary hosts via unspecified vectors,
as demonstrated by requests to intranet servers.

• Vulnerability: CVE-2022-37436

– CVSS Score: N/A
– Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause
the response headers to be truncated early, resulting in some headers
being incorporated into the response body. If the later headers have
any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2012-4360

  – CVSS Score: 4.3

  – Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2011-1176

  – CVSS Score: 4.3

  – Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2022-23943

  – CVSS Score: 7.5

  – Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

- Vulnerability: CVE-2011-2688

  – CVSS Score: 7.5

  – Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2023-25690

  – CVSS Score: N/A

  – Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2007-4723

  – CVSS Score: 7.5

  – Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2013-0941

- CVSS Score: 2.1
- Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2022-26377

  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2023-45802

  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-28614

  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2024-40898

  – CVSS Score: N/A
  – Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in
                  server/vhost context, allows to potentially leak NTML hashes to
                  a malicious server via SSRF and malicious requests.Users are
                  recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2022-28615

  – CVSS Score: 6.4
  – Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose
                  information due to a read beyond bounds in ap_strcmp_match() when
                  provided with an extremely large input buffer. While no code
                  distributed with the server can be coerced into such a call,
                  third-party modules or lua scripts that use ap_strcmp_match() may
                  hypothetically be affected.

- Vulnerability: CVE-2022-30556

  – CVSS Score: 5
  – Description: Apache HTTP Server 2.4.53 and earlier may return lengths to
                  applications calling r:wsread() that point past the end of the
                  storage allocated for the buffer.

- Vulnerability: CVE-2022-22719

  – CVSS Score: 5
  – Description: A carefully crafted request body can cause a read to a random memory
                  area which could cause the process to crash. This issue affects
                  Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2013-2765

  – CVSS Score: 5
  – Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server
                  allows remote attackers to cause a denial of service (NULL pointer
                  dereference, process crash, and disk consumption) via a POST request
                  with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2022-36760

  – CVSS Score: N/A
  – Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request
                  Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server
                  allows an attacker to smuggle requests to the AJP server it forwards
                  requests to. This issue affects Apache HTTP Server Apache HTTP
                  Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-29404

  – CVSS Score: 5
  – Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a
                  lua script that calls r:parsebody(0) may cause a denial of service
                  due to no default limit on possible input size.

- Vulnerability: CVE-2023-27522

  – CVSS Score: N/A
  – Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via
                  mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30
                  through 2.4.55.Special characters in the origin response header can
                  truncate/split the response forwarded to the client.

- Vulnerability: CVE-2013-4365
  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.
- Vulnerability: CVE-2022-22720
  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling
- Vulnerability: CVE-2022-28330
  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.
- Vulnerability: CVE-2023-31122
  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.
- Vulnerability: CVE-2012-4001
  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.
- Vulnerability: CVE-2024-38476
  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.
- Vulnerability: CVE-2024-27316
  - CVSS Score: N/A
  - Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.
- Vulnerability: CVE-2024-38474
  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.
- Vulnerability: CVE-2022-22721

- CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2006-20001
  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2009-0796
  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2007-3205
  - CVSS Score: 5
  - Description: The parse_str function in (1) PHP, (2) Hardened-PHP, and (3) Suhosin, when called without a second parameter, might allow remote attackers to overwrite arbitrary variables by specifying variable names and values in the string to be parsed. NOTE: it is not clear whether this is a design limitation of the function or a bug in PHP, although it is likely to be regarded as a bug in Hardened-PHP and Suhosin.

- Vulnerability: CVE-2022-31813
  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

- Vulnerability: CVE-2013-2220
  - CVSS Score: 7.5
  - Description: Buffer overflow in the radius_get_vendor_attr function in the Radius extension before 1.2.7 for PHP allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a large Vendor Specific Attributes (VSA) length value.

- Vulnerability: CVE-2022-37436
  - CVSS Score: N/A
  - Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2012-4360
  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2011-1176

  – CVSS Score: 4.3
  – Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2022-23943

  – CVSS Score: 7.5
  – Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

- Vulnerability: CVE-2024-40898

  – CVSS Score: N/A
  – Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2011-2688

  – CVSS Score: 7.5
  – Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2023-25690

  – CVSS Score: N/A
  – Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2007-4723

  – CVSS Score: 7.5
  – Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2013-0941

- CVSS Score: 2.1
- Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2022-26377

  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2023-45802

  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-28614

  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2012-3526

  – CVSS Score: 5
  – Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the
                  Apache HTTP Server allows remote attackers to cause a denial of
                  service (server or application crash) via multiple X-Forwarded-For
                  headers in a request.

- Vulnerability: CVE-2024-38477

  – CVSS Score: N/A
  – Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59
                  and earlier allows an attacker to crash the server via a malicious
                  request.Users are recommended to upgrade to version 2.4.60, which
                  fixes this issue.

- Vulnerability: CVE-2022-28615

  – CVSS Score: 6.4
  – Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose
                  information due to a read beyond bounds in ap_strcmp_match() when
                  provided with an extremely large input buffer. While no code
                  distributed with the server can be coerced into such a call,
                  third-party modules or lua scripts that use ap_strcmp_match() may
                  hypothetically be affected.

- Vulnerability: CVE-2022-30556

  – CVSS Score: 5
  – Description: Apache HTTP Server 2.4.53 and earlier may return lengths to
                  applications calling r:wsread() that point past the end of the
                  storage allocated for the buffer.

- Vulnerability: CVE-2022-22719

  – CVSS Score: 5
  – Description: A carefully crafted request body can cause a read to a random memory
                  area which could cause the process to crash. This issue affects
                  Apache HTTP Server 2.4.52 and earlier.

11.39 IP Address: 34.252.50.82

- Organization: Amazon Data Services Ireland Limited

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 12

- Medium Vulnerabilities: 30

- Low Vulnerabilities: 4

- Total Vulnerabilities: 46

Services Running on IP Address

- Service: Apache httpd

  – Port: 443
  – Version: 2.4.52
  – Location: /

Vulnerabilities Found

- Vulnerability: CVE-2024-27316

  – CVSS Score: N/A
  – Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

- Vulnerability: CVE-2013-2765

  – CVSS Score: 5
  – Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2022-36760

  – CVSS Score: N/A
  – Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-29404

  – CVSS Score: 5
  – Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2023-27522

  – CVSS Score: N/A
  – Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.Special characters in the origin response header can truncate/split the response forwarded to the client.

- Vulnerability: CVE-2013-4365

  – CVSS Score: 7.5

  – Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2022-22720

  – CVSS Score: 7.5

  – Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2022-28330

  – CVSS Score: 5

  – Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2023-31122

  – CVSS Score: N/A

  – Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2024-38476

  – CVSS Score: N/A

  – Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerly to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-38477

  – CVSS Score: N/A

  – Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-38474

  – CVSS Score: N/A

  – Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2022-22721

  – CVSS Score: 5.8

  – Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2006-20001

- CVSS Score: N/A
- Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2009-0796

  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2012-3526

  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2022-31813

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

- Vulnerability: CVE-2012-4001

  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2022-37436

  - CVSS Score: N/A
  - Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2012-4360

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2022-23943

  – CVSS Score: 7.5
  – Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

- Vulnerability: CVE-2011-2688

  – CVSS Score: 7.5
  – Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2023-25690

  – CVSS Score: N/A
  – Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2007-4723

  – CVSS Score: 7.5
  – Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2013-0941

  – CVSS Score: 2.1
  – Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  – CVSS Score: 4.3
  – Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2022-26377

  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2023-45802

  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-28614

  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2024-40898

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2022-28615

  - CVSS Score: 6.4
  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to
                 applications calling r:wsread() that point past the end of the
                 storage allocated for the buffer.

- Vulnerability: CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory
                 area which could cause the process to crash. This issue affects
                 Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2024-27316

  - CVSS Score: N/A
  - Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered
                 in nghttp2 in order to generate an informative HTTP 413 response.
                 If a client does not stop sending headers, this leads to memory
                 exhaustion.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server
                 allows remote attackers to cause a denial of service (NULL pointer
                 dereference, process crash, and disk consumption) via a POST request
                 with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2022-36760

  - CVSS Score: N/A
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request
                 Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server
                 allows an attacker to smuggle requests to the AJP server it forwards
                 requests to. This issue affects Apache HTTP Server Apache HTTP
                 Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-29404

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a
                 lua script that calls r:parsebody(0) may cause a denial of service
                 due to no default limit on possible input size.

- Vulnerability: CVE-2023-27522

  - CVSS Score: N/A
  - Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via
                 mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30
                 through 2.4.55.Special characters in the origin response header can
                 truncate/split the response forwarded to the client.

- Vulnerability: CVE-2013-4365

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function
                 in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache
                 HTTP Server allows remote attackers to have an unspecified impact via
                 unknown vectors.

- Vulnerability: CVE-2022-22720

- CVSS Score: 7.5
- Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- **Vulnerability: CVE-2022-28330**

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- **Vulnerability: CVE-2023-31122**

  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- **Vulnerability: CVE-2024-38476**

  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- **Vulnerability: CVE-2024-38477**

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- **Vulnerability: CVE-2024-38474**

  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- **Vulnerability: CVE-2022-22721**

  - CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- **Vulnerability: CVE-2006-20001**

  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- **Vulnerability: CVE-2009-0796**

  - CVSS Score: 2.6

- Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2012-3526

  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2022-31813

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

- Vulnerability: CVE-2012-4001

  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2022-37436

  - CVSS Score: N/A
  - Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2012-4360

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2022-23943

  - CVSS Score: 7.5
  - Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

- Vulnerability: CVE-2011-2688

    - CVSS Score: 7.5
    - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the
                   mod_authnz_external module 3.2.5 and earlier for the Apache HTTP
                   Server allows remote attackers to execute arbitrary SQL commands
                   via the user field.

- Vulnerability: CVE-2023-25690

    - CVSS Score: N/A
    - Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0
                   through 2.4.55 allow a HTTP Request Smuggling attack.Configurations
                   are affected when mod_proxy is enabled along with some form of
                   RewriteRule or ProxyPassMatch in which a non-specific pattern
                   matches some portion of the user-supplied request-target (URL)
                   data and is then re-inserted into the proxied request-target using
                   variable substitution. For example, something like:RewriteEngine
                   onRewriteRule "/here/(.*)" "http://example.com:8080/elsewhere?$1";
                   [P]ProxyPassReverse /here/ http://example.com:8080/Request
                   splitting/smuggling could result in bypass of access controls in the
                   proxy server, proxying unintended URLs to existing origin servers,
                   and cache poisoning. Users are recommended to update to at least
                   version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2007-4723

    - CVSS Score: 7.5
    - Description: Directory traversal vulnerability in Ragnarok Online Control Panel
                   4.3.4a, when the Apache HTTP Server is used, allows remote attackers
                   to bypass authentication via directory traversal sequences in a URI
                   that ends with the name of a publicly available page, as demonstrated
                   by a "/...../" sequence and an account_manage.php/login.php final
                   component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2013-0941

    - CVSS Score: 2.1
    - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5
                   for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM
                   Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows
                   use an improper encryption algorithm and a weak key for maintaining
                   the stored data of the node secret for the SecurID Authentication
                   API, which allows local users to obtain sensitive information via
                   cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

    - CVSS Score: 4.3
    - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication
                   Agent 7.1 before 7.1.1 for Web for Internet Information Services,
                   and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to
                   inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2022-26377

    - CVSS Score: 5
    - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request
                   Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server
                   allows an attacker to smuggle requests to the AJP server it forwards
                   requests to. This issue affects Apache HTTP Server Apache HTTP
                   Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2023-45802

  – CVSS Score: N/A
  – Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-28614

  – CVSS Score: 5
  – Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

- Vulnerability: CVE-2009-2299

  – CVSS Score: 5
  – Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2024-40898

  – CVSS Score: N/A
  – Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2022-28615

  – CVSS Score: 6.4
  – Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- Vulnerability: CVE-2022-30556

  – CVSS Score: 5
  – Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- Vulnerability: CVE-2022-22719

– CVSS Score: 5

– Description: A carefully crafted request body can cause a read to a random memory
                area which could cause the process to crash. This issue affects
                Apache HTTP Server 2.4.52 and earlier.

11.40 IP Address: 159.149.129.248

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 12

- Medium Vulnerabilities: 30

- Low Vulnerabilities: 4

- Total Vulnerabilities: 46

Services Running on IP Address

- Service: OpenSSH

  – Port: 22
  – Version: 8.9p1 Ubuntu-3ubuntu0.10
  – Location:

- Service: Apache httpd

  – Port: 80
  – Version: 2.4.52
  – Location: /

- Service: Apache httpd

  – Port: 443
  – Version: 2.4.52
  – Location: /

Vulnerabilities Found

- Vulnerability: CVE-2023-25690

  – CVSS Score: N/A
  – Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0
                  through 2.4.55 allow a HTTP Request Smuggling attack.Configurations
                  are affected when mod_proxy is enabled along with some form of
                  RewriteRule or ProxyPassMatch in which a non-specific pattern
                  matches some portion of the user-supplied request-target (URL)
                  data and is then re-inserted into the proxied request-target using
                  variable substitution. For example, something like:RewriteEngine
                  onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1";
                  [P]ProxyPassReverse /here/ http://example.com:8080/Request
                  splitting/smuggling could result in bypass of access controls in the
                  proxy server, proxying unintended URLs to existing origin servers,
                  and cache poisoning. Users are recommended to update to at least
                  version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2022-36760

  – CVSS Score: N/A
  – Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request
                  Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server
                  allows an attacker to smuggle requests to the AJP server it forwards
                  requests to. This issue affects Apache HTTP Server Apache HTTP
                  Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-29404

  – CVSS Score: 5
  – Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2023-27522

  – CVSS Score: N/A
  – Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.Special characters in the origin response header can truncate/split the response forwarded to the client.

- Vulnerability: CVE-2013-4365

  – CVSS Score: 7.5
  – Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2022-22720

  – CVSS Score: 7.5
  – Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2022-28330

  – CVSS Score: 5
  – Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2009-2299

  – CVSS Score: 5
  – Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2024-27316

  – CVSS Score: N/A
  – Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

- Vulnerability: CVE-2023-31122

  – CVSS Score: N/A
  – Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2022-22721

  – CVSS Score: 5.8

- Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

- **Vulnerability: CVE-2006-20001**

  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- **Vulnerability: CVE-2009-0796**

  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- **Vulnerability: CVE-2012-3526**

  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- **Vulnerability: CVE-2022-31813**

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

- **Vulnerability: CVE-2012-4001**

  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- **Vulnerability: CVE-2022-37436**

  - CVSS Score: N/A
  - Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- **Vulnerability: CVE-2012-4360**

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- **Vulnerability: CVE-2011-1176**

  - CVSS Score: 4.3

- Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk
  Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP
  Server does not properly handle certain configuration sections that
  specify NiceValue but not AssignUserID, which might allow remote
  attackers to gain privileges by leveraging the root uid and root gid
  of an mpm-itk process.

- **Vulnerability:** CVE-2022-23943

  - CVSS Score: 7.5
  - Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server
    allows an attacker to overwrite heap memory with possibly attacker
    provided data. This issue affects Apache HTTP Server 2.4 version
    2.4.52 and prior versions.

- **Vulnerability:** CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the
    mod_authnz_external module 3.2.5 and earlier for the Apache HTTP
    Server allows remote attackers to execute arbitrary SQL commands
    via the user field.

- **Vulnerability:** CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server
    allows remote attackers to cause a denial of service (NULL pointer
    dereference, process crash, and disk consumption) via a POST request
    with a large body and a crafted Content-Type header.

- **Vulnerability:** CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel
    4.3.4a, when the Apache HTTP Server is used, allows remote attackers
    to bypass authentication via directory traversal sequences in a URI
    that ends with the name of a publicly available page, as demonstrated
    by a "/...../" sequence and an account_manage.php/login.php final
    component for reaching the protected account_manage.php page.

- **Vulnerability:** CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5
    for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM
    Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows
    use an improper encryption algorithm and a weak key for maintaining
    the stored data of the node secret for the SecurID Authentication
    API, which allows local users to obtain sensitive information via
    cryptographic attacks on this data.

- **Vulnerability:** CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication
    Agent 7.1 before 7.1.1 for Web for Internet Information Services,
    and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to
    inject arbitrary web script or HTML via unspecified vectors.

- **Vulnerability:** CVE-2022-26377

  - CVSS Score: 5

– Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

• Vulnerability: CVE-2023-45802

    – CVSS Score: N/A

    – Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

• Vulnerability: CVE-2022-28614

    – CVSS Score: 5

    – Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

• Vulnerability: CVE-2024-40898

    – CVSS Score: N/A

    – Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

• Vulnerability: CVE-2022-28615

    – CVSS Score: 6.4

    – Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

• Vulnerability: CVE-2022-30556

    – CVSS Score: 5

    – Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

• Vulnerability: CVE-2022-22719

    – CVSS Score: 5

- Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2024-27316

  - CVSS Score: N/A
  - Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2022-36760

  - CVSS Score: N/A
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-29404

  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2023-27522

  - CVSS Score: N/A
  - Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.Special characters in the origin response header can truncate/split the response forwarded to the client.

- Vulnerability: CVE-2013-4365

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2022-22720

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2022-28330

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2023-31122

  – CVSS Score: N/A
  – Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP
                  Server.This issue affects Apache HTTP Server: through 2.4.57.

- Vulnerability: CVE-2024-38476

  – CVSS Score: N/A
  – Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are
                  vulnerably to information disclosure, SSRF or local script execution
                  viabackend applications whose response headers are malicious or
                  exploitable.Users are recommended to upgrade to version 2.4.60, which
                  fixes this issue.

- Vulnerability: CVE-2024-38477

  – CVSS Score: N/A
  – Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59
                  and earlier allows an attacker to crash the server via a malicious
                  request.Users are recommended to upgrade to version 2.4.60, which
                  fixes this issue.

- Vulnerability: CVE-2024-38474

  – CVSS Score: N/A
  – Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server
                  2.4.59 and earlier allows attacker to execute scripts indirectories
                  permitted by the configuration but not directly reachable by anyURL
                  or source disclosure of scripts meant to only to be executed as
                  CGI.Users are recommended to upgrade to version 2.4.60, which fixes
                  this issue.Some RewriteRules that capture and substitute unsafely
                  will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2022-22721

  – CVSS Score: 5.8
  – Description: If LimitXMLRequestBody is set to allow request bodies larger than
                  350MB (defaults to 1M) on 32 bit systems an integer overflow happens
                  which later causes out of bounds writes. This issue affects Apache
                  HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2006-20001

  – CVSS Score: N/A
  – Description: A carefully crafted If: request header can cause a memory read, or
                  write of a single zero byte, in a pool (heap) memory location beyond
                  the header value sent. This could cause the process to crash.This
                  issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2009-0796

  – CVSS Score: 2.6
  – Description: Cross-site scripting (XSS) vulnerability in Status.pm in
                  Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the
                  Apache HTTP Server, when /perl-status is accessible, allows remote
                  attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2012-3526

  – CVSS Score: 5

- Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the
  Apache HTTP Server allows remote attackers to cause a denial of
  service (server or application crash) via multiple X-Forwarded-For
  headers in a request.

- **Vulnerability:** CVE-2022-31813

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-*
    headers to the origin server based on client side Connection
    header hop-by-hop mechanism. This may be used to bypass IP based
    authentication on the origin server/application.

- **Vulnerability:** CVE-2012-4001

  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server
    does not properly verify its host name, which allows remote attackers
    to trigger HTTP requests to arbitrary hosts via unspecified vectors,
    as demonstrated by requests to intranet servers.

- **Vulnerability:** CVE-2022-37436

  - CVSS Score: N/A
  - Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause
    the response headers to be truncated early, resulting in some headers
    being incorporated into the response body. If the later headers have
    any security purpose, they will not be interpreted by the client.

- **Vulnerability:** CVE-2012-4360

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module
    0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote
    attackers to inject arbitrary web script or HTML via unspecified
    vectors.

- **Vulnerability:** CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk
    Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP
    Server does not properly handle certain configuration sections that
    specify NiceValue but not AssignUserID, which might allow remote
    attackers to gain privileges by leveraging the root uid and root gid
    of an mpm-itk process.

- **Vulnerability:** CVE-2022-23943

  - CVSS Score: 7.5
  - Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server
    allows an attacker to overwrite heap memory with possibly attacker
    provided data. This issue affects Apache HTTP Server 2.4 version
    2.4.52 and prior versions.

- **Vulnerability:** CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the
    mod_authnz_external module 3.2.5 and earlier for the Apache HTTP
    Server allows remote attackers to execute arbitrary SQL commands
    via the user field.

- **Vulnerability:** CVE-2023-25690

- CVSS Score: N/A

- Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "ˆ/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- **Vulnerability:** CVE-2007-4723

  - CVSS Score: 7.5

  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- **Vulnerability:** CVE-2013-0941

  - CVSS Score: 2.1

  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- **Vulnerability:** CVE-2013-0942

  - CVSS Score: 4.3

  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- **Vulnerability:** CVE-2022-26377

  - CVSS Score: 5

  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- **Vulnerability:** CVE-2023-45802

  - CVSS Score: N/A

- Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-28614

  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2024-40898

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2022-28615

  - CVSS Score: 6.4
  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- Vulnerability: CVE-2022-30556

  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- Vulnerability: CVE-2022-22719

  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

11.41 IP Address: 159.149.30.3

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 11

- Medium Vulnerabilities: 47

- Low Vulnerabilities: 4

- Total Vulnerabilities: 62

Services Running on IP Address

- Service: Apache httpd

  – Port: 80
  – Version: 2.4.29
  – Location: http://www.matematica.unimi.it

Vulnerabilities Found

- Vulnerability: CVE-2019-0220

  – CVSS Score: 5
  – Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38.
    When the path component of a request URL contains multiple
    consecutive slashes ('/'), directives such as LocationMatch and
    RewriteRule must account for duplicates in regular expressions while
    other aspects of the servers processing will implicitly collapse
    them.

- Vulnerability: CVE-2024-27316

  – CVSS Score: N/A
  – Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered
    in nghttp2 in order to generate an informative HTTP 413 response.
    If a client does not stop sending headers, this leads to memory
    exhaustion.

- Vulnerability: CVE-2011-2688

  – CVSS Score: 7.5
  – Description: SQL injection vulnerability in mysql/mysql-auth.pl in the
    mod_authnz_external module 3.2.5 and earlier for the Apache HTTP
    Server allows remote attackers to execute arbitrary SQL commands
    via the user field.

- Vulnerability: CVE-2013-2765

  – CVSS Score: 5
  – Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server
    allows remote attackers to cause a denial of service (NULL pointer
    dereference, process crash, and disk consumption) via a POST request
    with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2020-1934

  – CVSS Score: 5
  – Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use
    uninitialized memory when proxying to a malicious FTP server.

- Vulnerability: CVE-2018-17189

  – CVSS Score: 5
  – Description: In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 (mod_http2) connections.

- Vulnerability: CVE-2022-36760

  – CVSS Score: N/A
  – Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2020-35452

  – CVSS Score: 6.8
  – Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

- Vulnerability: CVE-2022-29404

  – CVSS Score: 5
  – Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2021-33193

  – CVSS Score: 5
  – Description: A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.

- Vulnerability: CVE-2009-0796

  – CVSS Score: 2.6
  – Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2013-4365

  – CVSS Score: 7.5
  – Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2018-1333

  – CVSS Score: 5

– Description: By specially crafting HTTP/2 requests, workers would be allocated
    60 seconds longer than necessary, leading to worker exhaustion and
    a denial of service. Fixed in Apache HTTP Server 2.4.34 (Affected
    2.4.18-2.4.30,2.4.33).

- Vulnerability: CVE-2022-22720

  – CVSS Score: 7.5
  – Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound
    connection when errors are encountered discarding the request body,
    exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2018-11763

  – CVSS Score: 4.3
  – Description: In Apache HTTP Server 2.4.17 to 2.4.34, by sending continuous, large
    SETTINGS frames a client can occupy a connection, server thread and
    CPU time without any connection timeout coming to effect. This
    affects only HTTP/2 connections. A possible mitigation is to not
    enable the h2 protocol.

- Vulnerability: CVE-2022-28330

  – CVSS Score: 5
  – Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond
    bounds when configured to process requests with the mod_isapi module.

- Vulnerability: CVE-2020-11993

  – CVSS Score: 4.3
  – Description: Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug
    was enabled for the HTTP/2 module and on certain traffic edge
    patterns, logging statements were made on the wrong connection,
    causing concurrent use of memory pools. Configuring the LogLevel of
    mod_http2 above "info" will mitigate this vulnerability for unpatched
    servers.

- Vulnerability: CVE-2021-32791

  – CVSS Score: 4.3
  – Description: mod_auth_openidc is an authentication/authorization module for the
    Apache 2.x HTTP server that functions as an OpenID Connect Relying
    Party, authenticating users against an OpenID Connect Provider.
    In mod_auth_openidc before version 2.4.9, the AES GCM encryption in
    mod_auth_openidc uses a static IV and AAD. It is important to fix
    because this creates a static nonce and since aes-gcm is a stream
    cipher, this can lead to known cryptographic issues, since the same
    key is being reused. From 2.4.9 onwards this has been patched to use
    dynamic values through usage of cjose AES encryption routines.

- Vulnerability: CVE-2021-32792

  – CVSS Score: 4.3
  – Description: mod_auth_openidc is an authentication/authorization module for the
    Apache 2.x HTTP server that functions as an OpenID Connect Relying
    Party, authenticating users against an OpenID Connect Provider. In
    mod_auth_openidc before version 2.4.9, there is an XSS vulnerability
    in when using 'OIDCPreservePost On'.

- Vulnerability: CVE-2023-31122

  – CVSS Score: N/A

- Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

- **Vulnerability:** CVE-2019-9517

  - CVSS Score: 7.8
  - Description: Some HTTP/2 implementations are vulnerable to unconstrained interal data buffering, potentially leading to a denial of service. The attacker opens the HTTP/2 window so the peer can send without constraint; however, they leave the TCP window closed so the peer cannot actually write (many of) the bytes on the wire. The attacker then sends a stream of requests for a large response object. Depending on how the servers queue the responses, this can consume excess memory, CPU, or both.

- **Vulnerability:** CVE-2024-38476

  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- **Vulnerability:** CVE-2024-38477

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- **Vulnerability:** CVE-2024-38474

  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- **Vulnerability:** CVE-2019-0196

  - CVSS Score: 5
  - Description: A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.

- **Vulnerability:** CVE-2019-0211

  - CVSS Score: 7.2
  - Description: In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.

- **Vulnerability:** CVE-2022-22721

- CVSS Score: 5.8
- Description: If LimitXMLRequestBody is set to allow request bodies larger than
  350MB (defaults to 1M) on 32 bit systems an integer overflow happens
  which later causes out of bounds writes. This issue affects Apache
  HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2006-20001

  - CVSS Score: N/A

  - Description: A carefully crafted If: request header can cause a memory read, or
    write of a single zero byte, in a pool (heap) memory location beyond
    the header value sent. This could cause the process to crash.This
    issue affects Apache HTTP Server 2.4.54 and earlier.

- Vulnerability: CVE-2019-10092

  - CVSS Score: 4.3

  - Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting
    issue was reported affecting the mod_proxy error page. An attacker
    could cause the link on the error page to be malformed and instead
    point to a page of their choice. This would only be exploitable
    where a server was set up with proxying enabled but was misconfigured
    in such a way that the Proxy Error page was displayed.

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1

  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5
    for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM
    Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows
    use an improper encryption algorithm and a weak key for maintaining
    the stored data of the node secret for the SecurID Authentication
    API, which allows local users to obtain sensitive information via
    cryptographic attacks on this data.

- Vulnerability: CVE-2019-17567

  - CVSS Score: 5

  - Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel
    configured on an URL that is not necessarily Upgraded by the origin
    server was tunneling the whole connection regardless, thus allowing
    for subsequent requests on the same connection to pass through
    with no HTTP validation, authentication or authorization possibly
    configured.

- Vulnerability: CVE-2017-15715

  - CVSS Score: 6.8

  - Description: In Apache httpd 2.4.0 to 2.4.29, the expression specified in
    <FilesMatch> could match '$' to a newline character in a malicious
    filename, rather than matching only the end of the filename. This
    could be exploited in environments where uploads of some files are
    are externally blocked, but only by matching the trailing portion of
    the filename.

- Vulnerability: CVE-2022-31813

  - CVSS Score: 7.5

  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-*
    headers to the origin server based on client side Connection
    header hop-by-hop mechanism. This may be used to bypass IP based
    authentication on the origin server/application.

- Vulnerability: CVE-2012-4001

  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2019-10098

  - CVSS Score: 5.8
  - Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.

- Vulnerability: CVE-2022-37436

  - CVSS Score: N/A
  - Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- Vulnerability: CVE-2012-4360

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2021-40438

  - CVSS Score: 6.8
  - Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2022-23943

  - CVSS Score: 7.5
  - Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

- Vulnerability: CVE-2020-1927

  - CVSS Score: 5.8
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.

1101

- Vulnerability: CVE-2018-17199

  – CVSS Score: 5
  – Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session
                  checks the session expiry time before decoding the session. This
                  causes session expiry time to be ignored for mod_session_cookie
                  sessions since the expiry time is loaded when the session is decoded.

- Vulnerability: CVE-2017-15710

  – CVSS Score: 5
  – Description: In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to
                  2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig,
                  uses the Accept-Language header value to lookup the right charset
                  encoding when verifying the user's credentials. If the header value
                  is not present in the charset conversion table, a fallback mechanism
                  is used to truncate it to a two characters value to allow a quick
                  retry (for example, 'en-US' is truncated to 'en'). A header value of
                  less than two characters forces an out of bound write of one NUL byte
                  to a memory location that is not part of the string. In the worst
                  case, quite unlikely, the process would crash which could be used as
                  a Denial of Service attack. In the more likely case, this memory is
                  already reserved for future use and the issue has no effect at all.

- Vulnerability: CVE-2018-1301

  – CVSS Score: 4.3
  – Description: A specially crafted request could have crashed the Apache HTTP Server
                  prior to version 2.4.30, due to an out of bound access after a size
                  limit is reached by reading the HTTP header. This vulnerability
                  is considered very hard if not impossible to trigger in non-debug
                  mode (both log and build level), so it is classified as low risk for
                  common server usage.

- Vulnerability: CVE-2018-1302

  – CVSS Score: 4.3
  – Description: When an HTTP/2 stream was destroyed after being handled, the Apache
                  HTTP Server prior to version 2.4.30 could have written a NULL pointer
                  potentially to an already freed memory. The memory pools maintained
                  by the server make this vulnerability hard to trigger in usual
                  configurations, the reporter and the team could not reproduce it
                  outside debug builds, so it is classified as low risk.

- Vulnerability: CVE-2018-1303

  – CVSS Score: 5
  – Description: A specially crafted HTTP request header could have crashed the Apache
                  HTTP Server prior to version 2.4.30 due to an out of bound read while
                  preparing data to be cached in shared memory. It could be used as
                  a Denial of Service attack against users of mod_cache_socache. The
                  vulnerability is considered as low risk since mod_cache_socache is not
                  widely used, mod_cache_disk is not concerned by this vulnerability.

- Vulnerability: CVE-2021-34798

  – CVSS Score: 5
  – Description: Malformed requests may cause the server to dereference a NULL
                  pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2023-25690

– CVSS Score: N/A

– Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

• Vulnerability: CVE-2021-32786

– CVSS Score: 5.8

– Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, `oidc_validate_redirect_url()` does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring `mod_auth_openidc` to only allow redirection whose destination matches a given regular expression.

• Vulnerability: CVE-2021-32785

– CVSS Score: 4.3

– Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache (`OIDCCacheEncrypt off`, `OIDCSessionType server-cache`, `OIDCCacheType redis`), `mod_auth_openidc` wrongly performed argument interpolation before passing Redis requests to `hiredis`, which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the `hiredis` API. As a workaround, this vulnerability can be mitigated by setting `OIDCCacheEncrypt` to `on`, as cache keys are cryptographically hashed before use when this option is enabled.

• Vulnerability: CVE-2020-9490

– CVSS Score: 5

– Description: Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.

- Vulnerability: CVE-2021-44224
  - CVSS Score: 6.4
  - Description: A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).

- Vulnerability: CVE-2007-4723
  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2021-44790
  - CVSS Score: 7.5
  - Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

- Vulnerability: CVE-2013-0942
  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2021-26690
  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service

- Vulnerability: CVE-2021-26691
  - CVSS Score: 7.5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow

- Vulnerability: CVE-2022-26377
  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2023-45802
  - CVSS Score: N/A

- Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that. This was found by the reporter during testing of CVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out. Users are recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-28614

  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

- Vulnerability: CVE-2020-13938

  - CVSS Score: 2.1
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

- Vulnerability: CVE-2019-10081

  - CVSS Score: 5
  - Description: HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example configured with "H2PushResource", could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client.

- Vulnerability: CVE-2018-1283

  - CVSS Score: 3.5
  - Description: In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to forward its session data to CGI applications (SessionEnv on, not the default), a remote user may influence their content by using a "Session" header. This comes from the "HTTP_SESSION" variable name used by mod_session to forward its data to CGIs, since the prefix "HTTP_" is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications.

- Vulnerability: CVE-2019-10082

  - CVSS Score: 6.4
  - Description: In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.

- Vulnerability: CVE-2018-1312

  - CVSS Score: 6.8

- Description: In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

- Vulnerability: CVE-2012-3526
  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2024-40898
  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2019-0217
  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.

- Vulnerability: CVE-2009-2299
  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2021-39275
  - CVSS Score: 7.5
  - Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2022-28615
  - CVSS Score: 6.4
  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- Vulnerability: CVE-2022-30556
  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

- Vulnerability: CVE-2022-22719

  – CVSS Score: 5

  – Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

11.42 IP Address: 159.149.129.224

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 6

- Medium Vulnerabilities: 24

- Low Vulnerabilities: 4

- Total Vulnerabilities: 34

Services Running on IP Address

- Service: Apache httpd

  – Port: 80
  – Version: 2.4.58
  – Location: https://adapt-lab.ricerca.di.unimi.it/

- Service: Apache httpd

  – Port: 443
  – Version: 2.4.58
  – Location: /

Vulnerabilities Found

- Vulnerability: CVE-2009-2299

  – CVSS Score: 5
  – Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module
                 before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before
                 3.1.1-11637, a module for the Apache HTTP Server, allows remote
                 attackers to cause a denial of service (memory consumption) via an
                 HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2024-27316

  – CVSS Score: N/A
  – Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered
                 in nghttp2 in order to generate an informative HTTP 413 response.
                 If a client does not stop sending headers, this leads to memory
                 exhaustion.

- Vulnerability: CVE-2009-1390

  – CVSS Score: 6.8
  – Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2)
                 GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS
                 certificate in the chain is accepted instead of verifying the entire
                 chain, which allows remote attackers to spoof trusted servers via a
                 man-in-the-middle attack.

- Vulnerability: CVE-2013-4365

  – CVSS Score: 7.5
  – Description: Heap-based buffer overflow in the fcgid_header_bucket_read function
                 in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache
                 HTTP Server allows remote attackers to have an unspecified impact via
                 unknown vectors.

- Vulnerability: CVE-2012-3526

  – CVSS Score: 5
  – Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2023-5678

  – CVSS Score: N/A
  – Description: Issue summary: Generating excessively long X9.42 DH keys or checkingexcessively long X9.42 DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_generate_key() togenerate an X9.42 DH key may experience long delays. Likewise, applicationsthat use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check()to check an X9.42 DH key or X9.42 DH parameters may experience long delays.Where the key or parameters that are being checked have been obtained froman untrusted source this may lead to a Denial of Service.While DH_check() performs all the necessary checks (as of CVE-2023-3817),DH_check_pub_key() doesn't make any of these checks, and is thereforevulnerable for excessively large P and Q parameters.Likewise, while DH_generate_key() performs a check for an excessively largeP, it doesn't check for an excessively large Q.An application that calls DH_generate_key() or DH_check_pub_key() andsupplies a key or parameters obtained from an untrusted source could bevulnerable to a Denial of Service attack.DH_generate_key() and DH_check_pub_key() are also called by a number ofother OpenSSL functions. An application calling any of those otherfunctions may similarly be affected. The other functions affected by thisare DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate().Also vulnerable are the OpenSSL pkey command line application when using the"-pubcheck" option, as well as the OpenSSL genpkey command line application.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2009-3766

  – CVSS Score: 6.8
  – Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when OpenSSL is used, does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

- Vulnerability: CVE-2024-38477

  – CVSS Score: N/A
  – Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-38474

  – CVSS Score: N/A

- Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server
    2.4.59 and earlier allows attacker to execute scripts indirectories
    permitted by the configuration but not directly reachable by anyURL
    or source disclosure of scripts meant to only to be executed as
    CGI.Users are recommended to upgrade to version 2.4.60, which fixes
    this issue.Some RewriteRules that capture and substitute unsafely
    will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2009-3765

    - CVSS Score: 6.8
    - Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does
        not properly handle a '\{}0' character in a domain name in the
        subject's Common Name (CN) field of an X.509 certificate, which
        allows man-in-the-middle attackers to spoof arbitrary SSL servers via
        a crafted certificate issued by a legitimate Certification Authority,
        a related issue to CVE-2009-2408.

- Vulnerability: CVE-2019-0190

    - CVSS Score: 5
    - Description: A bug exists in the way mod_ssl handled client renegotiations. A
        remote attacker could send a carefully crafted request that would
        cause mod_ssl to enter a loop leading to a denial of service. This
        bug can be only triggered with Apache HTTP Server version 2.4.37
        when using OpenSSL version 1.1.1 or later, due to an interaction in
        changes to handling of renegotiation attempts.

- Vulnerability: CVE-2009-0796

    - CVSS Score: 2.6
    - Description: Cross-site scripting (XSS) vulnerability in Status.pm in
        Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the
        Apache HTTP Server, when /perl-status is accessible, allows remote
        attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2024-0727

    - CVSS Score: N/A
    - Description: Issue summary: Processing a maliciously formatted PKCS12 file
        may lead OpenSSLto crash leading to a potential Denial of Service
        attackImpact summary: Applications loading files in the PKCS12
        format from untrustedsources might terminate abruptly.A file in
        PKCS12 format can contain certificates and keys and may come from
        anuntrusted source. The PKCS12 specification allows certain fields
        to be NULL, butOpenSSL does not correctly check for this case.
        This can lead to a NULL pointerdereference that results in OpenSSL
        crashing. If an application processes PKCS12files from an untrusted
        source using the OpenSSL APIs then that application willbe vulnerable
        to this issue.OpenSSL APIs that are vulnerable to this are:
        PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(),
        PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a
        similar issue in SMIME_write_PKCS7(). However since thisfunction
        is related to writing data we do not consider it security
        significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected
        by this issue.

- Vulnerability: CVE-2012-4001

    - CVSS Score: 5

- Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2012-4360

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2023-3817

  - CVSS Score: N/A
  - Description: Issue summary: Checking excessively long DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH key or DH parameters may experience longdelays. Where the key or parameters that are being checked have been obtainedfrom an untrusted source this may lead to a Denial of Service.The function DH_check() performs various checks on DH parameters. After fixingCVE-2023-3446 it was discovered that a large q parameter value can also triggeran overly long computation during some of these checks. A correct q value,if present, cannot be larger than the modulus p parameter, thus it isunnecessary to perform these checks if q is larger than p.An application that calls DH_check() and supplies a key or parameters obtainedfrom an untrusted source could be vulnerable to a Denial of Service attack.The function DH_check() is itself called by a number of other OpenSSL functions.An application calling any of those other functions may similarly be affected.The other functions affected by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable are the OpenSSL dhparam and pkeyparam command line applicationswhen using the "-check" option.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2023-4807

  - CVSS Score: N/A

- Description: Issue summary: The POLY1305 MAC (message authentication code) implementationcontains a bug that might corrupt the internal state of applications on theWindows 64 platform when running on newer X86_64 processors supporting theAVX512-IFMA instructions.Impact summary: If in an application that uses the OpenSSL library an attackercan influence whether the POLY1305 MAC algorithm is used, the applicationstate might be corrupted with various application dependent consequences.The POLY1305 MAC (message authentication code) implementation in OpenSSL doesnot save the contents of non-volatile XMM registers on Windows 64 platformwhen calculating the MAC of data larger than 64 bytes. Before returning tothe caller all the XMM registers are set to zero rather than restoring theirprevious content. The vulnerable code is used only on newer x86_64 processorssupporting the AVX512-IFMA instructions.The consequences of this kind of internal application state corruption canbe various – from no consequences, if the calling application does notdepend on the contents of non-volatile XMM registers at all, to the worstconsequences, where the attacker could get complete control of the applicationprocess. However given the contents of the registers are just zeroized sothe attacker cannot put arbitrary values inside, the most likely consequence,if any, would be an incorrect result of some application dependentcalculations or a crash leading to a denial of service.The POLY1305 MAC algorithm is most frequently used as part of theCHACHA20-POLY1305 AEAD (authenticated encryption with associated data)algorithm. The most common usage of this AEAD cipher is with TLS protocolversions 1.2 and 1.3 and a malicious client can influence whether this AEADcipher is used by the server. This implies that server applications usingOpenSSL can be potentially impacted. However we are currently not aware ofany concrete application that would be affected by this issue therefore weconsider this a Low severity security issue.As a workaround the AVX512-IFMA instructions support can be disabled atruntime by setting the environment variable OPENSSL_ia32cap: OPENSSL_ia32cap=:~0x200000The FIPS provider is not affected by this issue.
- Vulnerability: CVE-2023-6129
  - CVSS Score: N/A

– Description: Issue summary: The POLY1305 MAC (message authentication code)
                 implementationcontains a bug that might corrupt the internal
                 state of applications runningon PowerPC CPU based platforms if the
                 CPU provides vector instructions.Impact summary: If an attacker
                 can influence whether the POLY1305 MACalgorithm is used, the
                 application state might be corrupted with variousapplication
                 dependent consequences.The POLY1305 MAC (message authentication
                 code) implementation in OpenSSL forPowerPC CPUs restores the contents
                 of vector registers in a different orderthan they are saved. Thus
                 the contents of some of these vector registersare corrupted when
                 returning to the caller. The vulnerable code is used onlyon newer
                 PowerPC processors supporting the PowerISA 2.07 instructions.The
                 consequences of this kind of internal application state corruption
                 canbe various – from no consequences, if the calling application
                 does notdepend on the contents of non-volatile XMM registers
                 at all, to the worstconsequences, where the attacker could get
                 complete control of the applicationprocess. However unless the
                 compiler uses the vector registers for storingpointers, the most
                 likely consequence, if any, would be an incorrect resultof some
                 application dependent calculations or a crash leading to a denial
                 ofservice.The POLY1305 MAC algorithm is most frequently used as
                 part of theCHACHA20-POLY1305 AEAD (authenticated encryption with
                 associated data)algorithm. The most common usage of this AEAD cipher
                 is with TLS protocolversions 1.2 and 1.3. If this cipher is enabled
                 on the server a maliciousclient can influence whether this AEAD
                 cipher is used. This implies thatTLS server applications using
                 OpenSSL can be potentially impacted. Howeverwe are currently not
                 aware of any concrete application that would be affectedby this issue
                 therefore we consider this a Low severity security issue.

• Vulnerability: CVE-2013-2765

   – CVSS Score: 5
   – Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server
                 allows remote attackers to cause a denial of service (NULL pointer
                 dereference, process crash, and disk consumption) via a POST request
                 with a large body and a crafted Content-Type header.

• Vulnerability: CVE-2011-2688

   – CVSS Score: 7.5
   – Description: SQL injection vulnerability in mysql/mysql-auth.pl in the
                 mod_authnz_external module 3.2.5 and earlier for the Apache HTTP
                 Server allows remote attackers to execute arbitrary SQL commands
                 via the user field.

• Vulnerability: CVE-2009-3767

   – CVSS Score: 4.3
   – Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other
                 versions, when OpenSSL is used, does not properly handle a '\{}0'
                 character in a domain name in the subject's Common Name (CN) field
                 of an X.509 certificate, which allows man-in-the-middle attackers
                 to spoof arbitrary SSL servers via a crafted certificate issued by a
                 legitimate Certification Authority, a related issue to CVE-2009-2408.

• Vulnerability: CVE-2007-4723

   – CVSS Score: 7.5

- Description: Directory traversal vulnerability in Ragnarok Online Control Panel
  4.3.4a, when the Apache HTTP Server is used, allows remote attackers
  to bypass authentication via directory traversal sequences in a URI
  that ends with the name of a publicly available page, as demonstrated
  by a "/...../" sequence and an account_manage.php/login.php final
  component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5
    for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM
    Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows
    use an improper encryption algorithm and a weak key for maintaining
    the stored data of the node secret for the SecurID Authentication
    API, which allows local users to obtain sensitive information via
    cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication
    Agent 7.1 before 7.1.1 for Web for Internet Information Services,
    and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to
    inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2024-38476

  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are
    vulnerably to information disclosure, SSRF or local script execution
    viabackend applications whose response headers are malicious or
    exploitable.Users are recommended to upgrade to version 2.4.60, which
    fixes this issue.

- Vulnerability: CVE-2024-40898

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in
    server/vhost context, allows to potentially leak NTML hashes to
    a malicious server via SSRF and malicious requests.Users are
    recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2023-2975

  - CVSS Score: N/A
  - Description: Issue summary: The AES-SIV cipher implementation contains a bug
    that causesit to ignore empty associated data entries which are
    unauthenticated asa consequence.Impact summary: Applications that
    use the AES-SIV algorithm and want toauthenticate empty data entries
    as associated data can be mislead by removingadding or reordering
    such empty entries as these are ignored by the OpenSSLimplementation.
    We are currently unaware of any such applications.The AES-SIV
    algorithm allows for authentication of multiple associateddata
    entries along with the encryption. To authenticate empty data
    theapplication has to call EVP_EncryptUpdate() (or EVP_CipherUpdate())
    withNULL pointer as the output buffer and 0 as the input buffer
    length.The AES-SIV implementation in OpenSSL just returns success for
    such a callinstead of performing the associated data authentication
    operation.The empty data thus will not be authenticated.As this issue
    does not affect non-empty associated data authentication andwe expect
    it to be rare for an application to use empty associated dataentries
    this is qualified as Low severity issue.

- Vulnerability: CVE-2023-5363
  - CVSS Score: N/A
  - Description: Issue summary: A bug has been identified in the processing of key andinitialisation vector (IV) lengths. This can lead to potential truncationor overruns during the initialisation of some symmetric ciphers.Impact summary: A truncation in the IV can result in non-uniqueness,which could result in loss of confidentiality for some cipher modes.When calling EVP_EncryptInit_ex2(), EVP_DecryptInit_ex2() orEVP_CipherInit_ex2() the provided OSSL_PARAM array is processed afterthe key and IV have been established. Any alterations to the key length,via the "keylen" parameter or the IV length, via the "ivlen" parameter,within the OSSL_PARAM array will not take effect as intended, potentiallycausing truncation or overreading of these values. The following ciphersand cipher modes are impacted: RC2, RC4, RC5, CCM, GCM and OCB.For the CCM, GCM and OCB cipher modes, truncation of the IV can result inloss of confidentiality. For example, when following NIST's SP 800-38Dsection 8.2.1 guidance for constructing a deterministic IV for AES inGCM mode, truncation of the counter portion could lead to IV reuse.Both truncations and overruns of the key and overruns of the IV willproduce incorrect results and could, in some cases, trigger a memoryexception. However, these issues are not currently assessed as securitycritical.Changing the key and/or IV lengths is not considered to be a common operationand the vulnerable API was recently introduced. Furthermore it is likely thatapplication developers will have spotted this problem during testing sincedecryption would fail unless both peers in the communication were similarlyvulnerable. For these reasons we expect the probability of an application beingvulnerable to this to be quite low. However if an application is vulnerable thenthis issue is considered very serious. For these reasons we have assessed thisissue as Moderate severity overall.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this becausethe issue lies outside of the FIPS provider boundary.OpenSSL 3.1 and 3.0 are vulnerable to this issue.
- Vulnerability: CVE-2009-2299
  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.
- Vulnerability: CVE-2024-27316
  - CVSS Score: N/A
  - Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.
- Vulnerability: CVE-2009-1390
  - CVSS Score: 6.8
  - Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2) GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS certificate in the chain is accepted instead of verifying the entire chain, which allows remote attackers to spoof trusted servers via a man-in-the-middle attack.

- Vulnerability: CVE-2013-4365

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2012-3526

  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2023-5678

  - CVSS Score: N/A
  - Description: Issue summary: Generating excessively long X9.42 DH keys or checkingexcessively long X9.42 DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_generate_key() togenerate an X9.42 DH key may experience long delays. Likewise, applicationsthat use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check()to check an X9.42 DH key or X9.42 DH parameters may experience long delays.Where the key or parameters that are being checked have been obtained froman untrusted source this may lead to a Denial of Service.While DH_check() performs all the necessary checks (as of CVE-2023-3817),DH_check_pub_key() doesn't make any of these checks, and is thereforevulnerable for excessively large P and Q parameters.Likewise, while DH_generate_key() performs a check for an excessively largeP, it doesn't check for an excessively large Q.An application that calls DH_generate_key() or DH_check_pub_key() andsupplies a key or parameters obtained from an untrusted source could bevulnerable to a Denial of Service attack.DH_generate_key() and DH_check_pub_key() are also called by a number ofother OpenSSL functions. An application calling any of those otherfunctions may similarly be affected. The other functions affected by thisare DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate().Also vulnerable are the OpenSSL pkey command line application when using the"-pubcheck" option, as well as the OpenSSL genpkey command line application.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2009-3766

  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when OpenSSL is used, does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

- Vulnerability: CVE-2024-38477

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-38474

    – CVSS Score: N/A

    – Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server
      2.4.59 and earlier allows attacker to execute scripts indirectories
      permitted by the configuration but not directly reachable by anyURL
      or source disclosure of scripts meant to only to be executed as
      CGI.Users are recommended to upgrade to version 2.4.60, which fixes
      this issue.Some RewriteRules that capture and substitute unsafely
      will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2009-3765

    – CVSS Score: 6.8

    – Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does
      not properly handle a '\{}0' character in a domain name in the
      subject's Common Name (CN) field of an X.509 certificate, which
      allows man-in-the-middle attackers to spoof arbitrary SSL servers via
      a crafted certificate issued by a legitimate Certification Authority,
      a related issue to CVE-2009-2408.

- Vulnerability: CVE-2019-0190

    – CVSS Score: 5

    – Description: A bug exists in the way mod_ssl handled client renegotiations. A
      remote attacker could send a carefully crafted request that would
      cause mod_ssl to enter a loop leading to a denial of service. This
      bug can be only triggered with Apache HTTP Server version 2.4.37
      when using OpenSSL version 1.1.1 or later, due to an interaction in
      changes to handling of renegotiation attempts.

- Vulnerability: CVE-2009-0796

    – CVSS Score: 2.6

    – Description: Cross-site scripting (XSS) vulnerability in Status.pm in
      Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the
      Apache HTTP Server, when /perl-status is accessible, allows remote
      attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2024-0727

    – CVSS Score: N/A

    – Description: Issue summary: Processing a maliciously formatted PKCS12 file
      may lead OpenSSLto crash leading to a potential Denial of Service
      attackImpact summary: Applications loading files in the PKCS12
      format from untrustedsources might terminate abruptly.A file in
      PKCS12 format can contain certificates and keys and may come from
      anuntrusted source. The PKCS12 specification allows certain fields
      to be NULL, butOpenSSL does not correctly check for this case.
      This can lead to a NULL pointerdereference that results in OpenSSL
      crashing. If an application processes PKCS12files from an untrusted
      source using the OpenSSL APIs then that application willbe vulnerable
      to this issue.OpenSSL APIs that are vulnerable to this are:
      PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(),
      PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a
      similar issue in SMIME_write_PKCS7(). However since thisfunction
      is related to writing data we do not consider it security
      significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected
      by this issue.

- Vulnerability: CVE-2012-4001

- CVSS Score: 5
- Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2012-4360

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2023-3817

  - CVSS Score: N/A
  - Description: Issue summary: Checking excessively long DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH key or DH parameters may experience longdelays. Where the key or parameters that are being checked have been obtainedfrom an untrusted source this may lead to a Denial of Service.The function DH_check() performs various checks on DH parameters. After fixingCVE-2023-3446 it was discovered that a large q parameter value can also triggeran overly long computation during some of these checks. A correct q value,if present, cannot be larger than the modulus p parameter, thus it isunnecessary to perform these checks if q is larger than p.An application that calls DH_check() and supplies a key or parameters obtainedfrom an untrusted source could be vulnerable to a Denial of Service attack.The function DH_check() is itself called by a number of other OpenSSL functions.An application calling any of those other functions may similarly be affected.The other functions affected by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable are the OpenSSL dhparam and pkeyparam command line applicationswhen using the "-check" option.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

- Vulnerability: CVE-2023-4807

  - CVSS Score: N/A

- Description: Issue summary: The POLY1305 MAC (message authentication code) implementationcontains a bug that might corrupt the internal state of applications on theWindows 64 platform when running on newer X86_64 processors supporting theAVX512-IFMA instructions.Impact summary: If in an application that uses the OpenSSL library an attackercan influence whether the POLY1305 MAC algorithm is used, the applicationstate might be corrupted with various application dependent consequences.The POLY1305 MAC (message authentication code) implementation in OpenSSL doesnot save the contents of non-volatile XMM registers on Windows 64 platformwhen calculating the MAC of data larger than 64 bytes. Before returning tothe caller all the XMM registers are set to zero rather than restoring theirprevious content. The vulnerable code is used only on newer x86_64 processorssupporting the AVX512-IFMA instructions.The consequences of this kind of internal application state corruption canbe various – from no consequences, if the calling application does notdepend on the contents of non-volatile XMM registers at all, to the worstconsequences, where the attacker could get complete control of the applicationprocess. However given the contents of the registers are just zeroized sothe attacker cannot put arbitrary values inside, the most likely consequence,if any, would be an incorrect result of some application dependentcalculations or a crash leading to a denial of service.The POLY1305 MAC algorithm is most frequently used as part of theCHACHA20-POLY1305 AEAD (authenticated encryption with associated data)algorithm. The most common usage of this AEAD cipher is with TLS protocolversions 1.2 and 1.3 and a malicious client can influence whether this AEADcipher is used by the server. This implies that server applications usingOpenSSL can be potentially impacted. However we are currently not aware ofany concrete application that would be affected by this issue therefore weconsider this a Low severity security issue.As a workaround the AVX512-IFMA instructions support can be disabled atruntime by setting the environment variable OPENSSL_ia32cap: OPENSSL_ia32cap=:~0x200000The FIPS provider is not affected by this issue.
- Vulnerability: CVE-2023-6129
  - CVSS Score: N/A

— Description: Issue summary: The POLY1305 MAC (message authentication code)
implementationcontains a bug that might corrupt the internal
state of applications runningon PowerPC CPU based platforms if the
CPU provides vector instructions.Impact summary: If an attacker
can influence whether the POLY1305 MACalgorithm is used, the
application state might be corrupted with variousapplication
dependent consequences.The POLY1305 MAC (message authentication
code) implementation in OpenSSL forPowerPC CPUs restores the contents
of vector registers in a different orderthan they are saved. Thus
the contents of some of these vector registersare corrupted when
returning to the caller. The vulnerable code is used onlyon newer
PowerPC processors supporting the PowerISA 2.07 instructions.The
consequences of this kind of internal application state corruption
canbe various – from no consequences, if the calling application
does notdepend on the contents of non-volatile XMM registers
at all, to the worstconsequences, where the attacker could get
complete control of the applicationprocess. However unless the
compiler uses the vector registers for storingpointers, the most
likely consequence, if any, would be an incorrect resultof some
application dependent calculations or a crash leading to a denial
ofservice.The POLY1305 MAC algorithm is most frequently used as
part of theCHACHA20-POLY1305 AEAD (authenticated encryption with
associated data)algorithm. The most common usage of this AEAD cipher
is with TLS protocolversions 1.2 and 1.3. If this cipher is enabled
on the server a maliciousclient can influence whether this AEAD
cipher is used. This implies thatTLS server applications using
OpenSSL can be potentially impacted. Howeverwe are currently not
aware of any concrete application that would be affectedby this issue
therefore we consider this a Low severity security issue.

- Vulnerability: CVE-2013-2765

  — CVSS Score: 5
  — Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server
allows remote attackers to cause a denial of service (NULL pointer
dereference, process crash, and disk consumption) via a POST request
with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2011-2688

  — CVSS Score: 7.5
  — Description: SQL injection vulnerability in mysql/mysql-auth.pl in the
mod_authnz_external module 3.2.5 and earlier for the Apache HTTP
Server allows remote attackers to execute arbitrary SQL commands
via the user field.

- Vulnerability: CVE-2009-3767

  — CVSS Score: 4.3
  — Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other
versions, when OpenSSL is used, does not properly handle a '\{}0'
character in a domain name in the subject's Common Name (CN) field
of an X.509 certificate, which allows man-in-the-middle attackers
to spoof arbitrary SSL servers via a crafted certificate issued by a
legitimate Certification Authority, a related issue to CVE-2009-2408.

- Vulnerability: CVE-2007-4723

  — CVSS Score: 7.5

- Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2024-38476

  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-40898

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2023-2975

  - CVSS Score: N/A
  - Description: Issue summary: The AES-SIV cipher implementation contains a bug that causesit to ignore empty associated data entries which are unauthenticated asa consequence.Impact summary: Applications that use the AES-SIV algorithm and want toauthenticate empty data entries as associated data can be mislead by removingadding or reordering such empty entries as these are ignored by the OpenSSLimplementation. We are currently unaware of any such applications.The AES-SIV algorithm allows for authentication of multiple associateddata entries along with the encryption. To authenticate empty data theapplication has to call EVP_EncryptUpdate() (or EVP_CipherUpdate()) withNULL pointer as the output buffer and 0 as the input buffer length.The AES-SIV implementation in OpenSSL just returns success for such a callinstead of performing the associated data authentication operation.The empty data thus will not be authenticated.As this issue does not affect non-empty associated data authentication andwe expect it to be rare for an application to use empty associated dataentries this is qualified as Low severity issue.

- Vulnerability: CVE-2023-5363

  – CVSS Score: N/A

  – Description: Issue summary: A bug has been identified in the processing of key andinitialisation vector (IV) lengths. This can lead to potential truncationor overruns during the initialisation of some symmetric ciphers.Impact summary: A truncation in the IV can result in non-uniqueness,which could result in loss of confidentiality for some cipher modes.When calling EVP_EncryptInit_ex2(), EVP_DecryptInit_ex2() orEVP_CipherInit_ex2() the provided OSSL_PARAM array is processed afterthe key and IV have been established. Any alterations to the key length,via the "keylen" parameter or the IV length, via the "ivlen" parameter,within the OSSL_PARAM array will not take effect as intended, potentiallycausing truncation or overreading of these values. The following ciphersand cipher modes are impacted: RC2, RC4, RC5, CCM, GCM and OCB.For the CCM, GCM and OCB cipher modes, truncation of the IV can result inloss of confidentiality. For example, when following NIST's SP 800-38Dsection 8.2.1 guidance for constructing a deterministic IV for AES inGCM mode, truncation of the counter portion could lead to IV reuse.Both truncations and overruns of the key and overruns of the IV willproduce incorrect results and could, in some cases, trigger a memoryexception. However, these issues are not currently assessed as securitycritical.Changing the key and/or IV lengths is not considered to be a common operationand the vulnerable API was recently introduced. Furthermore it is likely thatapplication developers will have spotted this problem during testing sincedecryption would fail unless both peers in the communication were similarlyvulnerable. For these reasons we expect the probability of an application beingvulnerable to this to be quite low. However if an application is vulnerable thenthis issue is considered very serious. For these reasons we have assessed thisissue as Moderate severity overall.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by becausethe issue lies outside of the FIPS provider boundary.OpenSSL 3.1 and 3.0 are vulnerable to this issue.

11.43 IP Address: 159.149.147.114

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 6

- Medium Vulnerabilities: 15

- Low Vulnerabilities: 2

- Total Vulnerabilities: 23

Services Running on IP Address

- Service: Apache httpd

  – Port: 443
  – Version: 2.4.52
  – Location: /

Vulnerabilities Found

- Vulnerability: CVE-2024-27316

  – CVSS Score: N/A
  – Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

- Vulnerability: CVE-2013-2765

  – CVSS Score: 5
  – Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2022-36760

  – CVSS Score: N/A
  – Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-29404

  – CVSS Score: 5
  – Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

- Vulnerability: CVE-2023-27522

  – CVSS Score: N/A
  – Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.Special characters in the origin response header can truncate/split the response forwarded to the client.

- Vulnerability: CVE-2013-4365
  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.
- Vulnerability: CVE-2022-22720
  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling
- Vulnerability: CVE-2022-28330
  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.
- Vulnerability: CVE-2023-31122
  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.
- Vulnerability: CVE-2024-38476
  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.
- Vulnerability: CVE-2024-38477
  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.
- Vulnerability: CVE-2024-38474
  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.
- Vulnerability: CVE-2022-22721
  - CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.
- Vulnerability: CVE-2006-20001

- CVSS Score: N/A
- Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.

- **Vulnerability:** CVE-2009-0796

  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- **Vulnerability:** CVE-2012-3526

  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- **Vulnerability:** CVE-2022-31813

  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

- **Vulnerability:** CVE-2012-4001

  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- **Vulnerability:** CVE-2022-37436

  - CVSS Score: N/A
  - Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

- **Vulnerability:** CVE-2012-4360

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- **Vulnerability:** CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2022-23943

  - CVSS Score: 7.5
  - Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server
    allows an attacker to overwrite heap memory with possibly attacker
    provided data. This issue affects Apache HTTP Server 2.4 version
    2.4.52 and prior versions.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the
    mod_authnz_external module 3.2.5 and earlier for the Apache HTTP
    Server allows remote attackers to execute arbitrary SQL commands
    via the user field.

- Vulnerability: CVE-2023-25690

  - CVSS Score: N/A
  - Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0
    through 2.4.55 allow a HTTP Request Smuggling attack.Configurations
    are affected when mod_proxy is enabled along with some form of
    RewriteRule or ProxyPassMatch in which a non-specific pattern
    matches some portion of the user-supplied request-target (URL)
    data and is then re-inserted into the proxied request-target using
    variable substitution. For example, something like:RewriteEngine
    onRewriteRule "/here/(.*)" "http://example.com:8080/elsewhere?$1";
    [P]ProxyPassReverse /here/ http://example.com:8080/Request
    splitting/smuggling could result in bypass of access controls in the
    proxy server, proxying unintended URLs to existing origin servers,
    and cache poisoning. Users are recommended to update to at least
    version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel
    4.3.4a, when the Apache HTTP Server is used, allows remote attackers
    to bypass authentication via directory traversal sequences in a URI
    that ends with the name of a publicly available page, as demonstrated
    by a "/...../" sequence and an account_manage.php/login.php final
    component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5
    for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM
    Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows
    use an improper encryption algorithm and a weak key for maintaining
    the stored data of the node secret for the SecurID Authentication
    API, which allows local users to obtain sensitive information via
    cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication
    Agent 7.1 before 7.1.1 for Web for Internet Information Services,
    and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to
    inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2022-26377

  – CVSS Score: 5

  – Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

- Vulnerability: CVE-2023-45802

  – CVSS Score: N/A

  – Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2022-28614

  – CVSS Score: 5

  – Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

- Vulnerability: CVE-2009-2299

  – CVSS Score: 5

  – Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2024-40898

  – CVSS Score: N/A

  – Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2022-28615

  – CVSS Score: 6.4

  – Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

- Vulnerability: CVE-2022-30556

  – CVSS Score: 5
  – Description: Apache HTTP Server 2.4.53 and earlier may return lengths to
                  applications calling r:wsread() that point past the end of the
                  storage allocated for the buffer.

- Vulnerability: CVE-2022-22719

  – CVSS Score: 5
  – Description: A carefully crafted request body can cause a read to a random memory
                  area which could cause the process to crash. This issue affects
                  Apache HTTP Server 2.4.52 and earlier.

11.44   IP Address: 159.149.45.8

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 6

- Medium Vulnerabilities: 14

- Low Vulnerabilities: 4

- Total Vulnerabilities: 24

Services Running on IP Address

- Service: Apache httpd

    - Port: 80
    - Version: 2.4.59
    - Location: https://159.149.45.8/

- Service: Apache httpd

    - Port: 443
    - Version: 2.4.59
    - Location: /

Vulnerabilities Found

- Vulnerability: CVE-2013-0941

    - CVSS Score: 2.1
    - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5
                    for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM
                    Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows
                    use an improper encryption algorithm and a weak key for maintaining
                    the stored data of the node secret for the SecurID Authentication
                    API, which allows local users to obtain sensitive information via
                    cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

    - CVSS Score: 4.3
    - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication
                    Agent 7.1 before 7.1.1 for Web for Internet Information Services,
                    and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to
                    inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2012-4001

    - CVSS Score: 5
    - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server
                    does not properly verify its host name, which allows remote attackers
                    to trigger HTTP requests to arbitrary hosts via unspecified vectors,
                    as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2024-38476

    - CVSS Score: N/A

- Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-38477

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-38474

  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2024-40898

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2009-0796

  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5

- Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2013-4365

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2012-3526

  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2012-4360

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3

– Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2012-4001

  – CVSS Score: 5
  – Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2024-38476

  – CVSS Score: N/A
  – Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-38477

  – CVSS Score: N/A
  – Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-38474

  – CVSS Score: N/A
  – Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2024-40898

  – CVSS Score: N/A
  – Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2011-1176

  – CVSS Score: 4.3
  – Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2011-2688

  – CVSS Score: 7.5

– Description: SQL injection vulnerability in mysql/mysql-auth.pl in the
mod_authnz_external module 3.2.5 and earlier for the Apache HTTP
Server allows remote attackers to execute arbitrary SQL commands
via the user field.

- Vulnerability: CVE-2009-0796

  – CVSS Score: 2.6

  – Description: Cross-site scripting (XSS) vulnerability in Status.pm in
Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the
Apache HTTP Server, when /perl-status is accessible, allows remote
attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2009-2299

  – CVSS Score: 5

  – Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module
before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before
3.1.1-11637, a module for the Apache HTTP Server, allows remote
attackers to cause a denial of service (memory consumption) via an
HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2007-4723

  – CVSS Score: 7.5

  – Description: Directory traversal vulnerability in Ragnarok Online Control Panel
4.3.4a, when the Apache HTTP Server is used, allows remote attackers
to bypass authentication via directory traversal sequences in a URI
that ends with the name of a publicly available page, as demonstrated
by a "/...../" sequence and an account_manage.php/login.php final
component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2013-2765

  – CVSS Score: 5

  – Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server
allows remote attackers to cause a denial of service (NULL pointer
dereference, process crash, and disk consumption) via a POST request
with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2013-4365

  – CVSS Score: 7.5

  – Description: Heap-based buffer overflow in the fcgid_header_bucket_read function
in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache
HTTP Server allows remote attackers to have an unspecified impact via
unknown vectors.

- Vulnerability: CVE-2012-3526

  – CVSS Score: 5

  – Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the
Apache HTTP Server allows remote attackers to cause a denial of
service (server or application crash) via multiple X-Forwarded-For
headers in a request.

- Vulnerability: CVE-2012-4360

  – CVSS Score: 4.3

  – Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module
0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote
attackers to inject arbitrary web script or HTML via unspecified
vectors.

11.45   IP Address: 159.149.30.18

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 6

- Medium Vulnerabilities: 14

- Low Vulnerabilities: 4

- Total Vulnerabilities: 24

Services Running on IP Address

- Service: OpenSSH

    – Port: 22
    – Version: 9.6p1 Ubuntu 3ubuntu13.4
    – Location:

- Service: Apache httpd

    – Port: 80
    – Version: 2.4.58
    – Location: /

- Service: Apache httpd

    – Port: 443
    – Version: 2.4.58
    – Location: /

Vulnerabilities Found

- Vulnerability: CVE-2013-0941

    – CVSS Score: 2.1
    – Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5
        for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM
        Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows
        use an improper encryption algorithm and a weak key for maintaining
        the stored data of the node secret for the SecurID Authentication
        API, which allows local users to obtain sensitive information via
        cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

    – CVSS Score: 4.3
    – Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication
        Agent 7.1 before 7.1.1 for Web for Internet Information Services,
        and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to
        inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2012-4001

    – CVSS Score: 5
    – Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server
        does not properly verify its host name, which allows remote attackers
        to trigger HTTP requests to arbitrary hosts via unspecified vectors,
        as demonstrated by requests to intranet servers.

1134

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2024-38476

  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-38477

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- Vulnerability: CVE-2024-38474

  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- Vulnerability: CVE-2024-40898

  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2009-0796

- CVSS Score: 2.6
- Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2024-27316

  - CVSS Score: N/A
  - Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

- Vulnerability: CVE-2013-4365

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2012-3526

  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2012-4360

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1

- Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- **Vulnerability: CVE-2013-0942**

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- **Vulnerability: CVE-2012-4001**

  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- **Vulnerability: CVE-2013-2765**

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- **Vulnerability: CVE-2024-38476**

  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- **Vulnerability: CVE-2024-38477**

  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.

- **Vulnerability: CVE-2024-38474**

  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

- **Vulnerability: CVE-2024-40898**

  - CVSS Score: N/A

- Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in
  server/vhost context, allows to potentially leak NTML hashes to
  a malicious server via SSRF and malicious requests.Users are
  recommended to upgrade to version 2.4.62 which fixes this issue.

- Vulnerability: CVE-2011-1176

  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk
    Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP
    Server does not properly handle certain configuration sections that
    specify NiceValue but not AssignUserID, which might allow remote
    attackers to gain privileges by leveraging the root uid and root gid
    of an mpm-itk process.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the
    mod_authnz_external module 3.2.5 and earlier for the Apache HTTP
    Server allows remote attackers to execute arbitrary SQL commands
    via the user field.

- Vulnerability: CVE-2009-0796

  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in
    Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the
    Apache HTTP Server, when /perl-status is accessible, allows remote
    attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module
    before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before
    3.1.1-11637, a module for the Apache HTTP Server, allows remote
    attackers to cause a denial of service (memory consumption) via an
    HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel
    4.3.4a, when the Apache HTTP Server is used, allows remote attackers
    to bypass authentication via directory traversal sequences in a URI
    that ends with the name of a publicly available page, as demonstrated
    by a "/...../" sequence and an account_manage.php/login.php final
    component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2024-27316

  - CVSS Score: N/A
  - Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered
    in nghttp2 in order to generate an informative HTTP 413 response.
    If a client does not stop sending headers, this leads to memory
    exhaustion.

- Vulnerability: CVE-2013-4365

  - CVSS Score: 7.5

– Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2024-38276

  – CVSS Score: N/A
  – Description: Incorrect CSRF token checks resulted in multiple CSRF risks.

- Vulnerability: CVE-2012-3526

  – CVSS Score: 5
  – Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2012-4360

  – CVSS Score: 4.3
  – Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

11.46 IP Address: 159.149.147.194

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 4

- Medium Vulnerabilities: 10

- Low Vulnerabilities: 0

- Total Vulnerabilities: 14

Services Running on IP Address

- Service: nginx

    – Port: 80
    – Version: 1.14.2
    – Location: https://islab.di.unimi.it/

- Service: nginx

    – Port: 443
    – Version: 1.14.2
    – Location: /

Vulnerabilities Found

- Vulnerability: CVE-2023-44487

    – CVSS Score: N/A
    – Description: The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

- Vulnerability: CVE-2019-9516

    – CVSS Score: 6.8
    – Description: Some HTTP/2 implementations are vulnerable to a header leak, potentially leading to a denial of service. The attacker sends a stream of headers with a 0-length header name and 0-length header value, optionally Huffman encoded into 1-byte or greater headers. Some implementations allocate memory for these headers and keep the allocation alive until the session dies. This can consume excess memory.

- Vulnerability: CVE-2019-9513

    – CVSS Score: 7.8
    – Description: Some HTTP/2 implementations are vulnerable to resource loops, potentially leading to a denial of service. The attacker creates multiple request streams and continually shuffles the priority of the streams in a way that causes substantial churn to the priority tree. This can consume excess CPU.

- Vulnerability: CVE-2019-9511

    – CVSS Score: 7.8

- Description: Some HTTP/2 implementations are vulnerable to window size manipulation and stream prioritization manipulation, potentially leading to a denial of service. The attacker requests a large amount of data from a specified resource over multiple streams. They manipulate window size and stream priority to force the server to queue the data in 1-byte chunks. Depending on how efficiently this data is queued, this can consume excess CPU, memory, or both.

- Vulnerability: CVE-2021-23017

  - CVSS Score: 6.8
  - Description: A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting in worker process crash or potential other impact.

- Vulnerability: CVE-2021-3618

  - CVSS Score: 5.8
  - Description: ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MiTM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer.

- Vulnerability: CVE-2019-20372

  - CVSS Score: 4.3
  - Description: NGINX before 1.17.7, with certain error_page configurations, allows HTTP request smuggling, as demonstrated by the ability of an attacker to read unauthorized web pages in environments where NGINX is being fronted by a load balancer.

- Vulnerability: CVE-2018-16845

  - CVSS Score: 5.8
  - Description: nginx before versions 1.15.6, 1.14.1 has a vulnerability in the ngx_http_mp4_module, which might allow an attacker to cause infinite loop in a worker process, cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted mp4 file. The issue only affects nginx if it is built with the ngx_http_mp4_module (the module is not built by default) and the .mp4. directive is used in the configuration file. Further, the attack is only possible if an attacker is able to trigger processing of a specially crafted mp4 file with the ngx_http_mp4_module.

- Vulnerability: CVE-2023-44487

  - CVSS Score: N/A
  - Description: The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

- Vulnerability: CVE-2019-9516

  - CVSS Score: 6.8

- Description: Some HTTP/2 implementations are vulnerable to a header leak, potentially leading to a denial of service. The attacker sends a stream of headers with a 0-length header name and 0-length header value, optionally Huffman encoded into 1-byte or greater headers. Some implementations allocate memory for these headers and keep the allocation alive until the session dies. This can consume excess memory.

- Vulnerability: CVE-2019-9513

  - CVSS Score: 7.8
  - Description: Some HTTP/2 implementations are vulnerable to resource loops, potentially leading to a denial of service. The attacker creates multiple request streams and continually shuffles the priority of the streams in a way that causes substantial churn to the priority tree. This can consume excess CPU.

- Vulnerability: CVE-2019-9511

  - CVSS Score: 7.8
  - Description: Some HTTP/2 implementations are vulnerable to window size manipulation and stream prioritization manipulation, potentially leading to a denial of service. The attacker requests a large amount of data from a specified resource over multiple streams. They manipulate window size and stream priority to force the server to queue the data in 1-byte chunks. Depending on how efficiently this data is queued, this can consume excess CPU, memory, or both.

- Vulnerability: CVE-2021-23017

  - CVSS Score: 6.8
  - Description: A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting in worker process crash or potential other impact.

- Vulnerability: CVE-2021-3618

  - CVSS Score: 5.8
  - Description: ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MiTM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer.

- Vulnerability: CVE-2019-20372

  - CVSS Score: 4.3
  - Description: NGINX before 1.17.7, with certain error_page configurations, allows HTTP request smuggling, as demonstrated by the ability of an attacker to read unauthorized web pages in environments where NGINX is being fronted by a load balancer.

- Vulnerability: CVE-2018-16845

  - CVSS Score: 5.8

– Description: nginx before versions 1.15.6, 1.14.1 has a vulnerability in the ngx_http_mp4_module, which might allow an attacker to cause infinite loop in a worker process, cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted mp4 file. The issue only affects nginx if it is built with the ngx_http_mp4_module (the module is not built by default) and the .mp4. directive is used in the configuration file. Further, the attack is only possible if an attacker is able to trigger processing of a specially crafted mp4 file with the ngx_http_mp4_module.

11.47 IP Address: 159.149.53.100

- Organization: UNI-Milano

- Operating System: Ubuntu

- Critical Vulnerabilities: 0

- High Vulnerabilities: 3

- Medium Vulnerabilities: 8

- Low Vulnerabilities: 1

- Total Vulnerabilities: 12

Services Running on IP Address

- Service: nginx

  - Port: 80
  - Version: 1.18.0
  - Location: https://myariel.unimi.it/

- Service: nginx

  - Port: 443
  - Version: 1.18.0
  - Location: /

Vulnerabilities Found

- Vulnerability: CVE-2023-44487

  - CVSS Score: N/A
  - Description: The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

- Vulnerability: CVE-2021-23017

  - CVSS Score: 6.8
  - Description: A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting in worker process crash or potential other impact.

- Vulnerability: CVE-2021-3618

  - CVSS Score: 5.8
  - Description: ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MiTM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer.

- Vulnerability: CVE-2023-5544

  - CVSS Score: N/A

- Description: Wiki comments required additional sanitizing and access restrictions to prevent a stored XSS risk and potential IDOR risk.

- Vulnerability: CVE-2023-5545

  - CVSS Score: N/A
  - Description: H5P metadata automatically populated the author with the user's username, which could be sensitive information.

- Vulnerability: CVE-2023-5546

  - CVSS Score: N/A
  - Description: ID numbers displayed in the quiz grading report required additional sanitizing to prevent a stored XSS risk.

- Vulnerability: CVE-2023-5547

  - CVSS Score: N/A
  - Description: The course upload preview contained an XSS risk for users uploading unsafe data.

- Vulnerability: CVE-2023-5540

  - CVSS Score: N/A
  - Description: A remote code execution risk was identified in the IMSCP activity. By default this was only available to teachers and managers.

- Vulnerability: CVE-2023-5541

  - CVSS Score: N/A
  - Description: The CSV grade import method contained an XSS risk for users importing the spreadsheet, if it contained unsafe content.

- Vulnerability: CVE-2023-5543

  - CVSS Score: N/A
  - Description: When duplicating a BigBlueButton activity, the original meeting ID was also duplicated instead of using a new ID for the new activity. This could provide unintended access to the original meeting.

- Vulnerability: CVE-2023-5548

  - CVSS Score: N/A
  - Description: Stronger revision number limitations were required on file serving endpoints to improve cache poisoning protection.

- Vulnerability: CVE-2023-5549

  - CVSS Score: N/A
  - Description: Insufficient web service capability checks made it possible to move categories a user had permission to manage, to a parent category they did not have the capability to manage.

- Vulnerability: CVE-2023-23921

  - CVSS Score: N/A
  - Description: The vulnerability was found Moodle which exists due to insufficient sanitization of user-supplied data in some returnurl parameters. A remote attacker can trick the victim to follow a specially crafted link and execute arbitrary HTML and script code in user's browser in context of vulnerable website. This flaw allows a remote attacker to perform cross-site scripting (XSS) attacks.

- Vulnerability: CVE-2022-45152

- CVSS Score: N/A

- Description: A blind Server-Side Request Forgery (SSRF) vulnerability was found in Moodle. This flaw exists due to insufficient validation of user-supplied input in LTI provider library. The library does not utilise Moodle's inbuilt cURL helper, which resulted in a blind SSRF risk. An attacker can send a specially crafted HTTP request and trick the application to initiate requests to arbitrary systems. This vulnerability allows a remote attacker to perform SSRF attacks.

- Vulnerability: CVE-2022-45151

  - CVSS Score: N/A

  - Description: The stored-XSS vulnerability was discovered in Moodle which exists due to insufficient sanitization of user-supplied data in several "social" user profile fields. An attacker could inject and execute arbitrary HTML and script code in user's browser in context of vulnerable website.

- Vulnerability: CVE-2022-45150

  - CVSS Score: N/A

  - Description: A reflected cross-site scripting vulnerability was discovered in Moodle. This flaw exists due to insufficient sanitization of user-supplied data in policy tool. An attacker can trick the victim to open a specially crafted link that executes an arbitrary HTML and script code in user's browser in context of vulnerable website. This vulnerability may allow an attacker to perform cross-site scripting (XSS) attacks to gain access potentially sensitive information and modification of web pages.

- Vulnerability: CVE-2023-28333

  - CVSS Score: N/A

  - Description: The Mustache pix helper contained a potential Mustache injection risk if combined with user input (note: This did not appear to be implemented/exploitable anywhere in the core Moodle LMS).

- Vulnerability: CVE-2023-28332

  - CVSS Score: N/A

  - Description: If the algebra filter was enabled but not functional (eg the necessary binaries were missing from the server), it presented an XSS risk.

- Vulnerability: CVE-2024-38276

  - CVSS Score: N/A

  - Description: Incorrect CSRF token checks resulted in multiple CSRF risks.

- Vulnerability: CVE-2023-28330

  - CVSS Score: N/A

  - Description: Insufficient sanitizing in backup resulted in an arbitrary file read risk. The capability to access this feature is only available to teachers, managers and admins by default.

- Vulnerability: CVE-2022-40316

  - CVSS Score: N/A

  - Description: The H5P activity attempts report did not filter by groups, which in separate groups mode could reveal information to non-editing teachers about attempts/users in groups they should not have access to.

- Vulnerability: CVE-2023-28331

  – CVSS Score: N/A
  – Description: Content output by the database auto-linking filter required additional sanitizing to prevent an XSS risk.

- Vulnerability: CVE-2022-40314

  – CVSS Score: N/A
  – Description: A remote code execution risk when restoring backup files originating from Moodle 1.9 was identified.

- Vulnerability: CVE-2023-28334

  – CVSS Score: N/A
  – Description: Authenticated users were able to enumerate other users' names via the learning plans page.

- Vulnerability: CVE-2022-40313

  – CVSS Score: N/A
  – Description: Recursive rendering of Mustache template helpers containing user input could, in some cases, result in an XSS risk or a page failing to load.

- Vulnerability: CVE-2023-30944

  – CVSS Score: N/A
  – Description: The vulnerability was found Moodle which exists due to insufficient sanitization of user-supplied data in external Wiki method for listing pages. A remote attacker can send a specially crafted request to the affected application and execute limited SQL commands within the application database.

- Vulnerability: CVE-2022-35653

  – CVSS Score: N/A
  – Description: A reflected XSS issue was identified in the LTI module of Moodle. The vulnerability exists due to insufficient sanitization of user-supplied data in the LTI module. A remote attacker can trick the victim to follow a specially crafted link and execute arbitrary HTML and script code in user's browser in context of vulnerable website to steal potentially sensitive information, change appearance of the web page, can perform phishing and drive-by-download attacks. This vulnerability does not impact authenticated users.

- Vulnerability: CVE-2022-35652

  – CVSS Score: N/A
  – Description: An open redirect issue was found in Moodle due to improper sanitization of user-supplied data in mobile auto-login feature. A remote attacker can create a link that leads to a trusted website, however, when clicked, it redirects the victims to arbitrary URL/domain. Successful exploitation of this vulnerability may allow a remote attacker to perform a phishing attack and steal potentially sensitive information.

- Vulnerability: CVE-2022-35651

  – CVSS Score: N/A

– Description: A stored XSS and blind SSRF vulnerability was found in Moodle, occurs due to insufficient sanitization of user-supplied data in the SCORM track details. A remote attacker can trick the victim to follow a specially crafted link and execute arbitrary HTML and script code in user's browser in context of vulnerable website to steal potentially sensitive information, change appearance of the web page, can perform phishing and drive-by-download attacks.

- Vulnerability: CVE-2023-28336

  – CVSS Score: N/A

  – Description: Insufficient filtering of grade report history made it possible for teachers to access the names of users they could not otherwise access.

- Vulnerability: CVE-2024-34008

  – CVSS Score: N/A

  – Description: Actions in the admin management of analytics models did not include the necessary token to prevent a CSRF risk.

- Vulnerability: CVE-2023-35133

  – CVSS Score: N/A

  – Description: An issue in the logic used to check 0.0.0.0 against the cURL blocked hosts lists resulted in an SSRF risk. This flaw affects Moodle versions 4.2, 4.1 to 4.1.3, 4.0 to 4.0.8, 3.11 to 3.11.14, 3.9 to 3.9.21 and earlier unsupported versions.

- Vulnerability: CVE-2023-35132

  – CVSS Score: N/A

  – Description: A limited SQL injection risk was identified on the Mnet SSO access control page. This flaw affects Moodle versions 4.2, 4.1 to 4.1.3, 4.0 to 4.0.8, 3.11 to 3.11.14, 3.9 to 3.9.21 and earlier unsupported versions.

- Vulnerability: CVE-2023-35131

  – CVSS Score: N/A

  – Description: Content on the groups page required additional sanitizing to prevent an XSS risk. This flaw affects Moodle versions 4.2, 4.1 to 4.1.3, 4.0 to 4.0.8 and 3.11 to 3.11.14.

- Vulnerability: CVE-2023-1402

  – CVSS Score: N/A

  – Description: The course participation report required additional checks to prevent roles being displayed which the user did not have access to view.

- Vulnerability: CVE-2021-3618

  – CVSS Score: 5.8

  – Description: ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MiTM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer.

- Vulnerability: CVE-2023-5539

- CVSS Score: N/A
- Description: A remote code execution risk was identified in the Lesson activity. By default this was only available to teachers and managers.

- Vulnerability: CVE-2023-23923

    - CVSS Score: N/A
    - Description: The vulnerability was found Moodle which exists due to insufficient limitations on the "start page" preference. A remote attacker can set that preference for another user. The vulnerability allows a remote attacker to gain unauthorized access to otherwise restricted functionality.

- Vulnerability: CVE-2023-5551

    - CVSS Score: N/A
    - Description: Separate Groups mode restrictions were not honoured in the forum summary report, which would display users from other groups.

- Vulnerability: CVE-2023-5550

    - CVSS Score: N/A
    - Description: In a shared hosting environment that has been misconfigured to allow access to other users' content, a Moodle user who also has direct access to the web server outside of the Moodle webroot could utilise a local file include to achieve remote code execution.

- Vulnerability: CVE-2007-6538

    - CVSS Score: 7.5
    - Description: SQL injection vulnerability in ing/blocks/mrbs/code/web/view_entry.php in the MRBS plugin for Moodle allows remote attackers to execute arbitrary SQL commands via the id parameter.

- Vulnerability: CVE-2023-23922

    - CVSS Score: N/A
    - Description: The vulnerability was found Moodle which exists due to insufficient sanitization of user-supplied data in blog search. A remote attacker can trick the victim to follow a specially crafted link and execute arbitrary HTML and script code in user's browser in context of vulnerable website. This flaw allows a remote attacker to perform cross-site scripting (XSS) attacks.

- Vulnerability: CVE-2022-45149

    - CVSS Score: N/A
    - Description: A vulnerability was found in Moodle which exists due to insufficient validation of the HTTP request origin in course redirect URL. A user's CSRF token was unnecessarily included in the URL when being redirected to a course they have just restored. A remote attacker can trick the victim to visit a specially crafted web page and perform arbitrary actions on behalf of the victim on the vulnerable website. This flaw allows an attacker to perform cross-site request forgery attacks.

- Vulnerability: CVE-2023-28329

    - CVSS Score: N/A
    - Description: Insufficient validation of profile field availability condition resulted in an SQL injection risk (by default only available to teachers and managers).

- Vulnerability: CVE-2022-2986
  - CVSS Score: N/A
  - Description: Enabling and disabling installed H5P libraries did not include the necessary token to prevent a CSRF risk.

- Vulnerability: CVE-2022-40315
  - CVSS Score: N/A
  - Description: A limited SQL injection risk was identified in the "browse list of users" site administration page.

- Vulnerability: CVE-2023-44487
  - CVSS Score: N/A
  - Description: The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

- Vulnerability: CVE-2010-4208
  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the Flash component infrastructure in YUI 2.5.0 through 2.8.1, as used in Bugzilla, Moodle, and other products, allows remote attackers to inject arbitrary web script or HTML via vectors related to uploader/assets/uploader.swf.

- Vulnerability: CVE-2022-30599
  - CVSS Score: 7.5
  - Description: A flaw was found in moodle where an SQL injection risk was identified in Badges code relating to configuring criteria.

- Vulnerability: CVE-2022-30598
  - CVSS Score: 4
  - Description: A flaw was found in moodle where global search results could include author information on some activities where a user may not otherwise have access to it.

- Vulnerability: CVE-2022-40208
  - CVSS Score: N/A
  - Description: In Moodle, insufficient limitations in some quiz web services made it possible for students to bypass sequential navigation during a quiz attempt.

- Vulnerability: CVE-2022-30596
  - CVSS Score: 3.5
  - Description: A flaw was found in moodle where ID numbers displayed when bulk allocating markers to assignments required additional sanitizing to prevent a stored XSS risk.

- Vulnerability: CVE-2010-4207
  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the Flash component infrastructure in YUI 2.4.0 through 2.8.1, as used in Bugzilla, Moodle, and other products, allows remote attackers to inject arbitrary web script or HTML via vectors related to charts/assets/charts.swf.

- Vulnerability: CVE-2022-30597

  – CVSS Score: 5
  – Description: A flaw was found in moodle where the description user field was not hidden when being set as a hidden user field.

- Vulnerability: CVE-2022-30600

  – CVSS Score: 7.5
  – Description: A flaw was found in moodle where logic used to count failed login attempts could result in the account lockout threshold being bypassed.

- Vulnerability: CVE-2022-35650

  – CVSS Score: N/A
  – Description: The vulnerability was found in Moodle, occurs due to input validation error when importing lesson questions. This insufficient path checks results in arbitrary file read risk. This vulnerability allows a remote attacker to perform directory traversal attacks. The capability to access this feature is only available to teachers, managers and admins by default.

- Vulnerability: CVE-2022-35649

  – CVSS Score: N/A
  – Description: The vulnerability was found in Moodle, occurs due to improper input validation when parsing PostScript code. An omitted execution parameter results in a remote code execution risk for sites running GhostScript versions older than 9.50. Successful exploitation of this vulnerability may result in complete compromise of vulnerable system.

- Vulnerability: CVE-2021-23017

  – CVSS Score: 6.8
  – Description: A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting in worker process crash or potential other impact.

11.48 IP Address: 159.149.45.32

- Organization: UNI-Milano

- Operating System: Linux

- Critical Vulnerabilities: 0

- High Vulnerabilities: 3

- Medium Vulnerabilities: 7

- Low Vulnerabilities: 2

- Total Vulnerabilities: 12

Services Running on IP Address

- Service: OpenSSH

  - Port: 22
  - Version: 9.2p1 Debian 2+deb12u3
  - Location:

Vulnerabilities Found

- Vulnerability: CVE-2013-0941

  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2009-2299

  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.

- Vulnerability: CVE-2013-2765

  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.

- Vulnerability: CVE-2011-1176

- CVSS Score: 4.3
- Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

- Vulnerability: CVE-2011-2688

  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2009-0796

  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2007-4723

  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../ " sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.

- Vulnerability: CVE-2012-4001

  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.

- Vulnerability: CVE-2013-4365

  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

- Vulnerability: CVE-2012-3526

  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2012-4360

  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

11.49 IP Address: 159.149.53.132

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 2

- Medium Vulnerabilities: 2

- Low Vulnerabilities: 0

- Total Vulnerabilities: 4

Services Running on IP Address

- Service: Pure-FTPd

  – Port: 21
  – Version: N/A
  – Location:

- Service: Apache httpd

  – Port: 80
  – Version: N/A
  – Location: /

- Service: Apache httpd

  – Port: 443
  – Version: N/A
  – Location: /

Vulnerabilities Found

- Vulnerability: CVE-2013-2220

  – CVSS Score: 7.5
  – Description: Buffer overflow in the radius_get_vendor_attr function in the Radius extension before 1.2.7 for PHP allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a large Vendor Specific Attributes (VSA) length value.

- Vulnerability: CVE-2024-4577

  – CVSS Score: N/A
  – Description: In PHP versions8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in command line given toWin32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc.

- Vulnerability: CVE-2007-3205

  – CVSS Score: 5

- Description: The parse_str function in (1) PHP, (2) Hardened-PHP, and (3) Suhosin, when called without a second parameter, might allow remote attackers to overwrite arbitrary variables by specifying variable names and values in the string to be parsed. NOTE: it is not clear whether this is a design limitation of the function or a bug in PHP, although it is likely to be regarded as a bug in Hardened-PHP and Suhosin.

- Vulnerability: CVE-2024-5458

  - CVSS Score: N/A

  - Description: In PHP versions8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, due to a code logic error, filtering functions such as filter_var when validating URLs(FILTER_VALIDATE_URL) for certain types of URLs the function will result in invalid user information (username + password part of URLs) being treated as valid user information. This may lead to the downstream code accepting invalid URLs as valid and parsing them incorrectly.

- Vulnerability: CVE-2013-2220

  - CVSS Score: 7.5

  - Description: Buffer overflow in the radius_get_vendor_attr function in the Radius extension before 1.2.7 for PHP allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a large Vendor Specific Attributes (VSA) length value.

- Vulnerability: CVE-2024-4577

  - CVSS Score: N/A

  - Description: In PHP versions8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in command line given toWin32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc.

- Vulnerability: CVE-2007-3205

  - CVSS Score: 5

  - Description: The parse_str function in (1) PHP, (2) Hardened-PHP, and (3) Suhosin, when called without a second parameter, might allow remote attackers to overwrite arbitrary variables by specifying variable names and values in the string to be parsed. NOTE: it is not clear whether this is a design limitation of the function or a bug in PHP, although it is likely to be regarded as a bug in Hardened-PHP and Suhosin.

- Vulnerability: CVE-2024-5458

  - CVSS Score: N/A

  - Description: In PHP versions8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, due to a code logic error, filtering functions such as filter_var when validating URLs(FILTER_VALIDATE_URL) for certain types of URLs the function will result in invalid user information (username + password part of URLs) being treated as valid user information. This may lead to the downstream code accepting invalid URLs as valid and parsing them incorrectly.

11.50   IP Address: 159.149.53.246

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 1

- Medium Vulnerabilities: 1

- Low Vulnerabilities: 0

- Total Vulnerabilities: 2

Services Running on IP Address

- Service: nginx

  – Port: 80
  – Version: N/A
  – Location: https://icona.crc.unimi.it/

- Service: nginx

  – Port: 443
  – Version: N/A
  – Location: /

Vulnerabilities Found

- Vulnerability: CVE-2013-2220

  – CVSS Score: 7.5
  – Description: Buffer overflow in the radius_get_vendor_attr function in the Radius extension before 1.2.7 for PHP allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a large Vendor Specific Attributes (VSA) length value.

- Vulnerability: CVE-2024-4577

  – CVSS Score: N/A
  – Description: In PHP versions8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in command line given toWin32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc.

- Vulnerability: CVE-2007-3205

  – CVSS Score: 5
  – Description: The parse_str function in (1) PHP, (2) Hardened-PHP, and (3) Suhosin, when called without a second parameter, might allow remote attackers to overwrite arbitrary variables by specifying variable names and values in the string to be parsed. NOTE: it is not clear whether this is a design limitation of the function or a bug in PHP, although it is likely to be regarded as a bug in Hardened-PHP and Suhosin.

- Vulnerability: CVE-2024-5458

– CVSS Score: N/A

– Description: In PHP versions8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.*
                 before 8.3.8, due to a code logic error, filtering functions such
                 as filter_var when validating URLs(FILTER_VALIDATE_URL) for certain
                 types of URLs the function will result in invalid user information
                 (username + password part of URLs) being treated as valid user
                 information. This may lead to the downstream code accepting invalid
                 URLs as valid and parsing them incorrectly.

11.51 IP Address: 159.149.15.42

- Organization: UNI-Milano

- Operating System: Windows

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 12

- Low Vulnerabilities: 0

- Total Vulnerabilities: 12

Services Running on IP Address

- Service: Microsoft ftpd

  - Port: 21
  - Version: N/A
  - Location:

- Service: Microsoft IIS httpd

  - Port: 80
  - Version: 8.0
  - Location: https://srv-ariel.ctu.unimi.it/

- Service: Microsoft IIS httpd

  - Port: 443
  - Version: 8.0
  - Location: /

Vulnerabilities Found

- Vulnerability: CVE-2014-4078

  - CVSS Score: 5.1
  - Description: The IP Security feature in Microsoft Internet Information Services
                (IIS) 8.0 and 8.5 does not properly process wildcard allow and deny
                rules for domains within the "IP Address and Domain Restrictions"
                list, which makes it easier for remote attackers to bypass an
                intended rule set via an HTTP request, aka "IIS Security Feature
                Bypass Vulnerability."

- Vulnerability: CVE-2014-4078

  - CVSS Score: 5.1
  - Description: The IP Security feature in Microsoft Internet Information Services
                (IIS) 8.0 and 8.5 does not properly process wildcard allow and deny
                rules for domains within the "IP Address and Domain Restrictions"
                list, which makes it easier for remote attackers to bypass an
                intended rule set via an HTTP request, aka "IIS Security Feature
                Bypass Vulnerability."

- Vulnerability: CVE-2018-14040

  - CVSS Score: 4.3
  - Description: In Bootstrap before 4.1.2, XSS is possible in the collapse
                data-parent attribute.

- Vulnerability: CVE-2019-11358

  – CVSS Score: 4.3

  – Description: jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.

- Vulnerability: CVE-2016-10735

  – CVSS Score: 4.3

  – Description: In Bootstrap 3.x before 3.4.0 and 4.x-beta before 4.0.0-beta.2, XSS is possible in the data-target attribute, a different vulnerability than CVE-2018-14041.

- Vulnerability: CVE-2019-8331

  – CVSS Score: 4.3

  – Description: In Bootstrap before 3.4.1 and 4.3.x before 4.3.1, XSS is possible in the tooltip or popover data-template attribute.

- Vulnerability: CVE-2018-14042

  – CVSS Score: 4.3

  – Description: In Bootstrap before 4.1.2, XSS is possible in the data-container property of tooltip.

- Vulnerability: CVE-2018-20676

  – CVSS Score: 4.3

  – Description: In Bootstrap before 3.4.0, XSS is possible in the tooltip data-viewport attribute.

- Vulnerability: CVE-2018-20677

  – CVSS Score: 4.3

  – Description: In Bootstrap before 3.4.0, XSS is possible in the affix configuration target property.

- Vulnerability: CVE-2015-9251

  – CVSS Score: 4.3

  – Description: jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.

- Vulnerability: CVE-2020-11022

  – CVSS Score: 4.3

  – Description: In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

- Vulnerability: CVE-2020-11023

  – CVSS Score: 4.3

  – Description: In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

11.52   IP Address: 159.149.47.56

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 7

- Low Vulnerabilities: 0

- Total Vulnerabilities: 7

Services Running on IP Address

- Service: OpenSSH

    – Port: 22
    – Version: 8.4p1 Debian 5+deb11u3
    – Location:

- Service: nginx

    – Port: 443
    – Version: 1.18.0
    – Location: /

Vulnerabilities Found

- Vulnerability: CVE-2023-44487

    – CVSS Score: N/A
    – Description: The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

- Vulnerability: CVE-2021-23017

    – CVSS Score: 6.8
    – Description: A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting in worker process crash or potential other impact.

- Vulnerability: CVE-2021-3618

    – CVSS Score: 5.8
    – Description: ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MiTM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer.

- Vulnerability: CVE-2023-44487

    – CVSS Score: N/A

1160

– Description: The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

- Vulnerability: CVE-2019-11358

  – CVSS Score: 4.3
  – Description: jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.

- Vulnerability: CVE-2021-23017

  – CVSS Score: 6.8
  – Description: A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting in worker process crash or potential other impact.

- Vulnerability: CVE-2021-3618

  – CVSS Score: 5.8
  – Description: ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MiTM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer.

- Vulnerability: CVE-2020-11022

  – CVSS Score: 4.3
  – Description: In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

- Vulnerability: CVE-2020-11023

  – CVSS Score: 4.3
  – Description: In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

11.53 IP Address: 159.149.15.43

- Organization: UNI-Milano

- Operating System: Windows

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 4

- Low Vulnerabilities: 0

- Total Vulnerabilities: 4

Services Running on IP Address

- Service: Microsoft IIS httpd

    - Port: 443
    - Version: 10.0
    - Location: /

Vulnerabilities Found

- Vulnerability: CVE-2015-9251

    - CVSS Score: 4.3
    - Description: jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.

- Vulnerability: CVE-2019-11358

    - CVSS Score: 4.3
    - Description: jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.

- Vulnerability: CVE-2020-11022

    - CVSS Score: 4.3
    - Description: In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

- Vulnerability: CVE-2020-11023

    - CVSS Score: 4.3
    - Description: In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

11.54   IP Address: 159.149.47.62

- Organization: UNI-Milano

- Operating System: Ubuntu

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 4

- Low Vulnerabilities: 0

- Total Vulnerabilities: 4

Services Running on IP Address

- Service: OpenSSH

  - Port: 22
  - Version: 8.2p1 Ubuntu 4ubuntu0.11
  - Location:

- Service: nginx

  - Port: 80
  - Version: 1.18.0
  - Location: /

- Service: nginx

  - Port: 443
  - Version: 1.18.0
  - Location: /

Vulnerabilities Found

- Vulnerability: CVE-2023-44487

  - CVSS Score: N/A
  - Description: The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

- Vulnerability: CVE-2021-23017

  - CVSS Score: 6.8
  - Description: A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting in worker process crash or potential other impact.

- Vulnerability: CVE-2021-3618

  - CVSS Score: 5.8
  - Description: ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MiTM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer.

- Vulnerability: CVE-2023-44487

  - CVSS Score: N/A
  - Description: The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

- Vulnerability: CVE-2021-23017

  - CVSS Score: 6.8
  - Description: A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting in worker process crash or potential other impact.

- Vulnerability: CVE-2021-3618

  - CVSS Score: 5.8
  - Description: ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MiTM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer.

11.55 IP Address: 159.149.53.196

- Organization: UNI-Milano

- Operating System: Windows

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 2

- Low Vulnerabilities: 0

- Total Vulnerabilities: 2

Services Running on IP Address

- Service: Microsoft IIS httpd

  - Port: 443
  - Version: 10.0
  - Location: /

Vulnerabilities Found

- Vulnerability: CVE-2020-11022

  - CVSS Score: 4.3
  - Description: In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

- Vulnerability: CVE-2020-11023

  - CVSS Score: 4.3
  - Description: In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

11.56 IP Address: 159.149.47.77

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 2

- Low Vulnerabilities: 0

- Total Vulnerabilities: 2

Services Running on IP Address

- Service: nginx

  – Port: 80
  – Version: 1.20.1
  – Location: https://159.149.47.77/

Vulnerabilities Found

- Vulnerability: CVE-2023-44487

  – CVSS Score: N/A
  – Description: The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

- Vulnerability: CVE-2021-3618

  – CVSS Score: 5.8
  – Description: ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MiTM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer.

- Vulnerability: CVE-2023-44487

  – CVSS Score: N/A
  – Description: The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

- Vulnerability: CVE-2021-3618

  – CVSS Score: 5.8
  – Description: ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MiTM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer.

11.57 IP Address: 159.149.53.239

- Organization: UNI-Milano

- Operating System: Windows

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 2

- Low Vulnerabilities: 0

- Total Vulnerabilities: 2

Services Running on IP Address

- Service: Microsoft IIS httpd

  - Port: 443
  - Version: 8.0
  - Location: /

Vulnerabilities Found

- Vulnerability: CVE-2014-4078

  - CVSS Score: 5.1
  - Description: The IP Security feature in Microsoft Internet Information Services (IIS) 8.0 and 8.5 does not properly process wildcard allow and deny rules for domains within the "IP Address and Domain Restrictions" list, which makes it easier for remote attackers to bypass an intended rule set via an HTTP request, aka "IIS Security Feature Bypass Vulnerability."

- Vulnerability: CVE-2014-4078

  - CVSS Score: 5.1
  - Description: The IP Security feature in Microsoft Internet Information Services (IIS) 8.0 and 8.5 does not properly process wildcard allow and deny rules for domains within the "IP Address and Domain Restrictions" list, which makes it easier for remote attackers to bypass an intended rule set via an HTTP request, aka "IIS Security Feature Bypass Vulnerability."

11.58 IP Address: 159.149.145.84

- Organization: UNI-Milano

- Operating System: Ubuntu

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 2

- Low Vulnerabilities: 0

- Total Vulnerabilities: 2

Services Running on IP Address

- Service: OpenSSH

  - Port: 22
  - Version: 8.2p1 Ubuntu-4ubuntu0.11
  - Location:

- Service: nginx

  - Port: 443
  - Version: 1.18.0
  - Location: /

- Service: N/A

  - Port: 5001
  - Version: N/A
  - Location:

- Service: N/A

  - Port: 8000
  - Version: N/A
  - Location: /

- Service: N/A

  - Port: 8040
  - Version: N/A
  - Location: /

- Service: N/A

  - Port: 8545
  - Version: N/A
  - Location:

Vulnerabilities Found

- Vulnerability: CVE-2023-44487

  – CVSS Score: N/A
  – Description: The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

- Vulnerability: CVE-2021-23017

  – CVSS Score: 6.8
  – Description: A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting in worker process crash or potential other impact.

- Vulnerability: CVE-2021-3618

  – CVSS Score: 5.8
  – Description: ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MiTM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer.

11.59   IP Address: 159.149.53.90

- Organization: UNI-Milano

- Operating System: Windows

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 1

- Low Vulnerabilities: 0

- Total Vulnerabilities: 1

Services Running on IP Address

- Service: Microsoft IIS httpd

    - Port: 80
    - Version: 8.5
    - Location: /

Vulnerabilities Found

- Vulnerability: CVE-2014-4078

    - CVSS Score: 5.1
    - Description: The IP Security feature in Microsoft Internet Information Services
                    (IIS) 8.0 and 8.5 does not properly process wildcard allow and deny
                    rules for domains within the "IP Address and Domain Restrictions"
                    list, which makes it easier for remote attackers to bypass an
                    intended rule set via an HTTP request, aka "IIS Security Feature
                    Bypass Vulnerability."

11.60 IP Address: 18.192.231.252

- Organization: A100 ROW GmbH

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: N/A
  - Port: 80
  - Version: N/A
  - Location: https://urlcatch.com/

- Service: N/A
  - Port: 443
  - Version: N/A
  - Location: /

No vulnerabilities found for this IP address.

11.61   IP Address: 159.149.145.162

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: OpenSSH

  - Port: 22
  - Version: 8.2p1 Ubuntu-4ubuntu0.11
  - Location:

- Service: nginx

  - Port: 443
  - Version: 1.26.0
  - Location: /

No vulnerabilities found for this IP address.

11.62 IP Address: 159.149.147.186

- Organization: UNI-Milano
- Operating System: N/A
- Critical Vulnerabilities: 0
- High Vulnerabilities: 0
- Medium Vulnerabilities: 0
- Low Vulnerabilities: 0
- Total Vulnerabilities: 0

Services Running on IP Address

- Service: OpenSSH
    - Port: 22
    - Version: 8.9p1 Ubuntu 3ubuntu0.10
    - Location:
- Service: N/A
    - Port: 80
    - Version: N/A
    - Location: https://159.149.147.186:443/
- Service: N/A
    - Port: 443
    - Version: N/A
    - Location: /

No vulnerabilities found for this IP address.

11.63 IP Address: 159.149.47.22

- Organization: UNI-Milano

- Operating System: Ubuntu

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: OpenSSH

    - Port: 22
    - Version: 7.6p1 Ubuntu-4ubuntu0.5
    - Location:

No vulnerabilities found for this IP address.

11.64 IP Address: 159.149.53.247

- Organization: UNI-Milano

- Operating System: Windows

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: Microsoft IIS httpd

    – Port: 80
    – Version: 10.0
    – Location: /

- Service: Microsoft IIS httpd

    – Port: 443
    – Version: 10.0
    – Location: /

No vulnerabilities found for this IP address.

11.65 IP Address: 159.149.106.180

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: nginx

    - Port: 443
    - Version: N/A
    - Location: /

- Service: N/A

    - Port: 5060
    - Version: N/A
    - Location:

No vulnerabilities found for this IP address.

11.66 IP Address: 88.99.2.212

- Organization: Hetzner Online GmbH

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: N/A

  – Port: 443
  – Version: N/A
  – Location:

No vulnerabilities found for this IP address.

11.67 IP Address: 159.149.53.34

- Organization: UNI-Milano
- Operating System: Windows
- Critical Vulnerabilities: 0
- High Vulnerabilities: 0
- Medium Vulnerabilities: 0
- Low Vulnerabilities: 0
- Total Vulnerabilities: 0

Services Running on IP Address

- Service: Microsoft IIS httpd
    - Port: 443
    - Version: 10.0
    - Location: https://cas.unimi.it/login?service=https%3a%2f%2fpresenze.unimi.it%2fStartWeb%

No vulnerabilities found for this IP address.

11.68 IP Address: 159.149.53.130

- Organization: UNI-Milano
- Operating System: N/A
- Critical Vulnerabilities: 0
- High Vulnerabilities: 0
- Medium Vulnerabilities: 0
- Low Vulnerabilities: 0
- Total Vulnerabilities: 0

Services Running on IP Address

- Service: N/A
  - Port: 443
  - Version: N/A
  - Location: /

No vulnerabilities found for this IP address.

11.69 IP Address: 50.18.215.94

- Organization: Amazon.com, Inc.

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: N/A

    - Port: 80
    - Version: N/A
    - Location: https://irvingsda.org/

- Service: N/A

    - Port: 443
    - Version: N/A
    - Location: https://www.southindiaguide.com/

No vulnerabilities found for this IP address.

11.70 IP Address: 52.101.73.12

- Organization: Microsoft Corporation

- Operating System: Windows

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: Microsoft Exchange smtpd

  - Port: 25
  - Version: N/A
  - Location:

No vulnerabilities found for this IP address.

11.71 IP Address: 104.18.11.29

- Organization: Cloudflare, Inc.

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: N/A

  - Port: 80
  - Version: N/A
  - Location: https://www.unimi.it/

- Service: N/A

  - Port: 443
  - Version: N/A
  - Location: http://www.unimi.it/it

- Service: N/A

  - Port: 8880
  - Version: N/A
  - Location:

No vulnerabilities found for this IP address.

11.72 IP Address: 159.149.145.216

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: OpenSSH

  - Port: 22
  - Version: 8.9p1 Ubuntu-3ubuntu0.10
  - Location:

- Service: N/A

  - Port: 80
  - Version: N/A
  - Location: https://159.149.145.216/

No vulnerabilities found for this IP address.

11.73   IP Address: 159.149.10.1

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: N/A

    – Port: 53
    – Version: N/A
    – Location:

- Service: N/A

    – Port: 53
    – Version: N/A
    – Location:

- Service: N/A

    – Port: 123
    – Version: N/A
    – Location:

No vulnerabilities found for this IP address.

11.74   IP Address: 50.18.142.31

- Organization: Amazon.com, Inc.

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: N/A

  - Port: 80
  - Version: N/A
  - Location: https://karatekicks.netlify.app/

- Service: N/A

  - Port: 443
  - Version: N/A
  - Location: https://www.venturelaboinvestment.co.jp/

No vulnerabilities found for this IP address.

11.75 IP Address: 104.18.10.29

- Organization: Cloudflare, Inc.

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: N/A

  - Port: 80
  - Version: N/A
  - Location: https://www.unibs.it/

- Service: N/A

  - Port: 443
  - Version: N/A
  - Location: /

- Service: N/A

  - Port: 2087
  - Version: N/A
  - Location:

- Service: N/A

  - Port: 8880
  - Version: N/A
  - Location:

No vulnerabilities found for this IP address.

11.76 IP Address: 159.149.129.169

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: OpenSSH

  - Port: 22
  - Version: 8.2p1 Ubuntu-4ubuntu0.11
  - Location:

- Service: OpenSSH

  - Port: 2222
  - Version: 8.2p1 Ubuntu 4ubuntu0.11
  - Location:

No vulnerabilities found for this IP address.

11.77 IP Address: 52.101.68.29

- Organization: Microsoft Corporation

- Operating System: Windows

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: Microsoft Exchange smtpd

  - Port: 25
  - Version: N/A
  - Location:

No vulnerabilities found for this IP address.

11.78 IP Address: 159.149.129.229

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: Apache httpd

  - Port: 80
  - Version: N/A
  - Location: /

- Service: Apache httpd

  - Port: 443
  - Version: N/A
  - Location: /

No vulnerabilities found for this IP address.

11.79   IP Address: 159.149.145.136

- Organization: UNI-Milano
- Operating System: N/A
- Critical Vulnerabilities: 0
- High Vulnerabilities: 0
- Medium Vulnerabilities: 0
- Low Vulnerabilities: 0
- Total Vulnerabilities: 0

Services Running on IP Address

- Service: OpenSSH
  - Port: 22
  - Version: 8.9p1 Ubuntu-3ubuntu0.10
  - Location:

- Service: N/A
  - Port: 25
  - Version: N/A
  - Location:

- Service: nginx
  - Port: 80
  - Version: N/A
  - Location: https://159.149.145.136/

- Service: N/A
  - Port: 143
  - Version: N/A
  - Location:

- Service: nginx
  - Port: 443
  - Version: N/A
  - Location: /

- Service: N/A
  - Port: 465
  - Version: N/A
  - Location:

- Service: N/A
  - Port: 587
  - Version: N/A
  - Location:

- Service: N/A
  - Port: 993
  - Version: N/A
  - Location:

No vulnerabilities found for this IP address.

1190

11.80 IP Address: 78.47.83.247

- Organization: Hetzner Online GmbH

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: N/A
    - Port: 21
    - Version: N/A
    - Location:

- Service: N/A
    - Port: 22
    - Version: N/A
    - Location:

- Service: Apache httpd
    - Port: 80
    - Version: N/A
    - Location: https://yogaschule-karin-lehmann.de/

- Service: N/A
    - Port: 110
    - Version: N/A
    - Location:

- Service: N/A
    - Port: 143
    - Version: N/A
    - Location:

- Service: Apache httpd
    - Port: 443
    - Version: N/A
    - Location: /

- Service: N/A
    - Port: 465
    - Version: N/A
    - Location:

- Service: N/A

- Port: 587
  - Version: N/A
  - Location:

- Service: N/A
  - Port: 993
  - Version: N/A
  - Location:

- Service: N/A
  - Port: 995
  - Version: N/A
  - Location:

No vulnerabilities found for this IP address.

11.81 IP Address: 2606:4700::6812:b1d

- Organization: Cloudflare, Inc.

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: N/A

    - Port: 443
    - Version: N/A
    - Location: http://www.unimi.it/it

No vulnerabilities found for this IP address.

11.82 IP Address: 159.149.53.51

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: Pure-FTPd

  - Port: 21
  - Version: N/A
  - Location:

- Service: Apache httpd

  - Port: 80
  - Version: N/A
  - Location: https://159.149.53.51/

No vulnerabilities found for this IP address.

11.83 IP Address: 172.64.151.32

- Organization: Cloudflare, Inc.

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: N/A

  - Port: 80
  - Version: N/A
  - Location: https://ssl1.prod.s1search.co/

- Service: N/A

  - Port: 2087
  - Version: N/A
  - Location:

- Service: N/A

  - Port: 8880
  - Version: N/A
  - Location:

No vulnerabilities found for this IP address.

11.84 IP Address: 2606:4700::6812:a1d

- Organization: Cloudflare, Inc.

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: N/A

  – Port: 443
  – Version: N/A
  – Location: http://www.unimi.it/it

No vulnerabilities found for this IP address.

11.85 IP Address: 52.101.68.27

- Organization: Microsoft Corporation

- Operating System: Windows

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: Microsoft Exchange smtpd

    - Port: 25
    - Version: N/A
    - Location:

No vulnerabilities found for this IP address.

11.86 IP Address: 159.149.145.148

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: OpenSSH

  - Port: 22
  - Version: 8.9p1 Ubuntu-3ubuntu0.10
  - Location:

- Service: N/A

  - Port: 80
  - Version: N/A
  - Location: https://159.149.145.148/

- Service: Ollama

  - Port: 11434
  - Version: N/A
  - Location: /

No vulnerabilities found for this IP address.

11.87 IP Address: 159.149.47.225

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: nginx

  - Port: 80
  - Version: N/A
  - Location: https://159.149.47.225/

- Service: NoMachine NX Server remote desktop

  - Port: 4000
  - Version: 6.18.1
  - Location:

No vulnerabilities found for this IP address.

11.88 IP Address: 216.147.214.138

- Organization: Ex Libris (USA) Inc

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: N/A
  - Port: 80
  - Version: N/A
  - Location: https://eu02.primo.exlibrisgroup.com/

- Service: N/A
  - Port: 443
  - Version: N/A
  - Location: /

No vulnerabilities found for this IP address.

11.89 IP Address: 35.156.221.86

- Organization: A100 ROW GmbH

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: AWS ELB

  - Port: 80
  - Version: 2.0
  - Location: https://35.156.221.86:443/

No vulnerabilities found for this IP address.

11.90 IP Address: 52.59.135.101

- Organization: A100 ROW GmbH

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: AWS ELB

  - Port: 80
  - Version: 2.0
  - Location: https://52.59.135.101:443/

No vulnerabilities found for this IP address.

11.91 IP Address: 130.186.7.246

- Organization: CINECA - Casalecchio di Reno (BO)

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: N/A
    - Port: 80
    - Version: N/A
    - Location: https://sie.cdl.unimi.it/

- Service: Apache httpd
    - Port: 443
    - Version: N/A
    - Location: http://biotecnologia.cdl.unimi.it/it

No vulnerabilities found for this IP address.

11.92 IP Address: 159.149.105.179

- Organization: UNI-Milano
- Operating System: N/A
- Critical Vulnerabilities: 0
- High Vulnerabilities: 0
- Medium Vulnerabilities: 0
- Low Vulnerabilities: 0
- Total Vulnerabilities: 0

Services Running on IP Address

- Service: Apache httpd
    - Port: 443
    - Version: N/A
    - Location: /

No vulnerabilities found for this IP address.

11.93 IP Address: 159.149.53.252

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: Apache httpd

  - Port: 80
  - Version: N/A
  - Location: /

No vulnerabilities found for this IP address.

11.94   IP Address: 3.126.205.183

- Organization: A100 ROW GmbH

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: AWS ELB

  - Port: 443
  - Version: 2.0
  - Location: https://login.microsoftonline.com/21956b19-fed2-44b7-90cf-b6d281c0a42a/oauth2/

No vulnerabilities found for this IP address.

11.95 IP Address: 159.149.145.228

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: OpenSSH

  - Port: 22
  - Version: 8.2p1 Ubuntu-4ubuntu0.11
  - Location:

- Service: nginx

  - Port: 443
  - Version: 1.27.1
  - Location: /

- Service: OpenSSH

  - Port: 2222
  - Version: 8.2p1 Ubuntu-4ubuntu0.11
  - Location:

No vulnerabilities found for this IP address.

11.96 IP Address: 130.186.28.54

- Organization: CINECA - Casalecchio di Reno (BO)

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: N/A

  - Port: 80
  - Version: N/A
  - Location: https://130.186.28.54/

- Service: Apache httpd

  - Port: 443
  - Version: N/A
  - Location: /

No vulnerabilities found for this IP address.

11.97 IP Address: 159.149.145.95

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: OpenSSH

  - Port: 22
  - Version: 8.9p1 Ubuntu-3ubuntu0.10
  - Location:

- Service: PostgreSQL

  - Port: 5432
  - Version: 16.0 - 16.2
  - Location:

- Service: N/A

  - Port: 8080
  - Version: N/A
  - Location: /

No vulnerabilities found for this IP address.

11.98 IP Address: 159.149.116.206

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: nginx

  - Port: 443
  - Version: N/A
  - Location: /

No vulnerabilities found for this IP address.

11.99   IP Address: 3.70.101.28

- Organization: A100 ROW GmbH

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: N/A
    - Port: 80
    - Version: N/A
    - Location: https://kljastrond.com/

- Service: N/A
    - Port: 443
    - Version: N/A
    - Location: /

No vulnerabilities found for this IP address.

11.100 IP Address: 159.149.10.20

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: N/A
  - Port: 25
  - Version: N/A
  - Location:

- Service: N/A
  - Port: 110
  - Version: N/A
  - Location:

- Service: N/A
  - Port: 143
  - Version: N/A
  - Location:

- Service: Postfix smtpd
  - Port: 465
  - Version: N/A
  - Location:

- Service: N/A
  - Port: 993
  - Version: N/A
  - Location:

- Service: N/A
  - Port: 995
  - Version: N/A
  - Location:

No vulnerabilities found for this IP address.

11.101   IP Address: 104.18.36.224

- Organization: Cloudflare, Inc.

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: N/A
    - Port: 80
    - Version: N/A
    - Location: https://ssl1.prod.s1search.co/

- Service: N/A
    - Port: 8880
    - Version: N/A
    - Location:

No vulnerabilities found for this IP address.

11.102   IP Address: 52.101.68.8

- Organization: Microsoft Corporation

- Operating System: Windows

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: Microsoft Exchange smtpd

  - Port: 25
  - Version: N/A
  - Location:

No vulnerabilities found for this IP address.

11.103   IP Address: 159.149.145.164

- Organization: UNI-Milano
- Operating System: N/A
- Critical Vulnerabilities: 0
- High Vulnerabilities: 0
- Medium Vulnerabilities: 0
- Low Vulnerabilities: 0
- Total Vulnerabilities: 0

Services Running on IP Address

- Service: N/A
    - Port: 80
    - Version: N/A
    - Location: https://159.149.145.164/

No vulnerabilities found for this IP address.

11.104   IP Address: 159.149.53.241

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: Pure-FTPd

  - Port: 21
  - Version: N/A
  - Location:

- Service: Apache httpd

  - Port: 80
  - Version: N/A
  - Location: /

- Service: Apache httpd

  - Port: 443
  - Version: N/A
  - Location: /

No vulnerabilities found for this IP address.

11.105   IP Address: 159.149.145.161

- Organization: UNI-Milano

- Operating System: Linux

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: OpenSSH

    - Port: 22
    - Version: 8.9p1 Ubuntu 3ubuntu0.10
    - Location:

No vulnerabilities found for this IP address.

11.106 IP Address: 159.149.53.144

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: Apache httpd

  - Port: 80
  - Version: N/A
  - Location: https://unimi.primo.exlibrisgroup.com/

- Service: Apache httpd

  - Port: 443
  - Version: N/A
  - Location: https://unimi.primo.exlibrisgroup.com/

No vulnerabilities found for this IP address.

11.107 IP Address: 159.149.133.37

- Organization: UNI-Milano

- Operating System: Ubuntu

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: OpenSSH

  - Port: 22
  - Version: 9.6p1 Ubuntu-3ubuntu13.4
  - Location:

- Service: nginx

  - Port: 80
  - Version: 1.24.0
  - Location: /

- Service: nginx

  - Port: 443
  - Version: 1.24.0
  - Location: /

No vulnerabilities found for this IP address.

11.108   IP Address: 185.199.110.153

- Organization: GitHub, Inc.

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: N/A
  - Port: 80
  - Version: N/A
  - Location: /

- Service: N/A
  - Port: 443
  - Version: N/A
  - Location: /

No vulnerabilities found for this IP address.

11.109   IP Address: 159.149.104.138

- Organization: UNI-Milano

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: N/A

    - Port: 443
    - Version: N/A
    - Location: /

No vulnerabilities found for this IP address.

11.110 IP Address: 159.149.116.203

- Organization: UNI-Milano

- Operating System: Windows

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: Microsoft IIS httpd

    - Port: 80
    - Version: 10.0
    - Location: /

No vulnerabilities found for this IP address.

11.111   IP Address: 18.184.101.234

- Organization: A100 ROW GmbH

- Operating System: N/A

- Critical Vulnerabilities: 0

- High Vulnerabilities: 0

- Medium Vulnerabilities: 0

- Low Vulnerabilities: 0

- Total Vulnerabilities: 0

Services Running on IP Address

- Service: AWS ELB

  - Port: 80
  - Version: 2.0
  - Location: https://18.184.101.234:443/

- Service: N/A

  - Port: 443
  - Version: N/A
  - Location: /

No vulnerabilities found for this IP address.