Report for Domain: conad.it

Generated by Apollo

August 22, 2024

Summary of Findings

Below are some key statistics from the data provided:

- **Number of IPs**: 157
- **Number of Domains**: 167
- **Number of Emails**: 4
- **Number of Resolved Hosts**: 60
- **Number of Mail Servers**: 5
- **Number of URLs**: 60

IP Addresses found

Below is the list of IP addresses found:

- 52.51.238.226
- 63.33.34.226
- 178.19.147.44
- 34.250.129.210
- 34.252.201.201
- 52.16.9.41
- 212.35.217.197
- 151.0.185.49
- 109.168.115.125
- 52.210.8.241
- 52.48.120.101
- 52.101.68.3
- 195.103.103.67
- 88.48.254.216
- 52.211.9.207
- 185.127.134.97
- 54.194.141.210
- 52.211.67.199

- 54.154.106.249
- 52.16.137.238
- 34.241.181.233
- 54.170.134.201
- 34.248.87.156
- 151.11.251.115
- 54.229.255.32
- 151.101.131.10
- 34.254.16.163
- 54.220.131.240
- 54.194.178.83
- 151.11.251.89
- 52.210.104.122
- 46.137.117.50
- 52.210.127.205
- 52.210.77.134
- 3.122.148.93
- 40.68.184.232
- 52.48.201.30
- 54.72.41.246
- 52.213.192.243
- 109.68.26.105
- 52.157.89.4
- 149.72.45.82
- 54.78.116.130
- 88.48.254.212
- 151.11.251.114
- 52.31.57.107
- 52.210.69.61
- 195.103.103.97
- 63.32.160.121
- 52.211.65.105
- 46.51.207.138
- 146.75.55.10
- 52.213.179.200
- 52.16.225.72

- 213.171.166.88
- 52.50.88.161
- 54.154.197.101
- 95.216.54.125
- 15.161.61.5
- 128.65.125.179
- 151.11.251.125
- 54.78.138.11
- 54.170.100.107
- 151.11.251.73
- 151.11.251.107
- 195.103.103.92
- 151.101.3.10
- 193.240.211.109
- 34.255.210.70
- 34.253.26.23
- 151.11.251.118
- 54.220.186.7
- 54.72.34.250
- 54.76.88.210
- 165.22.20.19
- 54.73.124.6
- 35.233.86.30
- 52.18.34.50
- 128.65.125.180
- 109.68.26.92
- 52.213.201.198
- 34.250.105.197
- 217.29.160.31
- 54.75.85.203
- 63.32.26.88
- 151.11.251.101
- 62.101.80.232
- 151.11.251.81
- 81.24.236.129
- 80.211.62.104

- 34.242.149.90
- 88.48.254.200
- 63.32.225.158
- 151.101.67.10
- 52.211.105.177
- 52.210.221.125
- 3.248.134.241
- 54.194.42.165
- 34.240.71.165
- 63.34.224.0
- 18.202.157.184
- 54.76.102.248
- 54.171.29.175
- 109.68.26.113
- 52.18.240.201
- 63.140.62.222
- 217.64.205.178
- 34.253.59.24
- 52.210.230.161
- 54.220.116.192
- 151.101.195.10
- 3.127.103.86
- 52.49.3.128
- 109.68.26.97
- 54.220.187.182
- 52.209.52.225
- 52.101.68.18
- 52.18.64.111
- 54.73.61.50
- 34.254.57.254
- 52.211.37.138
- 52.101.73.22
- 99.81.72.6
- 15.160.39.142
- 116.203.32.52
- 63.32.7.7

- 109.68.26.91
- 79.125.61.213
- 77.39.208.224
- 77.39.208.226
- 109.68.24.221
- 99.81.195.173
- 40.119.147.105
- 159.65.113.205
- 89.31.78.25
- 52.209.158.57
- 34.255.51.222
- 54.229.254.21
- 52.213.125.100
- 52.50.84.159
- 52.31.208.124
- 52.48.246.2
- 151.11.251.108
- 109.68.26.86
- 54.246.172.171
- 52.215.27.44
- 52.18.0.64
- 99.80.6.39
- 54.228.39.217
- 34.247.223.243
- 109.68.24.219
- 52.17.142.196
- 52.31.137.103
- 52.50.105.114
- 52.101.73.11
- 195.103.103.95
- 54.171.27.201

Domain found

Below is the list of Domain found:

- s4c.altuoservizio.conad.it
- ilgrandeviaggio.conad.it
- mypass.conad.it
- s1a.altuoservizio.conad.it:195.103.103.67
- beneinsiemeoff.conad.it
- rtcconf.conad.it:151.11.251.83
- guidasocial.conad.it:guidasocial.conad.ditechonline.it
- ilgrandeviaggioinsieme.conad.it:109.68.26.116
- lyncdiscover.conad.it
- mobile.conad.it
- scontatievincenti.conad.it
- rosenthal.conad.it:109.68.24.219
- service.conad.it
- cambiaevinci.conad.it
- ilsaporedelleemozioni.conad.it:35.152.71.96
- supermercati.conad.it:217.29.160.31
- mail.conad.it
- chisiamo.conad.it:cdn.adobeaemcloud.com
- ilgrandeviaggioinsieme.conad.it:web.conad.ditechonline.it
- sport.conad.it:35.233.86.30
- digitalroom-test.conad.it
- chisiamo.conad.it:adobe-aem.map.fastly.net
- gepamweb.conad.it
- ilsaporedelleemozioni.conad.it:ilsaporedelleemozioni.leevia.com.
- wip.conad.it
- conadrad3.conad.it:151.11.251.89
- s3c.altuoservizio.conad.it:altuoservizio.spesainconad.it.
- beta.conad.it
- buonepratiche.conad.it:64:ff9b::a516:1413
- futuro.conad.it
- maestrideltaglio.conad.it
- iungo.conad.it
- s4c.altuoservizio.conad.it:altuoservizio.conadinunclick.it

- meet.conad.it
- vpn.conad.it
- o1.ptr9986.conad.it
- buonepratiche.conad.it
- lacasadeisogni.conad.it:40.68.184.232
- ilgrandeviaggio.conad.it:109.68.24.219
- guidasocialpetstore.conad.it:109.68.24.219
- s3c.altuoservizio.conad.it
- owa.conad.it
- scrittoridiclasse.conad.it
- altuoservizio.conad.it
- vincinatale.conad.it:52.16.137.238
- bonusbolletta.conad.it:52.16.137.238
- gustourevinci.conad.it:40.68.184.232
- kitchenaid.conad.it
- o1.ptr9986.conad.it:149.72.45.82
- apriamoleporte.conad.it
- s3c.altuoservizio.conad.it:altuoservizio.spesainconad.it
- tupperware.conad.it
- webkit.conad.it:80.211.62.104
- geodomino.conad.it
- s1b.altuoservizio.conad.it
- analytics.conad.it
- premiateelambiente.conad.it
- mipremio-pin.conad.it:54.220.186.7
- concorsoversonatura.conad.it
- mipremio.conad.it:52.157.89.4
- s2c.altuoservizio.conad.it:altuoservizio.conadacasa.it
- clubfamiglia.conad.it
- inostriori.conad.it:212.35.217.197
- author.conad.it
- conadrad1.conad.it
- concorsoversonatura.conad.it:15.161.61.5
- 2Fchisiamo.conad.it
- amicocalendario.conad.it
- staging.conad.it

- backupinsiemeperlascuola.conad.it
- portale.conad.it
- sport.conad.it
- vincinatale.conad.it
- 60evinci.conad.it
- scopriversonatura.conad.it
- festeggiamoinsieme.conad.it
- insiemeperlascuola.conad.it
- guidasocial.conad.it:109.68.24.221
- viaggi.conad.it
- ilsaporedelleemozioni.conad.it:15.160.39.142
- ilgrandeviaggio.conad.it:web.conad.ditechonline.it.
- sip.conad.it
- ilgrandeviaggio.conad.it:web.conad.ditechonline.it
- mipremio-pin.conad.it:46.137.117.50
- smtp2.conad.it:151.13.145.172
- sip.conad.it:sipdir.online.lync.com.
- *.conad.it
- conadrad1.conad.it:88.48.254.216
- travel-346f43f22d2d.conad.it
- sip.conad.it:sipdir.online.lync.com
- s1b.altuoservizio.conad.it:195.103.103.95
- webkit.conad.it
- sslvpn.conad.it
- smtp.conad.it
- fileuploader.conad.it
- digitalroom.conad.it:185.127.134.97
- guidasocialspazio.conad.it
- smtp.conad.it:151.11.251.70
- conad.it
- mipremio.conad.it
- s4c.altuoservizio.conad.it:altuoservizio.conadinunclick.it.
- beneinsieme.conad.it
- tms.conad.it
- ilsaporedelleemozioni.conad.it:ilsaporedelleemozioni.leevia.com
- app.conad.it

- s2c.altuoservizio.conad.it
- s1c.altuoservizio.conad.it
- sftp.conad.it
- dialin.conad.it
- digitalroom.conad.it
- amicocalendario.conad.it:40.68.184.232
- tsgateway.conad.it:88.48.254.200
- insiemeperlascuola.conad.it:193.240.211.109
- chisiamo.conad.it
- pim.conad.it
- s5c.altuoservizio.conad.it
- volantini.conad.it
- conadrad3.conad.it
- altuoservizio.conad.it:109.68.24.219
- smtp2.conad.it
- gustourevinci.conad.it
- leclercdrive.conad.it
- ilsaporedelleemozioni.conad.it
- s1a.altuoservizio.conad.it
- admin.conad.it
- mipremio-pin.conad.it
- webapps.conad.it
- amicheperlapelle.conad.it
- apriamoleporte.conad.it:62.101.80.232
- supermercati.conad.it
- altuoservizio.conad.it:109.68.26.92
- guidasocialpetstore.conad.it:guidasocial.conad.ditechonline.it
- ilgrandeviaggioinsieme.conad.it
- buonepratiche.conad.it:165.22.20.19
- chisiamo.conad.it:cdn.adobeaemcloud.com.
- guidasocialpetstore.conad.it:guidasocial.conad.ditechonline.it.
- amicheperlapelle.conad.it:109.168.115.125
- digitalroom-test.conad.it:128.65.125.180
- rtc.conad.it
- s1d.altuoservizio.conad.it
- ilsaporedelleemozioni.conad.it:15.161.70.98

- smart.conad.it
- ilsaporedelleemozioni.conad.it:a393b781b9aef4e6da7752bfa21e858b-484e20c8e231fcb2.elb.eu-south-1.amazonaws.com
- tsgateway.conad.it
- insiemeperlascuola.conad.it:213.171.166.88
- clubfamiglia.conad.it:52.16.137.238
- lyncweb.conad.it
- prodotti.conad.it
- beta.conad.it:109.68.24.219
- backupinsiemeperlascuola.conad.it:193.240.211.109
- inostriori.conad.it
- secure.conad.it
- spesaonline.conad.it
- s2c.altuoservizio.conad.it:altuoservizio.conadacasa.it.
- crm.conad.it
- editor.conad.it
- guidasocial.conad.it
- newsletter.conad.it
- bonusbolletta.conad.it
- concorso.11paralleli.conad.it
- my.conad.it
- rtcconf.conad.it
- s1d.altuoservizio.conad.it:195.103.103.97
- tsgateway.conad.it:con-tsgateway-prd.trafficmanager.net
- rtc.conad.it:151.11.251.80
- invitoaumbriajazz.conad.it
- lacasadeisogni.conad.it

URLs found

Below is the list of URLs found:

- www.conad.it
- secure.conad.it
- ilsaporedelleemozioni.conad.it
- ilgrandeviaggioinsieme.conad.it
- www.conad.it
- www.conad.it

- webapps.conad.it
- dialin.conad.it
- gepamweb.conad.it
- sftp.conad.it
- mypass.conad.it
- lyncweb.conad.it
- scontatievincenti.conad.it
- leclercdrive.conad.it
- www.conad.it
- wip.conad.it
- tsgateway.conad.it
- service.conad.it
- www.conad.it
- mipremio-pin.conad.it
- newsletter.conad.it
- my.conad.it
- rtcconf.conad.it
- s1a.altuoservizio.conad.it
- www.conad.it
- tupperware.conad.it
- tms.conad.it
- www.conad.it
- lacasadeisogni.conad.it
- prodotti.conad.it
- altuoservizio.conad.it
- portale.conad.it
- www.conad.it
- altuoservizio.conad.it
- lyncdiscover.conad.it
- staging.conad.it
- chisiamo.conad.it
- insiemeperlascuola.conad.it
- editor.conad.it
- smart.conad.it
- www.scopriversonatura.conad.it
- spesaonline.conad.it

- futuro.conad.it
- meet.conad.it
- crm.conad.it
- pim.conad.it
- www.newsletter.conad.it
- rtc.conad.it
- supermercati.conad.it
- mipremio.conad.it
- www.conad.it
- sslvpn.conad.it
- fileuploader.conad.it
- gustourevinci.conad.it
- VPN.conad.it
- my.conad.it
- iungo.conad.it
- guidasocial.conad.it
- dao.prepagataconad.it
- spesaonline.conad.it

Emails found

Below is the list of Emails found:

- jane.doe@conad.it
- janedoe@conad.it
- dpo@conad.it
- jdoe@conad.it

Resolved Hosts

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

- **admin.conad.it** : 109.68.26.86
- **altuoservizio.conad.it** : 109.68.26.92
- **amicheperlapelle.conad.it** : 109.168.115.125
- **amicocalendario.conad.it** : 40.68.184.232
- **analytics.conad.it** : 63.140.62.222
- **apriamoleporte.conad.it** : 62.101.80.232
- **backupinsiemeperlascuola.conad.it** : 193.240.211.109
- **bonusbolletta.conad.it** : 52.16.137.238

- **buonepratiche.conad.it** : 165.22.20.19
- **chisiamo.conad.it** : 146.75.55.10
- **clubfamiglia.conad.it** : 52.16.137.238
- **conad.it** : 151.101.131.10
- **conadrad1.conad.it** : 88.48.254.216
- **conadrad3.conad.it** : 151.11.251.89
- **concorsoversonatura.conad.it** : 15.161.61.5
- **crm.conad.it** : 40.119.147.105
- **digitalroom-test.conad.it** : 128.65.125.180
- **digitalroom.conad.it** : 185.127.134.97
- **editor.conad.it** : 109.68.26.91
- **fileuploader.conad.it** : 151.11.251.107
- **futuro.conad.it** : 146.75.55.10
- **gepamweb.conad.it** : 151.11.251.115
- **guidasocial.conad.it** : 109.68.26.113
- **guidasocialpetstore.conad.it** : 109.68.26.113
- **guidasocialspazio.conad.it** : 109.68.26.113
- **gustourevinci.conad.it** : 40.68.184.232
- **ilgrandeviaggio.conad.it** : 109.68.26.97
- **ilgrandeviaggioinsieme.conad.it** : 109.68.26.97
- **ilsaporedelleemozioni.conad.it** : 15.160.39.142
- **inostriori.conad.it** : 212.35.217.197
- **insiemeperlascuola.conad.it** : 213.171.166.88
- **iungo.conad.it** : 151.11.251.125
- **lacasadeisogni.conad.it** : 40.68.184.232
- **maestrideltaglio.conad.it** : 77.39.208.226
- **mipremio-pin.conad.it** : 54.220.186.7
- **mipremio.conad.it** : 52.157.89.4
- **my.conad.it** : 146.75.55.10
- **o1.ptr9986.conad.it** : 149.72.45.82
- **pim.conad.it** : 146.75.55.10
- **portale.conad.it** : 151.11.251.114
- **premiateelambiente.conad.it** : 77.39.208.224
- **prodotti.conad.it** : 217.29.160.31
- **s1a.altuoservizio.conad.it** : 195.103.103.67
- **s1b.altuoservizio.conad.it** : 195.103.103.95

- **s1c.altuoservizio.conad.it** : 195.103.103.92
- **s1d.altuoservizio.conad.it** : 195.103.103.97
- **scontatievincenti.conad.it** : 40.68.184.232
- **service.conad.it** : 109.68.26.91
- **spesaonline.conad.it** : 146.75.55.10
- **sport.conad.it** : 35.233.86.30
- **sslvpn.conad.it** : 151.11.251.101
- **supermercati.conad.it** : 217.29.160.31
- **tms.conad.it** : 109.68.26.105
- **travel-346f43f22d2d.conad.it** : 116.203.32.52
- **tsgateway.conad.it** : 151.11.251.108
- **viaggi.conad.it** : 116.203.32.52
- **vincinatale.conad.it** : 52.16.137.238
- **volantini.conad.it** : 34.247.223.243
- **webapps.conad.it** : 151.11.251.118
- **webkit.conad.it** : 80.211.62.104

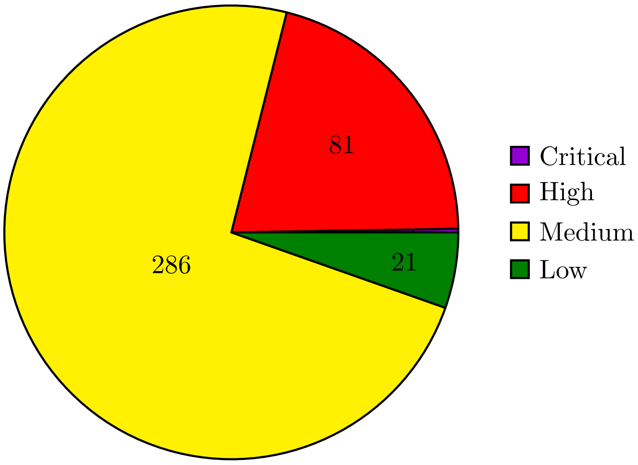
Server Mail found

Below is the list of Server Mail found:

- 52.101.73.22
- 52.101.68.3
- 52.101.73.11
- conad-it.mail.protection.outlook.com.
- 52.101.68.18

Pie Chart of Vulnerabilities

Pie chart showing the distribution of vulnerabilities for the domain `conad.it`:



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
212.35.217.197	1	0	6	1
80.211.62.104	0	22	94	8
54.220.186.7	0	16	20	0
52.16.137.238	0	12	30	4
109.168.115.125	0	11	60	5
34.252.201.201	0	10	33	3
63.33.34.226	0	6	6	0
54.171.29.175	0	2	2	0
213.171.166.88	0	2	1	0
52.31.208.124	0	0	10	0
34.240.71.165	0	0	6	0
185.127.134.97	0	0	6	0
52.211.9.207	0	0	4	0
52.210.69.61	0	0	3	0
52.211.37.138	0	0	3	0
151.11.251.108	0	0	1	0
151.11.251.115	0	0	1	0
54.194.42.165	0	0	0	0
52.18.0.64	0	0	0	0
52.101.68.10	0	0	0	0
52.18.240.201	0	0	0	0
52.50.84.159	0	0	0	0
52.101.68.16	0	0	0	0
151.101.195.10	0	0	0	0
52.48.201.30	0	0	0	0
52.213.201.198	0	0	0	0
54.78.116.130	0	0	0	0
52.50.88.161	0	0	0	0
54.76.88.210	0	0	0	0
34.250.105.197	0	0	0	0
52.213.192.243	0	0	0	0
79.125.61.213	0	0	0	0
109.68.26.86	0	0	0	0
34.242.149.90	0	0	0	0
52.49.3.128	0	0	0	0
116.203.32.52	0	0	0	0
63.140.62.27	0	0	0	0
109.68.26.97	0	0	0	0
165.22.20.19	0	0	0	0
54.170.100.107	0	0	0	0
34.254.16.163	0	0	0	0
52.101.73.26	0	0	0	0
52.210.221.125	0	0	0	0
54.72.34.250	0	0	0	0
35.233.86.30	0	0	0	0
95.216.54.125	0	0	0	0
46.51.207.138	0	0	0	0
35.152.71.96	0	0	0	0
52.215.27.44	0	0	0	0
54.220.187.182	0	0	0	0

IP Address	Critical	High	Medium	Low
151.101.131.10	0	0	0	0
99.81.195.173	0	0	0	0
52.51.238.226	0	0	0	0
99.80.6.39	0	0	0	0
34.250.129.210	0	0	0	0
52.210.230.161	0	0	0	0
54.78.157.58	0	0	0	0
54.220.116.192	0	0	0	0
3.127.103.86	0	0	0	0
52.31.137.103	0	0	0	0
63.32.7.7	0	0	0	0
52.210.127.205	0	0	0	0
52.213.125.100	0	0	0	0
151.0.185.49	0	0	0	0
3.248.134.241	0	0	0	0
63.32.160.121	0	0	0	0
217.29.160.31	0	0	0	0
151.101.67.10	0	0	0	0
52.101.68.36	0	0	0	0
81.24.236.129	0	0	0	0
159.65.113.205	0	0	0	0
109.68.24.219	0	0	0	0
193.240.211.109	0	0	0	0
146.75.55.10	0	0	0	0
151.101.3.10	0	0	0	0
151.11.251.101	0	0	0	0

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

Shodan Results for IP Addresses

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

IP Address: 54.194.42.165

- **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**: AWS ELB
  - **Port**: 80
  - **Version**: 2.0
  - **Location**: https://54.194.42.165:443/

No vulnerabilities found for this IP address.

IP Address: 52.18.0.64

- **Organization**: Amazon Data Services Ireland Limited
- **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.

IP Address: 151.11.251.108

- **Organization**: CONAD NAZIONALE
- **Operating System**: Windows
- **Critical Vulnerabilities**: 0
- **High Vulnerabilities**: 0
- **Medium Vulnerabilities**: 1
- **Low Vulnerabilities**: 0
- **Total Vulnerabilities**: 1

Services Running on IP Address

- **Service**: N/A
  - **Port**: 80
  - **Version**: N/A
  - **Location**: https://151.11.251.108/
- **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."`

IP Address: 52.101.68.10

- **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.

IP Address: 52.18.240.201

- **Organization**: Amazon Data Services Ireland Limited
- **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://52.18.240.201:443/

No vulnerabilities found for this IP address.

IP Address: 52.50.84.159

- **Organization**: Amazon Data Services Ireland Limited
- **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://52.50.84.159:443/
- **Service**: N/A
  - **Port**: 443
  - **Version**: N/A
  - **Location**: /

No vulnerabilities found for this IP address.

IP Address: 52.101.68.16

- **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.

IP Address: 34.252.201.201

- **Organization**: Amazon Data Services Ireland Limited
- **Operating System**: N/A
- **Critical Vulnerabilities**: 0
- **High Vulnerabilities**: 10
- **Medium Vulnerabilities**: 33
- **Low Vulnerabilities**: 3
- **Total Vulnerabilities**: 46

Services Running on IP Address

- **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-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-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-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.

IP Address: 151.11.251.115

- **Organization**: CONAD NAZIONALE
- **Operating System**: Windows
- **Critical Vulnerabilities**: 0
- **High Vulnerabilities**: 0
- **Medium Vulnerabilities**: 1
- **Low Vulnerabilities**: 0
- **Total Vulnerabilities**: 1

Services Running on IP Address

- **Service**: N/A
  - **Port**: 80
  - **Version**: N/A
  - **Location**: https://151.11.251.115/GePAMWeb/
- **Service**: Microsoft IIS httpd
  - **Port**: 443
  - **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."`

IP Address: 109.168.115.125

- **Organization**: EDP SRL
- **Operating System**: N/A
- **Critical Vulnerabilities**: 0
- **High Vulnerabilities**: 11
- **Medium Vulnerabilities**: 60
- **Low Vulnerabilities**: 5
- **Total Vulnerabilities**: 76

Services Running on IP Address

- **Service**: Apache httpd
  - **Port**: 80
  - **Version**: 2.4.7
  - **Location**: /
- **Service**: N/A
  - **Port**: 8008
  - **Version**: N/A
  - **Location**: https://109.168.115.125:8015/

Vulnerabilities Found

- **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-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-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-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-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-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-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-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-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-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-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-2013-4365
  - **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-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-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-2022-28330
  - **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-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-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-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-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-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-2013-5704

  - **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-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-2019-17567
  - **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-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-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-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-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-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-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-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-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-2020-11985
  - **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-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-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-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-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-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-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-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-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-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.

IP Address: 151.101.195.10

- **Organization**: Fastly, 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.daikin.se/
- **Service**: N/A
  - **Port**: 443
  - **Version**: N/A
  - **Location**: http://uhceservices-stgcloud.optum.com/en/prelogin

No vulnerabilities found for this IP address.

IP Address: 212.35.217.197

- **Organization**: SEEWEB s.r.l.
- **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**: Pure-FTPd
  - **Port**: 21
  - **Version**: N/A
  - **Location**:
- **Service**: OpenSSH
  - **Port**: 22
  - **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.

IP Address: 52.48.201.30

- **Organization**: Amazon Data Services Ireland Limited
- **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://52.48.201.30:443/

No vulnerabilities found for this IP address.

IP Address: 52.213.201.198

- **Organization**: Amazon Data Services Ireland Limited
- **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**: Metabase
  - **Port**: 443
  - **Version**: N/A
  - **Location**: /
- **Service**: N/A
  - **Port**: 8000
  - **Version**: N/A
  - **Location**:

No vulnerabilities found for this IP address.

IP Address: 54.78.116.130

- **Organization**: Amazon Data Services Ireland Limited
- **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://54.78.116.130

No vulnerabilities found for this IP address.

IP Address: 52.211.9.207

- **Organization**: Amazon Data Services Ireland Limited
- **Operating System**: N/A
- **Critical Vulnerabilities**: 0
- **High Vulnerabilities**: 0
- **Medium Vulnerabilities**: 4
- **Low Vulnerabilities**: 0
- **Total Vulnerabilities**: 4

Services Running on IP Address

- **Service**: AWS ELB
  - **Port**: 80
  - **Version**: 2.0
  - **Location**: https://52.211.9.207:443/

Vulnerabilities Found

- **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-2018-14040
  - **CVSS Score**: 4.3
  - **Description**: `In Bootstrap before 4.1.2, XSS is possible in the collapse data-parent attribute.`
- **Vulnerability**: CVE-2018-14041
  - **CVSS Score**: 4.3
  - **Description**: `In Bootstrap before 4.1.2, XSS is possible in the data-target property of scrollspy.`
- **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.`

IP Address: 52.50.88.161

- **Organization**: Amazon Data Services Ireland Limited
- **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://52.50.88.161:443/

No vulnerabilities found for this IP address.

IP Address: 54.76.88.210

- **Organization**: Amazon Technologies 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**: /

No vulnerabilities found for this IP address.

IP Address: 34.250.105.197

- **Organization**: Amazon Data Services Ireland Limited
- **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://34.250.105.197:443/

No vulnerabilities found for this IP address.

IP Address: 52.31.208.124

- **Organization**: Amazon Data Services Ireland Limited
- **Operating System**: N/A
- **Critical Vulnerabilities**: 0
- **High Vulnerabilities**: 0
- **Medium Vulnerabilities**: 10
- **Low Vulnerabilities**: 0
- **Total Vulnerabilities**: 10

Services Running on IP Address

- **Service**: N/A
  - **Port**: 443
  - **Version**: N/A
  - **Location**: /

Vulnerabilities Found

- **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.`

IP Address: 52.213.192.243

- **Organization**: Amazon Data Services Ireland Limited
- **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://52.213.192.243:443/

No vulnerabilities found for this IP address.

IP Address: 79.125.61.213

- **Organization**: Amazon Data Services Ireland Ltd
- **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://79.125.61.213:443/

No vulnerabilities found for this IP address.

IP Address: 109.68.26.86

- **Organization**: TEKNE S.R.L.
- **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://109.68.26.86/
- **Service**: N/A
  - **Port**: 443
  - **Version**: N/A
  - **Location**: /

No vulnerabilities found for this IP address.

IP Address: 34.242.149.90

- **Organization**: Amazon Data Services Ireland Limited
- **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**: /

No vulnerabilities found for this IP address.

IP Address: 52.49.3.128

- **Organization**: Amazon Data Services Ireland Limited
- **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://52.49.3.128:443/

No vulnerabilities found for this IP address.

IP Address: 116.203.32.52

- **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**: nginx
  - **Port**: 80
  - **Version**: N/A
  - **Location**: https://116.203.32.52/
- **Service**: nginx
  - **Port**: 443
  - **Version**: N/A
  - **Location**: /

No vulnerabilities found for this IP address.

IP Address: 54.171.29.175

- **Organization**: Amazon Technologies Inc.
- **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**: nginx
  - **Port**: 80
  - **Version**: N/A
  - **Location**: https://www.freeprintsapp.de
- **Service**: nginx
  - **Port**: 443
  - **Version**: N/A
  - **Location**: https://54.171.29.175/error

Vulnerabilities Found

- **Vulnerability**: CVE-2023-0568
  - **CVSS Score**: N/A
  - **Description**: In PHP 8.0.X before 8.0.28, 8.1.X before 8.1.16 and 8.2.X before 8.2.3, core path resolution function allocate buffer one byte too small. When resolving paths with lengths close to system MAXPATHLEN setting, this may lead to the byte after the allocated buffer being overwritten with NUL value, which might lead to unauthorized data access or modification.
- **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-2023-0662
  - **CVSS Score**: N/A
  - **Description**: In PHP 8.0.X before 8.0.28, 8.1.X before 8.1.16 and 8.2.X before 8.2.3, excessive number of parts in HTTP form upload can cause high resource consumption and excessive number of log entries. This can cause denial of service on the affected server by exhausting CPU resources or disk space.
- **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-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-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-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-2024-5585
  - **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-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-2023-0567
  - **CVSS Score**: N/A
  - **Description**: In PHP 8.0.X before 8.0.28, 8.1.X before 8.1.16 and 8.2.X before 8.2.3, password_verify() function may accept some invalid Blowfish hashes as valid. If such invalid hash ever ends up in the password database, it may lead to an application allowing any password for this entry as valid.

- **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-2023-0568
  - **CVSS Score**: N/A
  - **Description**: In PHP 8.0.X before 8.0.28, 8.1.X before 8.1.16 and 8.2.X before 8.2.3, core path resolution function allocate buffer one byte too small. When resolving paths with lengths close to system MAXPATHLEN setting, this may lead to the byte after the allocated buffer being overwritten with NUL value, which might lead to unauthorized data access or modification.

- **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-2023-0662
  - **CVSS Score**: N/A
  - **Description**: In PHP 8.0.X before 8.0.28, 8.1.X before 8.1.16 and 8.2.X before 8.2.3, excessive number of parts in HTTP form upload can cause high resource consumption and excessive number of log entries. This can cause denial of service on the affected server by exhausting CPU resources or disk space.
- **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-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-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-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-2024-5585
  - **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-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-2023-0567
  - **CVSS Score**: N/A
  - **Description**: In PHP 8.0.X before 8.0.28, 8.1.X before 8.1.16 and 8.2.X before 8.2.3, password_verify() function may accept some invalid Blowfish hashes as valid. If such invalid hash ever ends up in the password database, it may lead to an application allowing any password for this entry as valid.
- **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.

IP Address: 63.140.62.27

- **Organization**: Adobe 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.

IP Address: 109.68.26.97

- **Organization**: TEKNE S.R.L.
- **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.

IP Address: 165.22.20.19

- **Organization**: DigitalOcean, LLC
- **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**: 7.9p1 Debian 10+deb10u4
  - **Location**:

No vulnerabilities found for this IP address.

IP Address: 54.170.100.107

- **Organization**: Amazon Technologies 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**: /

No vulnerabilities found for this IP address.

IP Address: 52.16.137.238

- **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**: 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 "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-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-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-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.

IP Address: 34.254.16.163

- **Organization**: Amazon Data Services Ireland Limited
- **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.

IP Address: 52.101.73.26

- **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.

IP Address: 52.210.221.125

- **Organization**: Amazon Data Services Ireland Limited
- **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.

IP Address: 54.220.186.7

- **Organization**: Amazon.com, Inc.
- **Operating System**: Ubuntu
- **Critical Vulnerabilities**: 0
- **High Vulnerabilities**: 16
- **Medium Vulnerabilities**: 20
- **Low Vulnerabilities**: 0
- **Total Vulnerabilities**: 36

Services Running on IP Address

- **Service**: nginx
  - **Port**: 80
  - **Version**: 1.14.0
  - **Location**: /
- **Service**: nginx
  - **Port**: 8000
  - **Version**: 1.14.0
  - **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-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-2018-16843
  - **CVSS Score**: 7.8
  - **Description**: nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive memory consumption. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.

- **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-2018-16844
  - **CVSS Score**: 7.8
  - **Description**: nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive CPU usage. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.

- **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-2018-16843
  - **CVSS Score**: 7.8
  - **Description**: nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive memory consumption. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.
- **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-2018-16844
  - **CVSS Score**: 7.8
  - **Description**: nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive CPU usage. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.

- **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-2018-16843
  - **CVSS Score**: 7.8
  - **Description**: nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive memory consumption. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.

- **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-2018-16844
  - **CVSS Score**: 7.8
  - **Description**: nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive CPU usage. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.
- **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-2018-16843
  - **CVSS Score**: 7.8
  - **Description**: `nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive memory consumption. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.`
- **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-2018-16844
  - **CVSS Score**: 7.8
  - **Description**: `nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive CPU usage. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.`
- **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.`

IP Address: 54.72.34.250

- **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**: 443
  - **Version**: N/A
  - **Location**: /

No vulnerabilities found for this IP address.

IP Address: 35.233.86.30

- **Organization**: Google LLC
- **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**: 9.2p1 Debian 2+deb12u3
  - **Location**:
- **Service**: nginx
  - **Port**: 80
  - **Version**: 1.22.1
  - **Location**: https://35.233.86.30/
- **Service**: nginx
  - **Port**: 443
  - **Version**: 1.22.1
  - **Location**: /

No vulnerabilities found for this IP address.

IP Address: 95.216.54.125

- **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**: Apache httpd
  - **Port**: 80
  - **Version**: N/A
  - **Location**: https://www.sec4u.co/

No vulnerabilities found for this IP address.

IP Address: 46.51.207.138

- **Organization**: Amazon Web Services, Elastic Compute Cloud, EC2, EU
- **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://46.51.207.138:443/

No vulnerabilities found for this IP address.

IP Address: 35.152.71.96

- **Organization**: Amazon Data Services Italy
- **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.

IP Address: 213.171.166.88

- **Organization**: SEEWEB s.r.l.
- **Operating System**: N/A
- **Critical Vulnerabilities**: 0
- **High Vulnerabilities**: 2
- **Medium Vulnerabilities**: 1
- **Low Vulnerabilities**: 0
- **Total Vulnerabilities**: 3

Services Running on IP Address

- **Service**: N/A
  - **Port**: 21
  - **Version**: N/A
  - **Location**:
- **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**: 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**: Postfix smtpd

  - **Port**: 587
  - **Version**: N/A
  - **Location**:

- **Service**: N/A
  - **Port**: 993
  - **Version**: N/A
  - **Location**:

- **Service**: N/A
  - **Port**: 995
  - **Version**: N/A
  - **Location**:

- **Service**: N/A
  - **Port**: 8443
  - **Version**: N/A
  - **Location**: /

- **Service**: N/A
  - **Port**: 8880
  - **Version**: N/A
  - **Location**:

Vulnerabilities Found

- **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-2022-37454
  - **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-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-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-2013-2220
  - **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-2007-3205
  - **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.

IP Address: 34.240.71.165

- **Organization**: Amazon Data Services Ireland Limited
- **Operating System**: N/A
- **Critical Vulnerabilities**: 0
- **High Vulnerabilities**: 0
- **Medium Vulnerabilities**: 6
- **Low Vulnerabilities**: 0
- **Total Vulnerabilities**: 6

Services Running on IP Address

- **Service**: nginx
  - **Port**: 80
  - **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-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-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-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.

IP Address: 52.210.69.61

- **Organization**: Amazon Data Services Ireland Limited
- **Operating System**: N/A
- **Critical Vulnerabilities**: 0
- **High Vulnerabilities**: 0
- **Medium Vulnerabilities**: 3
- **Low Vulnerabilities**: 0
- **Total Vulnerabilities**: 3

Services Running on IP Address

- **Service**: nginx
  - **Port**: 80
  - **Version**: 1.16.1
  - **Location**: /
- **Service**: Apache Tomcat
  - **Port**: 443
  - **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.
- **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.

IP Address: 52.215.27.44

- **Organization**: Amazon Data Services Ireland Limited
- **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.

IP Address: 63.33.34.226

- **Organization**: Amazon Data Services Ireland Limited
- **Operating System**: N/A
- **Critical Vulnerabilities**: 0
- **High Vulnerabilities**: 6
- **Medium Vulnerabilities**: 6
- **Low Vulnerabilities**: 0
- **Total Vulnerabilities**: 12

Services Running on IP Address

- **Service**: AWS ELB
  - **Port**: 80
  - **Version**: 2.0
  - **Location**: https://63.33.34.226:443/
- **Service**: nginx
  - **Port**: 443
  - **Version**: 1.13.10
  - **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-2018-16844
  - **CVSS Score**: 7.8
  - **Description**: nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive CPU usage. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.
- **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-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-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-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-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-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-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-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-2018-16843
  - **CVSS Score**: 7.8
  - **Description**: nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive memory consumption. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.

- **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-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-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.

IP Address: 54.220.187.182

- **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**: AWS ELB
  - **Port**: 80
  - **Version**: 2.0
  - **Location**: https://54.220.187.182:443/
- **Service**: N/A
  - **Port**: 443
  - **Version**: N/A
  - **Location**: /

No vulnerabilities found for this IP address.

IP Address: 151.101.131.10

- **Organization**: Fastly, 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.raiffeisen.al/
- **Service**: N/A
  - **Port**: 443
  - **Version**: N/A
  - **Location**: http://www.walgreenshealth.com/home

No vulnerabilities found for this IP address.

IP Address: 99.81.195.173

- **Organization**: Amazon Data Services Ireland Limited
- **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://denied.alfa.net/

No vulnerabilities found for this IP address.

IP Address: 52.51.238.226

- **Organization**: Amazon Data Services Ireland Limited
- **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**: 1.22.1
  - **Location**: /

No vulnerabilities found for this IP address.

IP Address: 99.80.6.39

- **Organization**: Amazon Data Services Ireland Limited
- **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**: /
- **Service**: AWS ELB
  - **Port**: 443
  - **Version**: 2.0
  - **Location**: /
- **Service**: N/A
  - **Port**: 8443
  - **Version**: N/A
  - **Location**:

No vulnerabilities found for this IP address.

IP Address: 34.250.129.210

- **Organization**: Amazon Data Services Ireland Limited
- **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://34.250.129.210:443/

No vulnerabilities found for this IP address.

IP Address: 80.211.62.104

- **Organization**: Aruba S.p.A. - Cloud Services DC1
- **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**: /

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-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-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-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-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-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-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-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-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-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-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-2022-22719
  - **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-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.

IP Address: 52.210.230.161

- **Organization**: Amazon Data Services Ireland Limited
- **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**: Microsoft IIS httpd
  - **Port**: 80
  - **Version**: 10.0
  - **Location**: https://52.210.230.161/
- **Service**: AWS ELB
  - **Port**: 443
  - **Version**: 2.0
  - **Location**: /

No vulnerabilities found for this IP address.

IP Address: 52.211.37.138

- **Organization**: Amazon Data Services Ireland Limited
- **Operating System**: N/A
- **Critical Vulnerabilities**: 0
- **High Vulnerabilities**: 0
- **Medium Vulnerabilities**: 3
- **Low Vulnerabilities**: 0
- **Total Vulnerabilities**: 3

Services Running on IP Address

- **Service**: nginx
  - **Port**: 443
  - **Version**: 1.16.1
  - **Location**: https://mazda-oauth-user-non-prod-eu-west-1.grade-x-ap.com/rest/oauth2/auth?client_id=e8a0f6

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-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.`

IP Address: 185.127.134.97

- **Organization**: ALL42 s.r.l.
- **Operating System**: N/A
- **Critical Vulnerabilities**: 0
- **High Vulnerabilities**: 0
- **Medium Vulnerabilities**: 6
- **Low Vulnerabilities**: 0
- **Total Vulnerabilities**: 6

Services Running on IP Address

- **Service**: OpenResty
  - **Port**: 80
  - **Version**: N/A
  - **Location**: /
- **Service**: OpenResty
  - **Port**: 443
  - **Version**: N/A
  - **Location**: /

Vulnerabilities Found

- **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-2018-14042
  - **CVSS Score**: 4.3
  - **Description**: `In Bootstrap before 4.1.2, XSS is possible in the data-container property of tooltip.`
- **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-2018-20676
  - **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.`

IP Address: 54.78.157.58

- **Organization**: Amazon Data Services Ireland Limited
- **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://54.78.157.58:443/
- **Service**: N/A
  - **Port**: 443
  - **Version**: N/A
  - **Location**: /

No vulnerabilities found for this IP address.

IP Address: 54.220.116.192

- **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**: AWS ELB
  - **Port**: 80
  - **Version**: 2.0
  - **Location**: https://dareboost.com:443/

No vulnerabilities found for this IP address.

IP Address: 3.127.103.86

- **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://3.127.103.86:443/

No vulnerabilities found for this IP address.

IP Address: 52.31.137.103

- **Organization**: Amazon Data Services Ireland Limited
- **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://52.31.137.103:443/

No vulnerabilities found for this IP address.

IP Address: 63.32.7.7

- **Organization**: Amazon Data Services Ireland Limited
- **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://63.32.7.7:443/

No vulnerabilities found for this IP address.

IP Address: 52.210.127.205

- **Organization**: Amazon Data Services Ireland Limited
- **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**: /

No vulnerabilities found for this IP address.

IP Address: 52.213.125.100

- **Organization**: Amazon Data Services Ireland Limited
- **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**: 22
  - **Version**: N/A
  - **Location**:

No vulnerabilities found for this IP address.

IP Address: 151.0.185.49

- **Organization**: Fastweb SpA
- **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://s5c.altuoservizio.conad.it/
- **Service**: Apache httpd
  - **Port**: 443
  - **Version**: N/A
  - **Location**: https://altuoservizio.conad.it

No vulnerabilities found for this IP address.

IP Address: 3.248.134.241

- **Organization**: Amazon Data Services Ireland Limited
- **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**: 22
  - **Version**: N/A
  - **Location**:

No vulnerabilities found for this IP address.

IP Address: 63.32.160.121

- **Organization**: Amazon Data Services Ireland Limited
- **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.

IP Address: 217.29.160.31

- **Organization**: SOFTEC SPA
- **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**: ProFTPD
  - **Port**: 21
  - **Version**: N/A
  - **Location**:
- **Service**: Apache httpd
  - **Port**: 80
  - **Version**: N/A
  - **Location**: /
- **Service**: Apache httpd
  - **Port**: 443
  - **Version**: N/A
  - **Location**:
- **Service**: Apache Tomcat/Coyote JSP engine
  - **Port**: 8080
  - **Version**: 1.1
  - **Location**: /

No vulnerabilities found for this IP address.

IP Address: 151.101.67.10

- **Organization**: Fastly, 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.raiffeisenleasing-kosovo.com/
- **Service**: N/A
  - **Port**: 443
  - **Version**: N/A
  - **Location**: http://assets.lixil.com/content/lixil-assets/jp/top.html

No vulnerabilities found for this IP address.

IP Address: 52.101.68.36

- **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.

IP Address: 81.24.236.129

- **Organization**: Datacenter services of Ifinet at Caldera site
- **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**: BigIP
  - **Port**: 80
  - **Version**: N/A
  - **Location**: https://81.24.236.129/
- **Service**: BigIP
  - **Port**: 443
  - **Version**: N/A
  - **Location**: https://deda.cloud

No vulnerabilities found for this IP address.

IP Address: 159.65.113.205

- **Organization**: DigitalOcean, LLC
- **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-3ubuntu0.4
  - **Location**:

No vulnerabilities found for this IP address.

IP Address: 109.68.24.219

- **Organization**: TEKNE S.R.L.
- **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.

IP Address: 193.240.211.109

- **Organization**: FRO2006079038DIR-994450/3
- **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.

IP Address: 146.75.55.10

- **Organization**: FASTLY
- **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.

IP Address: 151.101.3.10

- **Organization**: Fastly, 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://healthplanofnevada.com/
- **Service**: N/A
  - **Port**: 443
  - **Version**: N/A
  - **Location**: http://www.uhcfedretirees.com/

No vulnerabilities found for this IP address.

IP Address: 151.11.251.101

- **Organization**: CONAD NAZIONALE
- **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**: /
- **Service**: N/A
  - **Port**: 8443
  - **Version**: N/A
  - **Location**: /

No vulnerabilities found for this IP address.