Report for Domain: edison.it

Generated by Apollo

August 22, 2024

Summary of Findings

Below are some key statistics from the data provided:

- **Number of IPs**: 134
- **Number of Domains**: 206
- **Number of Emails**: 10
- **Number of Resolved Hosts**: 93
- **Number of Mail Servers**: 4
- **Number of URLs**: 59

IP Addresses found

Below is the list of IP addresses found:

- 108.138.192.7
- 52.51.233.170
- 3.120.219.35
- 95.174.28.207
- 18.245.86.74
- 51.15.59.206
- 212.239.76.156
- 137.135.246.66
- 204.246.191.9
- 151.22.39.125
- 185.91.71.118
- 54.192.76.24
- 13.32.27.63
- 3.127.90.246
- 0.0.0.0
- 34.248.167.34
- 151.22.39.122
- 18.66.139.99

- 62.94.137.200
- 195.103.103.30
- 52.49.152.75
- 35.156.181.89
- 99.86.159.110
- 108.138.26.35
- 52.97.232.200
- 2600:9000:2490:ac00:1b:9b8a:f480:93a1
- 156.54.148.62
- 151.22.39.38
- 108.157.194.117
- 151.22.39.9
- 151.22.38.214
- 151.22.38.130
- 52.49.89.252
- 3.121.156.227
- 51.91.24.51
- 213.92.46.9
- 40.126.32.136
- 65.9.66.8
- 108.138.192.101
- 2600:9000:2490:1200:1b:9b8a:f480:93a1
- 54.192.76.109
- 151.22.38.131
- 18.195.47.200
- 18.245.46.30
- 151.22.39.19
- 151.22.39.24
- 63.33.242.246
- 37.72.32.244
- 93.186.242.241
- 3.74.25.135
- 2600:9000:2490:c200:1b:9b8a:f480:93a1
- 151.22.38.175
- 40.87.138.215
- 195.231.62.154

- 3.64.96.148
- 204.246.191.51
- 3.65.111.227
- 212.73.193.150
- 151.22.38.133
- 3.125.77.225
- 204.246.191.8
- 99.84.224.213
- 62.94.137.182
- 18.66.192.87
- 151.22.38.198
- 99.86.159.64
- 109.168.22.85
- 52.50.23.25
- 151.22.38.252
- 40.126.32.66
- 151.22.39.27
- 108.138.192.108
- 18.173.233.124
- 151.22.38.14
- 20.190.159.2
- 52.85.132.76
- 40.126.32.131
- 54.192.76.55
- 212.35.216.126
- 52.211.124.234
- 13.74.182.99
- 151.101.65.195
- 37.72.32.254
- 3.160.212.120
- 40.126.32.74
- 54.192.76.85
- 18.173.205.109
- 3.64.78.167
- 89.197.73.20
- 37.72.32.255

- 2600:9000:2729:6c00:19:89bd:7b40:93a1
- 151.22.39.163
- 3.66.39.13
- 151.22.38.13
- 93.186.249.30
- 213.217.29.85
- 3.126.218.72
- 51.75.86.118
- 151.22.38.156
- 204.246.191.61
- 51.38.105.34
- 18.202.92.68
- 151.22.39.54
- 94.124.69.67
- 151.101.1.195
- 151.22.39.18
- 162.55.172.85
- 3.160.212.90
- 151.22.38.140
- 18.66.218.109
- 20.190.160.14
- 54.76.95.70
- 83.211.69.255
- 108.156.91.85
- 37.72.32.222
- 151.22.39.6
- 3.126.233.235
- 109.168.22.86
- 46.28.2.183
- 40.126.32.6
- 151.22.38.155
- 62.94.137.206
- 151.22.39.45
- 51.178.13.239
- 108.156.2.25
- 99.86.4.85

- 94.127.86.211
- 52.213.159.238
- 62.94.137.201
- 151.22.38.152
- 151.22.38.163
- 99.84.88.78
- 151.22.38.234
- 151.22.38.70

Domain found

Below is the list of Domain found:

- crm.free.edison.it
- fmw.edison.it
- tagmanager-dnf.edison.it
- extranet2010.edison.it
- gatewaymi.edison.it
- hubatoa.edison.it
- tagmanager-140.edison.it
- qlv.free.edison.it
- tagmanager.edison.it
- portaleproduttori2.edison.it
- hub.edison.it
- MI045WLC5508CED.corp.edison.it
- ty-dev.edison.it
- lync.edison.it
- edicerpiteas01.corp.edison.it
- cbc.corp.edison.it
- password-reset.edison.it
- portalesrm.edison.it
- documentali-synergy-synvendors.edison.it
- edison.it
- niceprod.edison.it
- portale.edison.it
- er.edison.it
- mi045wlc5508ced.corp.edison.it
- ocr.edison.it

- dev-resource-edisonmysun.edison.it
- iag.free.edison.it
- EDIREPPITEAS01.corp.edison.it
- edito-test-01.corp.edison.it
- areaclienti.prep.edison.it
- stonecert.edison.it
- vpnlondon.edison.it
- enterpriseregistration.corp.edison.it
- sso.edison.it
- bonus.edison.it
- tagmanager-frendy.edison.it
- desi.corp.edison.it
- monitoraggiomar-test.edison.it
- vpn-fornitori.edison.it
- etools2.edison.it
- enterpriseregistration.egypt.edison.it
- visitatori.edison.it
- hedgingportal.corp.edison.it
- ebidtest.corp.edison.it
- cbctest.corp.edison.it
- vireoxmobile.edison.it
- facilitysolutions.edison.it
- dep.edison.it
- authsaptest.edison.it
- thorprod.corp.edison.it
- EDICERPITEAS01.corp.edison.it
- adt-temp.edison.it
- phishingalert.edison.it
- elyx.edison.it
- etools1.edison.it
- ssl-eesm-ot.edison.it
- fgt.egypt.edison.it
- edisonmediacenter.edison.it
- fgt.Egypt.edison.it
- certauth.sso.edison.it
- *.edison.it

- uag.free.edison.it
- ssl.edison.it
- ediaw01.free.edison.it
- enterpriseregistration.fenice.edison.it
- documentale-ITG.edison.it
- qvmobiletest.corp.edison.it
- portaleproduttori-qa.edison.it
- escomas-qa.edison.it
- MI045ISE3305CED.corp.edison.it
- owebapp.edison.it
- admpowerpro.edison.it
- autodiscover.edison.it
- er-fa.edison.it
- enterpriseregistration.edison.it
- collaudo-dof.edison.it
- monitoraggiomar.edison.it
- lyncdiscover.edison.it
- edisonbrandcenter.edison.it
- cbc.edison.it
- vpnclientleonardo.edison.it
- cpq-service-qa.edison.it
- eas.edison.it
- ediprdalvcms01.corp.edison.it
- energybrain-efs.edison.it
- thorprep.corp.edison.it
- free.edison.it
- sip.edison.it
- edisonnextbrandcenter.edison.it
- editstpiteas01.corp.edison.it
- ema.edison.it
- stories.efficienzaenergetica.edison.it
- srm.edison.it
- outlook.corp.edison.it
- daemobile.edison.it
- consipsl3.edison.it
- dof.edison.it

- ty.edison.it
- efficienzaenergetica.edison.it
- sancarlo.edison.it
- lead-qa.edison.it
- documentali-pandora.edison.it
- pss.edison.it
- MI045ISE3305DR.corp.edison.it
- centraleterni.edison.it
- directorsdocuments.edison.it
- adt.edison.it
- 140anni.edison.it
- vpn.edison.it
- centralesimeri.edison.it
- da.edison.it
- collaudo-noi.edison.it
- dnf.edison.it
- cmor.edison.it
- crm.prep.edison.it
- chargeandgo.edison.it
- documentale-stoccaggio.edison.it
- comparatoreofferte.edison.it
- mi045ise3305dr.corp.edison.it
- smtppub.edison.it
- gateway.edison.it
- ediema01.corp.edison.it
- epm.edison.it
- pec.edison.it
- stone.edison.it
- legacy.edison.it
- corp.edison.it
- gdc.edison.it
- edoc.edison.it
- extranet.edison.it
- enefcampus.edison.it
- noi.edison.it
- segnalazioni.edison.it

- asid.edison.it
- editoowanl01.corp.edison.it
- vpnbackup.edison.it
- wicket.edison.it
- lead-prospect-qa.edison.it
- mdm.free.edison.it
- cbcmobile.edison.it
- powerprocert.edison.it
- mies2-lotto2.edison.it
- citrix.edison.it
- webcon.edison.it
- thortestatoa.edison.it
- desitest.corp.edison.it
- commission-qa.edison.it
- iotprosumer-b2b-dev.edison.it
- elp.edison.it
- gatewayfr.edison.it
- ediema.edison.it
- er-ta.edison.it
- ediweb.edison.it
- crmee.edison.it
- wsnomitsrg.edison.it
- EDIPRDPITEAS01.corp.edison.it
- lyncws.edison.it
- softweb.edison.it
- open.edison.it
- ocr-test.edison.it
- av.edison.it
- dnf-qa.edison.it
- edireppiteas01.corp.edison.it
- gen-e.edison.it
- admpowerprocert.edison.it
- hubtest.edison.it
- stonesvil.edison.it
- cowprep.corp.edison.it
- ebid.corp.edison.it

- EDITSTPITEAS01.corp.edison.it
- teleriscaldamento.edison.it
- centraletorviscosa.edison.it
- spfk.edison.it
- trayport.edison.it
- dep2010.edison.it
- edisonfornature.edison.it
- indep2010.edison.it
- energiachecambiatutto.edison.it
- nicesvil.edison.it
- authsap.edison.it
- portaleproduttori.edison.it
- portaleproduttori1.edison.it
- ediprdpiteas01.corp.edison.it
- inge.edison.it
- wsnomitsrgtest.edison.it
- storage-hub.edison.it
- move.edison.it
- cpq-service.edison.it
- flooratrieste.edison.it
- olo2olo.edison.it
- email.edison.it
- indep.edison.it
- mi045ise3305ced.corp.edison.it
- ty-qa.edison.it
- documentale-itg.edison.it
- mi045wlc5508dr.corp.edison.it
- elearning.edison.it
- inwelldiary.edison.it
- erm.corp.edison.it
- mail.edison.it
- leonardo.edison.it
- hub.portal.edison.it
- powerpro.edison.it
- MI045WLC5508DR.corp.edison.it
- authsapdev.edison.it
- ediprdenras11.corp.edison.it

URLs found

Below is the list of URLs found:

- smtppub.edison.it
- wicket.edison.it
- adt-temp.edison.it
- centralesimeri.edison.it
- portaleproduttori-qa.edison.it
- gatewaymi.edison.it
- crm.free.edison.it
- portaleproduttori.edison.it
- tagmanager-dnf.edison.it
- documentali-pandora.edison.it
- flooratrieste.edison.it
- lead-qa.edison.it
- cpq-service.edison.it
- ty-dev.edison.it
- www.efficienzaenergetica.edison.it
- ediema.edison.it
- www.edison.it
- epm.edison.it
- ty-qa.edison.it
- er-fa.edison.it
- visitatori.edison.it
- dnf-qa.edison.it
- www.centralecandela.edison.it
- energybrain-efs.edison.it
- 140anni.edison.it
- ty.edison.it
- ocr-test.edison.it
- tagmanager-140.edison.it
- gatewayfr.edison.it
- storage-hub.edison.it
- vpnbackup.edison.it
- tagmanager.edison.it
- iotprosumer-b2b-dev.edison.it

- portale.edison.it:52000
- www.edison.it
- www.ediartasme.edison.it
- cpq-service-qa.edison.it
- dnf.edison.it
- lead-prospect-qa.edison.it
- sancarlo.edison.it
- er-fa.edison.it
- login.microsoftonline.com
- www.edison.it
- phishingalert.edison.it
- tagmanager-frendy.edison.it
- portale.edison.it:8050
- powerpro.edison.it
- commission-qa.edison.it
- dev-resource-edisonmysun.edison.it
- ocr.edison.it
- srm.edison.it
- gatewaymi.edison.it
- escomas-qa.edison.it
- centraleterni.edison.it
- documentali-synergy-synvendors.edison.it
- cbcmobile.edison.it
- cbc.edison.it
- er-fa.edison.it
- www.prep.edison.it

Emails found

Below is the list of Emails found:

- edison@pec.edison.it
- ufficiostampa@edison.it
- investor.relations@edison.it
- elena.distaso@edison.it
- allacci_subentri@edison.it
- edisonnext@pec.edison.it
- jane.doe@edison.it
- servizioclienti@edison.it
- cristina.parenti@edison.it
- '@edison.it

Resolved Hosts

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

- **140anni.edison.it** : 108.157.194.117
- **adt.edison.it** : 3.126.233.235
- **authsap.edison.it** : 3.64.78.167
- **authsapdev.edison.it** : 3.125.77.225
- **autodiscover.edison.it** : 52.97.232.200
- **cbc.edison.it** : 3.65.111.227
- **cbcmobile.edison.it** : 151.22.39.24
- **centralesimeri.edison.it** : 3.120.219.35
- **centraleterni.edison.it** : 35.156.181.89
- **centraletorviscosa.edison.it** : 3.126.233.235
- **chargeandgo.edison.it** : 109.168.22.86
- **commission-qa.edison.it** : 3.121.156.227
- **comparatoreofferte.edison.it** : 35.156.181.89
- **consipsl3.edison.it** : 156.54.148.62
- **cpq-service-qa.edison.it** : 3.121.156.227
- **cpq-service.edison.it** : 35.156.181.89
- **crm.free.edison.it** : 151.22.38.163
- **crm.prep.edison.it** : 151.22.38.152
- **crmee.edison.it** : 151.22.38.156
- **daemobile.edison.it** : 151.22.38.140
- **dev-resource-edisonmysun.edison.it** : 108.138.192.108
- **directorsdocuments.edison.it** : 40.87.138.215
- **dnf-qa.edison.it** : 18.66.218.109
- **dnf.edison.it** : 108.138.192.101
- **documentali-pandora.edison.it** : 3.66.39.13
- **documentali-synergy-synvendors.edison.it** : 3.65.111.227
- **ediema.edison.it** : 151.22.38.234
- **edison.it** : 51.75.86.118
- **edisonbrandcenter.edison.it** : 46.28.2.183
- **edisonfornature.edison.it** : 0.0.0.0
- **edisonmediacenter.edison.it** : 46.28.2.183
- **edisonnextbrandcenter.edison.it** : 46.28.2.183
- **efficienzaenergetica.edison.it** : 54.76.95.70

- **elearning.edison.it** : 94.124.69.67
- **elp.edison.it** : 35.156.181.89
- **ema.edison.it** : 3.120.219.35
- **enefcampus.edison.it** : 51.91.24.51
- **energybrain-efs.edison.it** : 151.22.39.125
- **enterpriseregistration.corp.edison.it** : 40.126.32.6
- **enterpriseregistration.edison.it** : 40.126.32.66
- **enterpriseregistration.fenice.edison.it** : 40.126.32.131
- **epm.edison.it** : 3.126.233.235
- **er-fa.edison.it** : 37.72.32.255
- **er-ta.edison.it** : 37.72.32.222
- **er.edison.it** : 37.72.32.254
- **escomas-qa.edison.it** : 108.156.2.25
- **flooratrieste.edison.it** : 3.126.233.235
- **fmw.edison.it** : 151.22.39.54
- **gateway.edison.it** : 151.22.38.133
- **gatewayfr.edison.it** : 3.127.90.246
- **gatewaymi.edison.it** : 151.22.38.252
- **gen-e.edison.it** : 93.186.242.241
- **iag.free.edison.it** : 151.22.38.70
- **iotprosumer-b2b-dev.edison.it** : 3.121.156.227
- **lead-prospect-qa.edison.it** : 3.121.156.227
- **lead-qa.edison.it** : 3.121.156.227
- **mail.edison.it** : 151.22.38.175
- **mies2-lotto2.edison.it** : 151.22.39.163
- **monitoraggiomar-test.edison.it** : 63.33.242.246
- **monitoraggiomar.edison.it** : 34.248.167.34
- **ocr-test.edison.it** : 3.121.156.227
- **ocr.edison.it** : 35.156.181.89
- **olo2olo.edison.it** : 3.120.219.35
- **open.edison.it** : 0.0.0.0
- **phishingalert.edison.it** : 99.86.159.110
- **portaleproduttori-qa.edison.it** : 99.86.159.64
- **portaleproduttori.edison.it** : 3.120.219.35
- **powerpro.edison.it** : 35.156.181.89
- **pss.edison.it** : 151.22.38.155

- **sancarlo.edison.it** : 151.22.39.163
- **segnalazioni.edison.it** : 95.174.28.207
- **smtppub.edison.it** : 151.22.38.131
- **srm.edison.it** : 213.92.46.9
- **ssl-eesm-ot.edison.it** : 151.22.39.122
- **ssl.edison.it** : 151.22.38.13
- **storage-hub.edison.it** : 3.64.96.148
- **stories.efficienzaenergetica.edison.it** : 151.101.1.195
- **tagmanager-140.edison.it** : 35.156.181.89
- **tagmanager-dnf.edison.it** : 3.126.233.235
- **tagmanager-frendy.edison.it** : 3.126.233.235
- **tagmanager.edison.it** : 3.120.219.35
- **ty-dev.edison.it** : 3.160.212.90
- **ty-qa.edison.it** : 108.138.192.7
- **ty.edison.it** : 3.160.212.120
- **vireoxmobile.edison.it** : 37.72.32.244
- **visitatori.edison.it** : 151.22.39.24
- **vpn-fornitori.edison.it** : 151.22.38.133
- **vpn.edison.it** : 151.22.38.14
- **vpnbackup.edison.it** : 212.239.76.156
- **vpnclientleonardo.edison.it** : 195.231.62.154
- **wicket.edison.it** : 3.120.219.35
- **wsnomitsrg.edison.it** : 3.74.25.135
- **wsnomitsrgtest.edison.it** : 18.195.47.200

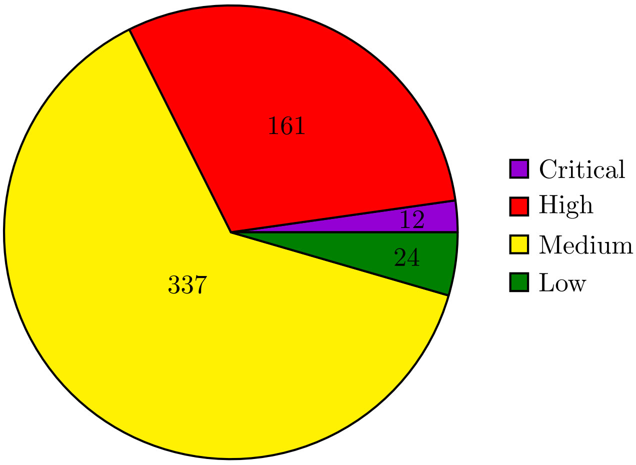
Server Mail found

Below is the list of Server Mail found:

- 213.217.29.85
- 185.91.71.118
- edison.esvacloud.com.
- edison2.esvacloud.com.

Pie Chart of Vulnerabilities

Pie chart showing the distribution of vulnerabilities for the domain `edison.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
156.54.148.62	10	98	121	4
151.22.39.163	2	4	20	2
109.168.22.85	0	27	73	4
54.76.95.70	0	26	106	10
212.35.216.126	0	6	14	4
109.168.22.86	0	0	3	0
151.22.39.24	0	0	0	0
3.65.111.227	0	0	0	0
3.127.90.246	0	0	0	0
62.94.137.206	0	0	0	0
3.64.78.167	0	0	0	0
52.49.89.252	0	0	0	0
95.174.28.207	0	0	0	0
151.22.38.133	0	0	0	0
93.186.242.241	0	0	0	0
62.94.137.182	0	0	0	0
52.50.23.25	0	0	0	0
151.101.65.195	0	0	0	0
37.72.32.255	0	0	0	0
213.217.29.85	0	0	0	0
3.126.233.235	0	0	0	0
3.66.39.13	0	0	0	0
52.211.124.234	0	0	0	0
35.156.181.89	0	0	0	0
94.124.69.67	0	0	0	0
151.22.39.125	0	0	0	0
52.98.242.232	0	0	0	0
3.121.156.227	0	0	0	0
151.22.39.122	0	0	0	0

IP Address	Critical	High	Medium	Low
151.101.1.195	0	0	0	0
46.28.2.183	0	0	0	0
3.120.219.35	0	0	0	0
3.125.77.225	0	0	0	0
51.178.13.239	0	0	0	0
3.126.218.72	0	0	0	0
18.202.92.68	0	0	0	0
89.197.73.20	0	0	0	0
3.127.119.45	0	0	0	0
62.94.137.201	0	0	0	0
151.22.38.13	0	0	0	0
185.91.71.118	0	0	0	0
52.49.152.75	0	0	0	0
151.22.38.14	0	0	0	0
151.22.38.252	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: 151.22.39.24

- Organization: edison
- 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://151.22.39.24/
- Service: N/A
  - Port: 443
  - Version: N/A
  - Location:

No vulnerabilities found for this IP address.

IP Address: 3.65.111.227

- Organization: A100 ROW GmbH
- Operating System: N/A
- Critical Vulnerabilities: 0
- High Vulnerabilities: 0
- Medium Vulnerabilities: 0
- Low Vulnerabilities: 0
- Total Vulnerabilities: 0

Services Running on IP Address

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

No vulnerabilities found for this IP address.

IP Address: 3.127.90.246

- 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: Apache httpd
  - Port: 443
  - Version: N/A
  - Location: /

No vulnerabilities found for this IP address.

IP Address: 62.94.137.206

- Organization: EDISON 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: N/A
  - Port: 179
  - Version: N/A
  - Location:

No vulnerabilities found for this IP address.

IP Address: 3.64.78.167

- Organization: A100 ROW GmbH
- Operating System: N/A
- Critical Vulnerabilities: 0
- High Vulnerabilities: 0
- Medium Vulnerabilities: 0
- Low Vulnerabilities: 0
- Total Vulnerabilities: 0

Services Running on IP Address

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

No vulnerabilities found for this IP address.

IP Address: 52.49.89.252

- 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://52.49.89.252:443/
- Service: AWS ELB
  - Port: 443
  - Version: 2.0
  - Location: /

No vulnerabilities found for this IP address.

IP Address: 95.174.28.207

- Organization: SEEWEB 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://segnalazioni.edison.it/
- Service: N/A
  - Port: 443
  - Version: N/A
  - Location: http://wpmmuemkjmory654metcd6ibxhtmsv5t7z2ybads7kdjwrzaedfjuoqd.onion/

No vulnerabilities found for this IP address.

IP Address: 151.22.38.133

- Organization: edison
- 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: 10443
  - Version: N/A
  - Location: /

No vulnerabilities found for this IP address.

IP Address: 93.186.242.241

- Organization: Aruba Business srl - Dedicated Servers
- 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://gen-e.edison.it/
- Service: nginx
  - Port: 443
  - Version: N/A
  - Location: http://www.gen-e.edison.it/

No vulnerabilities found for this IP address.

IP Address: 62.94.137.182

- Organization: EDF EN Service Italia
- 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: 179
  - Version: N/A
  - Location:

No vulnerabilities found for this IP address.

IP Address: 52.50.23.25

- 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: 151.101.65.195

- 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://haveyouseenthis.dog/
- Service: N/A
  - Port: 443
  - Version: N/A
  - Location: /

No vulnerabilities found for this IP address.

IP Address: 37.72.32.255

- Organization: Netalia DTC Milano
- Operating System: N/A
- Critical Vulnerabilities: 0
- High Vulnerabilities: 0
- Medium Vulnerabilities: 0
- Low Vulnerabilities: 0
- Total Vulnerabilities: 0

Services Running on IP Address

- Service: N/A
  - Port: 179
  - Version: N/A
  - Location:

No vulnerabilities found for this IP address.

IP Address: 213.217.29.85

- Organization: Libraesva srl
- 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: Postfix smtpd
  - Port: 25
  - Version: N/A
  - Location:
- Service: Apache httpd
  - Port: 80
  - Version: N/A
  - Location: https://213.217.29.85/
- Service: Postfix smtpd
  - Port: 465
  - Version: N/A
  - Location:
- Service: Postfix smtpd
  - Port: 587
  - Version: N/A
  - Location:

No vulnerabilities found for this IP address.

IP Address: 3.126.233.235

- Organization: A100 ROW GmbH
- Operating System: N/A
- Critical Vulnerabilities: 0
- High Vulnerabilities: 0
- Medium Vulnerabilities: 0
- Low Vulnerabilities: 0
- Total Vulnerabilities: 0

Services Running on IP Address

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

No vulnerabilities found for this IP address.

IP Address: 212.35.216.126

- Organization: SEEWEB s.r.l.
- Operating System: N/A
- Critical Vulnerabilities: 0
- High Vulnerabilities: 6
- Medium Vulnerabilities: 14
- Low Vulnerabilities: 4
- Total Vulnerabilities: 24

Services Running on IP Address

- Service: Apache httpd
  - Port: 80
  - Version: 2.4.57
  - Location: /

Vulnerabilities Found

- Vulnerability: CVE-2013-0941
  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.
- Vulnerability: CVE-2013-0942
  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
- Vulnerability: CVE-2012-4001
  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.
- Vulnerability: CVE-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-2013-2765
  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.
- Vulnerability: CVE-2011-1176
  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.
- Vulnerability: CVE-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-2011-2688
  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.
- Vulnerability: CVE-2009-0796
  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.
- Vulnerability: CVE-2023-43622

  - CVSS Score: N/A
  - Description: An attacker, opening a HTTP/2 connection with an initial window size of 0, was able to block handling of that connection indefinitely in Apache HTTP Server. This could be used to exhaust worker resources in the server, similar to the well known "slow loris" attack pattern.This has been fixed in version 2.4.58, so that such connection are terminated properly after the configured connection timeout.This issue affects Apache HTTP Server: from 2.4.55 through 2.4.57.Users are recommended to upgrade to version 2.4.58, which fixes the issue.

- Vulnerability: CVE-2007-4723
  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.
- Vulnerability: CVE-2024-40898
  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.
- Vulnerability: CVE-2013-4365
  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.
- Vulnerability: CVE-2012-3526
  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.
- Vulnerability: CVE-2012-4360
  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
- Vulnerability: CVE-2013-0941
  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2013-0942
  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
- Vulnerability: CVE-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-2012-4001
  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.
- Vulnerability: CVE-2011-1176
  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.
- Vulnerability: CVE-2023-45802
  - 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-2011-2688
  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.
- Vulnerability: CVE-2009-0796
  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.
- Vulnerability: CVE-2023-43622
  - CVSS Score: N/A
  - Description: An attacker, opening a HTTP/2 connection with an initial window size of 0, was able to block handling of that connection indefinitely in Apache HTTP Server. This could be used to exhaust worker resources in the server, similar to the well known "slow loris" attack pattern.This has been fixed in version 2.4.58, so that such connection are terminated properly after the configured connection timeout.This issue affects Apache HTTP Server: from 2.4.55 through 2.4.57.Users are recommended to upgrade to version 2.4.58, which fixes the issue.
- Vulnerability: CVE-2007-4723
  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.
- Vulnerability: CVE-2013-2765
  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.
- Vulnerability: CVE-2013-4365
  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.
- Vulnerability: CVE-2012-3526
  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2012-4360
  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

IP Address: 3.66.39.13

- Organization: A100 ROW GmbH
- Operating System: N/A
- Critical Vulnerabilities: 0
- High Vulnerabilities: 0
- Medium Vulnerabilities: 0
- Low Vulnerabilities: 0
- Total Vulnerabilities: 0

Services Running on IP Address

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

No vulnerabilities found for this IP address.

IP Address: 52.211.124.234

- 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: PostgreSQL
  - Port: 5432
  - Version: 9.6.0 or later
  - Location:

No vulnerabilities found for this IP address.

IP Address: 35.156.181.89

- Organization: A100 ROW GmbH
- Operating System: N/A
- Critical Vulnerabilities: 0
- High Vulnerabilities: 0
- Medium Vulnerabilities: 0
- Low Vulnerabilities: 0
- Total Vulnerabilities: 0

Services Running on IP Address

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

No vulnerabilities found for this IP address.

IP Address: 94.124.69.67

- Organization: MainStreaming S.p.A.
- Operating System: N/A
- Critical Vulnerabilities: 0
- High Vulnerabilities: 0
- Medium Vulnerabilities: 0
- Low Vulnerabilities: 0
- Total Vulnerabilities: 0

Services Running on IP Address

- Service: N/A
  - Port: 53
  - Version: N/A
  - Location:
- Service: N/A
  - Port: 53
  - Version: N/A
  - Location:
- Service: nginx
  - Port: 80
  - Version: N/A
  - Location: /
- Service: nginx
  - Port: 443
  - Version: N/A
  - Location: /

No vulnerabilities found for this IP address.

IP Address: 151.22.39.125

- Organization: edison
- 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: 52.98.242.232

- 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 IIS httpd
  - Port: 80
  - Version: 10.0
  - Location: https://52.98.242.232/owa/

No vulnerabilities found for this IP address.

IP Address: 3.121.156.227

- Organization: A100 ROW GmbH
- Operating System: N/A
- Critical Vulnerabilities: 0
- High Vulnerabilities: 0
- Medium Vulnerabilities: 0
- Low Vulnerabilities: 0
- Total Vulnerabilities: 0

Services Running on IP Address

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

No vulnerabilities found for this IP address.

IP Address: 54.76.95.70

- Organization: Amazon Technologies Inc.
- Operating System: Ubuntu
- Critical Vulnerabilities: 0
- High Vulnerabilities: 26
- Medium Vulnerabilities: 106
- Low Vulnerabilities: 10
- Total Vulnerabilities: 142

Services Running on IP Address

- Service: OpenSSH
  - Port: 22
  - Version: 7.2p2 Ubuntu 4ubuntu2.8
  - Location:
- Service: Apache httpd
  - Port: 80
  - Version: 2.4.18
  - Location: https://www.54.76.95.70/
- Service: Apache httpd
  - Port: 443
  - Version: 2.4.18
  - Location: https://www.54.76.95.70/

Vulnerabilities Found

- Vulnerability: CVE-2019-0220
  - CVSS Score: 5
  - Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.
- Vulnerability: CVE-2017-3169
  - CVSS Score: 7.5
  - Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.
- Vulnerability: CVE-2017-7679
  - CVSS Score: 7.5
  - Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.
- Vulnerability: CVE-2013-2765

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

- Vulnerability: CVE-2020-1934
  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.
- Vulnerability: CVE-2018-17189
  - CVSS Score: 5
  - Description: In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 (mod_http2) connections.
- Vulnerability: CVE-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-2017-9798
  - CVSS Score: 5
  - Description: Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.
- Vulnerability: CVE-2016-1546
  - CVSS Score: 4.3
  - Description: The Apache HTTP Server 2.4.17 and 2.4.18, when mod_http2 is enabled, does not limit the number of simultaneous stream workers for a single HTTP/2 connection, which allows remote attackers to cause a denial of service (stream-processing outage) via modified flow-control windows.
- Vulnerability: CVE-2022-29404
  - CVSS Score: 5

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

- Vulnerability: CVE-2021-33193
  - CVSS Score: 5
  - Description: A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.
- Vulnerability: CVE-2009-0796
  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.
- Vulnerability: CVE-2013-4365
  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.
- Vulnerability: CVE-2018-1333
  - CVSS Score: 5
  - Description: By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.18-2.4.30,2.4.33).
- Vulnerability: CVE-2022-22720
  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling
- Vulnerability: CVE-2018-11763
  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.17 to 2.4.34, by sending continuous, large SETTINGS frames a client can occupy a connection, server thread and CPU time without any connection timeout coming to effect. This affects only HTTP/2 connections. A possible mitigation is to not enable the h2 protocol.
- Vulnerability: CVE-2022-28330
  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.
- Vulnerability: CVE-2021-32791
  - CVSS Score: 4.3

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

- Vulnerability: CVE-2021-32792
  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using ‘OIDCPreservePost On‘.
- Vulnerability: CVE-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-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-2016-5387
  - CVSS Score: 6.8
  - Description: The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.
- Vulnerability: CVE-2012-4360
  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
- Vulnerability: CVE-2021-40438
  - CVSS Score: 6.8
  - Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.
- Vulnerability: CVE-2011-1176
  - CVSS Score: 4.3

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

- Vulnerability: CVE-2022-23943
  - CVSS Score: 7.5
  - Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.
- Vulnerability: CVE-2020-1927
  - CVSS Score: 5.8
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.
- Vulnerability: CVE-2018-17199
  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.
- Vulnerability: CVE-2017-9788
  - CVSS Score: 6.4
  - Description: In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.
- Vulnerability: CVE-2017-15710
  - CVSS Score: 5
  - Description: In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.
- Vulnerability: CVE-2016-4975
  - CVSS Score: 4.3

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

- Vulnerability: CVE-2018-1302
  - CVSS Score: 4.3
  - Description: When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.
- Vulnerability: CVE-2018-1303
  - CVSS Score: 5
  - Description: A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache. The vulnerability is considered as low risk since mod_cache_socache is not widely used, mod_cache_disk is not concerned by this vulnerability.
- Vulnerability: CVE-2017-3167
  - CVSS Score: 7.5
  - Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.
- Vulnerability: CVE-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-2021-44224
  - CVSS Score: 6.4
  - Description: A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).

- Vulnerability: CVE-2020-11985
  - CVSS Score: 4.3
  - Description: IP address spoofing when proxying using mod_remoteip and mod_rewrite For configurations using proxying with mod_remoteip and certain mod_rewrite rules, an attacker could spoof their IP address for logging and PHP scripts. Note this issue was fixed in Apache HTTP Server 2.4.24 but was retrospectively allocated a low severity CVE in 2020.

- Vulnerability: CVE-2021-44790
  - CVSS Score: 7.5
  - Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.
- Vulnerability: CVE-2013-0942
  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
- Vulnerability: CVE-2016-4979
  - CVSS Score: 5
  - Description: The Apache HTTP Server 2.4.18 through 2.4.20, when mod_http2 and mod_ssl are enabled, does not properly recognize the "SSLVerifyClient require" directive for HTTP/2 request authorization, which allows remote attackers to bypass intended access restrictions by leveraging the ability to send multiple requests over a single connection and aborting a renegotiation.
- Vulnerability: CVE-2012-3526
  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.
- Vulnerability: CVE-2018-1301
  - CVSS Score: 4.3
  - Description: A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.
- Vulnerability: CVE-2021-26690
  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service
- Vulnerability: CVE-2021-26691
  - CVSS Score: 7.5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow
- Vulnerability: CVE-2022-26377
  - CVSS Score: 5

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

- Vulnerability: CVE-2007-4723
  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.
- Vulnerability: CVE-2023-45802
  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.
- Vulnerability: CVE-2022-28614
  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.
- Vulnerability: CVE-2020-13938
  - CVSS Score: 2.1
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows
- Vulnerability: CVE-2018-1283
  - CVSS Score: 3.5
  - Description: In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to forward its session data to CGI applications (SessionEnv on, not the default), a remote user may influence their content by using a "Session" header. This comes from the "HTTP_SESSION" variable name used by mod_session to forward its data to CGIs, since the prefix "HTTP_" is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications.
- Vulnerability: CVE-2019-10082

  - CVSS Score: 6.4
  - Description: In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.

- Vulnerability: CVE-2018-1312
  - CVSS Score: 6.8
  - Description: In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.
- Vulnerability: CVE-2016-8740
  - CVSS Score: 5
  - Description: The mod_http2 module in the Apache HTTP Server 2.4.17 through 2.4.23, when the Protocols configuration includes h2 or h2c, does not restrict request-header length, which allows remote attackers to cause a denial of service (memory consumption) via crafted CONTINUATION frames in an HTTP/2 request.
- Vulnerability: CVE-2016-8743
  - CVSS Score: 5
  - Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.
- Vulnerability: CVE-2024-40898
  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.
- Vulnerability: CVE-2019-0217
  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.
- Vulnerability: CVE-2021-39275
  - CVSS Score: 7.5
  - Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.
- Vulnerability: CVE-2022-28615
  - CVSS Score: 6.4

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

- Vulnerability: CVE-2022-30556
  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.
- Vulnerability: CVE-2022-22719
  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.
- Vulnerability: CVE-2019-0220
  - CVSS Score: 5
  - Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.
- Vulnerability: CVE-2017-3169
  - CVSS Score: 7.5
  - Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.
- Vulnerability: CVE-2017-7679
  - CVSS Score: 7.5
  - Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.
- Vulnerability: CVE-2013-2765
  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.
- Vulnerability: CVE-2020-1934
  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.
- Vulnerability: CVE-2018-17189
  - CVSS Score: 5

  - Description: In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 (mod_http2) connections.

- Vulnerability: CVE-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-2017-9798
  - CVSS Score: 5
  - Description: Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.
- Vulnerability: CVE-2016-1546
  - CVSS Score: 4.3
  - Description: The Apache HTTP Server 2.4.17 and 2.4.18, when mod_http2 is enabled, does not limit the number of simultaneous stream workers for a single HTTP/2 connection, which allows remote attackers to cause a denial of service (stream-processing outage) via modified flow-control windows.
- Vulnerability: CVE-2022-29404
  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.
- Vulnerability: CVE-2021-33193
  - CVSS Score: 5
  - Description: A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.
- Vulnerability: CVE-2009-0796
  - CVSS Score: 2.6

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

- Vulnerability: CVE-2013-4365
  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.
- Vulnerability: CVE-2018-1333
  - CVSS Score: 5
  - Description: By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.18-2.4.30,2.4.33).
- Vulnerability: CVE-2022-22720
  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling
- Vulnerability: CVE-2018-11763
  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.17 to 2.4.34, by sending continuous, large SETTINGS frames a client can occupy a connection, server thread and CPU time without any connection timeout coming to effect. This affects only HTTP/2 connections. A possible mitigation is to not enable the h2 protocol.
- Vulnerability: CVE-2022-28330
  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.
- Vulnerability: CVE-2021-32791
  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.
- Vulnerability: CVE-2021-32792
  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.

- Vulnerability: CVE-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-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-2016-5387
  - CVSS Score: 6.8
  - Description: The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.
- Vulnerability: CVE-2012-4360
  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
- Vulnerability: CVE-2021-40438
  - CVSS Score: 6.8
  - Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.
- Vulnerability: CVE-2011-1176
  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.
- Vulnerability: CVE-2022-23943
  - CVSS Score: 7.5
  - Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.
- Vulnerability: CVE-2020-1927
  - CVSS Score: 5.8

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

- Vulnerability: CVE-2018-17199
  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.
- Vulnerability: CVE-2017-9788
  - CVSS Score: 6.4
  - Description: In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.
- Vulnerability: CVE-2017-15710
  - CVSS Score: 5
  - Description: In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.
- Vulnerability: CVE-2016-4975
  - CVSS Score: 4.3
  - Description: Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).
- Vulnerability: CVE-2018-1302
  - CVSS Score: 4.3
  - Description: When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.
- Vulnerability: CVE-2018-1303

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

- Vulnerability: CVE-2017-3167
  - CVSS Score: 7.5
  - Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.

- Vulnerability: CVE-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-2021-44224
  - CVSS Score: 6.4
  - Description: A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).
- Vulnerability: CVE-2020-11985
  - CVSS Score: 4.3
  - Description: IP address spoofing when proxying using mod_remoteip and mod_rewrite For configurations using proxying with mod_remoteip and certain mod_rewrite rules, an attacker could spoof their IP address for logging and PHP scripts. Note this issue was fixed in Apache HTTP Server 2.4.24 but was retrospectively allocated a low severity CVE in 2020.
- Vulnerability: CVE-2021-44790
  - CVSS Score: 7.5
  - Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.
- Vulnerability: CVE-2013-0942
  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
- Vulnerability: CVE-2016-4979

  - CVSS Score: 5
  - Description: The Apache HTTP Server 2.4.18 through 2.4.20, when mod_http2 and mod_ssl are enabled, does not properly recognize the "SSLVerifyClient require" directive for HTTP/2 request authorization, which allows remote attackers to bypass intended access restrictions by leveraging the ability to send multiple requests over a single connection and aborting a renegotiation.
- Vulnerability: CVE-2012-3526
  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.
- Vulnerability: CVE-2018-1301
  - CVSS Score: 4.3
  - Description: A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.
- Vulnerability: CVE-2021-26690
  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service
- Vulnerability: CVE-2021-26691
  - CVSS Score: 7.5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow
- Vulnerability: CVE-2022-26377
  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.
- Vulnerability: CVE-2007-4723
  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.
- Vulnerability: CVE-2023-45802
  - CVSS Score: N/A

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

- Vulnerability: CVE-2022-28614
  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.
- Vulnerability: CVE-2020-13938
  - CVSS Score: 2.1
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows
- Vulnerability: CVE-2018-1283
  - CVSS Score: 3.5
  - Description: In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to forward its session data to CGI applications (SessionEnv on, not the default), a remote user may influence their content by using a "Session" header. This comes from the "HTTP_SESSION" variable name used by mod_session to forward its data to CGIs, since the prefix "HTTP_" is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications.
- Vulnerability: CVE-2019-10082
  - CVSS Score: 6.4
  - Description: In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.
- Vulnerability: CVE-2018-1312
  - CVSS Score: 6.8
  - Description: In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.
- Vulnerability: CVE-2016-8740
  - CVSS Score: 5

  - Description: The mod_http2 module in the Apache HTTP Server 2.4.17 through 2.4.23, when the Protocols configuration includes h2 or h2c, does not restrict request-header length, which allows remote attackers to cause a denial of service (memory consumption) via crafted CONTINUATION frames in an HTTP/2 request.

- Vulnerability: CVE-2016-8743
  - CVSS Score: 5
  - Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.
- Vulnerability: CVE-2024-40898
  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.
- Vulnerability: CVE-2019-0217
  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.
- Vulnerability: CVE-2021-39275
  - CVSS Score: 7.5
  - Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.
- Vulnerability: CVE-2022-28615
  - CVSS Score: 6.4
  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.
- Vulnerability: CVE-2022-30556
  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.
- Vulnerability: CVE-2022-22719
  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

IP Address: 151.22.39.163

- Organization: edison
- Operating System: N/A
- Critical Vulnerabilities: 2
- High Vulnerabilities: 4
- Medium Vulnerabilities: 20
- Low Vulnerabilities: 2
- Total Vulnerabilities: 28

Services Running on IP Address

- Service: BigIP
  - Port: 80
  - Version: N/A
  - Location: https://151.22.39.163/
- Service: Apache httpd
  - Port: 443
  - Version: 2.4.53
  - Location: /

Vulnerabilities Found

- Vulnerability: CVE-2009-2299
  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.
- Vulnerability: CVE-2024-27316
  - CVSS Score: N/A
  - Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.
- Vulnerability: CVE-2013-2765
  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.
- Vulnerability: CVE-2022-36760
  - CVSS Score: N/A
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

- Vulnerability: CVE-2022-2097
  - CVSS Score: 5
  - Description: AES OCB mode for 32-bit x86 platforms using the AES-NI assembly optimised implementation will not encrypt the entirety of the data under some circumstances. This could reveal sixteen bytes of data that was preexisting in the memory that wasn't written. In the special case of "in place" encryption, sixteen bytes of the plaintext would be revealed. Since OpenSSL does not support OCB based cipher suites for TLS and DTLS, they are both unaffected. Fixed in OpenSSL 3.0.5 (Affected 3.0.0-3.0.4). Fixed in OpenSSL 1.1.1q (Affected 1.1.1-1.1.1p).
- Vulnerability: CVE-2023-27522
  - CVSS Score: N/A
  - Description: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.Special characters in the origin response header can truncate/split the response forwarded to the client.
- Vulnerability: CVE-2022-4304
  - CVSS Score: N/A
  - Description: A timing based side channel exists in the OpenSSL RSA Decryption implementationwhich could be sufficient to recover a plaintext across a network in aBleichenbacher style attack. To achieve a successful decryption an attackerwould have to be able to send a very large number of trial messages fordecryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5,RSA-OEAP and RSASVE.For example, in a TLS connection, RSA is commonly used by a client to send anencrypted pre-master secret to the server. An attacker that had observed agenuine connection between a client and a server could use this flaw to sendtrial messages to the server and record the time taken to process them. After asufficiently large number of messages the attacker could recover the pre-mastersecret used for the original connection and thus be able to decrypt theapplication data sent over that connection.
- Vulnerability: CVE-2013-4365
  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.
- Vulnerability: CVE-2009-1390
  - CVSS Score: 6.8
  - Description: Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2) GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS certificate in the chain is accepted instead of verifying the entire chain, which allows remote attackers to spoof trusted servers via a man-in-the-middle attack.
- Vulnerability: CVE-2022-28330
  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.
- Vulnerability: CVE-2023-5678

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

- Vulnerability: CVE-2022-2068
  - CVSS Score: 10
  - Description: In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze).
- Vulnerability: CVE-2009-3766
  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.16 and other versions before 1.5.19, when OpenSSL is used, does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.
- Vulnerability: CVE-2022-1292
  - CVSS Score: 10

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

- Vulnerability: CVE-2024-38474
  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.
- Vulnerability: CVE-2009-3765
  - CVSS Score: 6.8
  - Description: mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.
- Vulnerability: CVE-2019-0190
  - CVSS Score: 5
  - Description: A bug exists in the way mod_ssl handled client renegotiations. A remote attacker could send a carefully crafted request that would cause mod_ssl to enter a loop leading to a denial of service. This bug can be only triggered with Apache HTTP Server version 2.4.37 when using OpenSSL version 1.1.1 or later, due to an interaction in changes to handling of renegotiation attempts.
- Vulnerability: CVE-2022-30556
  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.
- Vulnerability: CVE-2006-20001
  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.
- Vulnerability: CVE-2009-0796
  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.

- Vulnerability: CVE-2024-0727
  - CVSS Score: N/A
  - Description: Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSLto crash leading to a potential Denial of Service attackImpact summary: Applications loading files in the PKCS12 format from untrustedsources might terminate abruptly.A file in PKCS12 format can contain certificates and keys and may come from anuntrusted source. The PKCS12 specification allows certain fields to be NULL, butOpenSSL does not correctly check for this case. This can lead to a NULL pointerdereference that results in OpenSSL crashing. If an application processes PKCS12files from an untrusted source using the OpenSSL APIs then that application willbe vulnerable to this issue.OpenSSL APIs that are vulnerable to this are: PKCS12_parse(),PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes()and PKCS12_newpass().We have also fixed a similar issue in SMIME_write_PKCS7(). However since thisfunction is related to writing data we do not consider it security significant.The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.
- Vulnerability: CVE-2023-0464
  - CVSS Score: N/A
  - Description: A security vulnerability has been identified in all supported versionsof OpenSSL related to the verification of X.509 certificate chainsthat include policy constraints. Attackers may be able to exploit thisvulnerability by creating a malicious certificate chain that triggersexponential use of computational resources, leading to a denial-of-service(DoS) attack on affected systems.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.
- Vulnerability: CVE-2023-0465
  - CVSS Score: N/A
  - Description: Applications that use a non-default option when verifying certificates may bevulnerable to an attack from a malicious CA to circumvent certain checks.Invalid certificate policies in leaf certificates are silently ignored byOpenSSL and other certificate policy checks are skipped for that certificate.A malicious CA could use this to deliberately assert invalid certificate policiesin order to circumvent policy checking on the certificate altogether.Policy processing is disabled by default but can be enabled by passingthe '-policy' argument to the command line utilities or by calling the'X509_VERIFY_PARAM_set1_policies()' function.
- Vulnerability: CVE-2023-0466
  - CVSS Score: N/A

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

- Vulnerability: CVE-2012-4001
  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.
- Vulnerability: CVE-2022-37436
  - CVSS Score: N/A
  - Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.
- Vulnerability: CVE-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-2022-31813
  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.
- Vulnerability: CVE-2024-38476
  - CVSS Score: N/A

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

- Vulnerability: CVE-2022-30522
  - CVSS Score: 5
  - Description: If Apache HTTP Server 2.4.53 is configured to do transformations with mod_sed in contexts where the input to mod_sed may be very large, mod_sed may make excessively large memory allocations and trigger an abort.

- Vulnerability: CVE-2022-4450
  - CVSS Score: N/A
  - Description: The function PEM_read_bio_ex() reads a PEM file from a BIO and parses anddecodes the "name" (e.g. "CERTIFICATE"), any header data and the payload data.If the function succeeds then the "name_out", "header" and "data" arguments arepopulated with pointers to buffers containing the relevant decoded data. Thecaller is responsible for freeing those buffers. It is possible to construct aPEM file that results in 0 bytes of payload data. In this case PEM_read_bio_ex()will return a failure code but will populate the header argument with a pointerto a buffer that has already been freed. If the caller also frees this bufferthen a double free will occur. This will most likely lead to a crash. Thiscould be exploited by an attacker who has the ability to supply malicious PEMfiles for parsing to achieve a denial of service attack.The functions PEM_read_bio() and PEM_read() are simple wrappers aroundPEM_read_bio_ex() and therefore these functions are also directly affected.These functions are also called indirectly by a number of other OpenSSLfunctions including PEM_X509_INFO_read_bio_ex() andSSL_CTX_use_serverinfo_file() which are also vulnerable. Some OpenSSL internaluses of these functions are not vulnerable because the caller does not free theheader argument if PEM_read_bio_ex() returns a failure code. These locationsinclude the PEM_read_bio_TYPE() functions as well as the decoders introduced inOpenSSL 3.0.The OpenSSL asn1parse command line application is also impacted by this issue.

- Vulnerability: CVE-2023-0286
  - CVSS Score: N/A
  - Description: There is a type confusion vulnerability relating to X.400 address processinginside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING butthe public structure definition for GENERAL_NAME incorrectly specified the typeof the x400Address field as ASN1_TYPE. This field is subsequently interpreted bythe OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than anASN1_STRING.When CRL checking is enabled (i.e. the application sets theX509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to passarbitrary pointers to a memcmp call, enabling them to read memory contents orenact a denial of service. In most cases, the attack requires the attacker toprovide both the certificate chain and CRL, neither of which need to have avalid signature. If the attacker only controls one of these inputs, the otherinput must already contain an X.400 address as a CRL distribution point, whichis uncommon. As such, this vulnerability is most likely to only affectapplications which have implemented their own functionality for retrieving CRLsover a network.

- Vulnerability: CVE-2023-3817
  - CVSS Score: N/A
  - Description: Issue summary: Checking excessively long DH keys or parameters may be very slow.Impact summary: Applications that use the functions DH_check(), DH_check_ex()or EVP_PKEY_param_check() to check a DH key or DH parameters may experience longdelays. Where the key or parameters that are being checked have been obtainedfrom an untrusted source this may lead to a Denial of Service.The function DH_check() performs various checks on DH parameters. After fixingCVE-2023-3446 it was discovered that a large q parameter value can also triggeran overly long computation during some of these checks. A correct q value,if present, cannot be larger than the modulus p parameter, thus it isunnecessary to perform these checks if q is larger than p.An application that calls DH_check() and supplies a key or parameters obtainedfrom an untrusted source could be vulnerable to a Denial of Service attack.The function DH_check() is itself called by a number of other OpenSSL functions.An application calling any of those other functions may similarly be affected.The other functions affected by this are DH_check_ex() andEVP_PKEY_param_check().Also vulnerable are the OpenSSL dhparam and pkeyparam command line applicationswhen using the "-check" option.The OpenSSL SSL/TLS implementation is not affected by this issue.The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.
- Vulnerability: CVE-2023-4807
  - CVSS Score: N/A

  - Description: Issue summary: The POLY1305 MAC (message authentication code) implementationcontains a bug that might corrupt the internal state of applications on theWindows 64 platform when running on newer X86_64 processors supporting theAVX512-IFMA instructions.Impact summary: If in an application that uses the OpenSSL library an attackercan influence whether the POLY1305 MAC algorithm is used, the applicationstate might be corrupted with various application dependent consequences.The POLY1305 MAC (message authentication code) implementation in OpenSSL doesnot save the contents of non-volatile XMM registers on Windows 64 platformwhen calculating the MAC of data larger than 64 bytes. Before returning tothe caller all the XMM registers are set to zero rather than restoring theirprevious content. The vulnerable code is used only on newer x86_64 processorssupporting the AVX512-IFMA instructions.The consequences of this kind of internal application state corruption canbe various - from no consequences, if the calling application does notdepend on the contents of non-volatile XMM registers at all, to the worstconsequences, where the attacker could get complete control of the applicationprocess. However given the contents of the registers are just zeroized sothe attacker cannot put arbitrary values inside, the most likely consequence,if any, would be an incorrect result of some application dependentcalculations or a crash leading to a denial of service.The POLY1305 MAC algorithm is most frequently used as part of theCHACHA20-POLY1305 AEAD (authenticated encryption with associated data)algorithm. The most common usage of this AEAD cipher is with TLS protocolversions 1.2 and 1.3 and a malicious client can influence whether this AEADcipher is used by the server. This implies that server applications usingOpenSSL can be potentially impacted. However we are currently not aware ofany concrete application that would be affected by this issue therefore weconsider this a Low severity security issue.As a workaround the AVX512-IFMA instructions support can be disabled atruntime by setting the environment variable OPENSSL_ia32cap: OPENSSL_ia32cap=:˜0x200000The FIPS provider is not affected by this issue.

- Vulnerability: CVE-2023-25690
  - CVSS Score: N/A
  - Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "/̂here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

- Vulnerability: CVE-2011-2688
  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.

- Vulnerability: CVE-2009-3767
  - CVSS Score: 4.3
  - Description: libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other versions, when OpenSSL is used, does not properly handle a '\{}0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.
- Vulnerability: CVE-2007-4723
  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.
- Vulnerability: CVE-2013-0941
  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.
- Vulnerability: CVE-2013-0942
  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
- Vulnerability: CVE-2024-38477
  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.
- Vulnerability: CVE-2022-26377
  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.
- Vulnerability: CVE-2023-45802
  - CVSS Score: N/A

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

- Vulnerability: CVE-2022-28614
  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.
- Vulnerability: CVE-2023-2650
  - CVSS Score: N/A

  - Description: Issue summary: Processing some specially crafted ASN.1 object identifiers ordata containing them may be very slow.Impact summary: Applications that use OBJ_obj2txt() directly, or use any ofthe OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no messagesize limit may experience notable to very long delays when processing thosemessages, which may lead to a Denial of Service.An OBJECT IDENTIFIER is composed of a series of numbers - sub-identifiers -most of which have no size limit. OBJ_obj2txt() may be used to translatean ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSLtype ASN1_OBJECT) to its canonical numeric text form, which are thesub-identifiers of the OBJECT IDENTIFIER in decimal form, separated byperiods.When one of the sub-identifiers in the OBJECT IDENTIFIER is very large(these are sizes that are seen as absurdly large, taking up tens or hundredsof KiBs), the translation to a decimal number in text may take a very longtime. The time complexity is O(n2̂) with 'n' being the size of thesub-identifiers in bytes (*).With OpenSSL 3.0, support to fetch cryptographic algorithms using names /identifiers in string form was introduced. This includes using OBJECTIDENTIFIERs in canonical numeric text form as identifiers for fetchingalgorithms.Such OBJECT IDENTIFIERs may be received through the ASN.1 structureAlgorithmIdentifier, which is commonly used in multiple protocols to specifywhat cryptographic algorithm should be used to sign or verify, encrypt ordecrypt, or digest passed data.Applications that call OBJ_obj2txt() directly with untrusted data areaffected, with any version of OpenSSL. If the use is for the mere purposeof display, the severity is considered low.In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME,CMS, CMP/CRMF or TS. It also impacts anything that processes X.509certificates, including simple things like verifying its signature.The impact on TLS is relatively low, because all versions of OpenSSL have a100KiB limit on the peer's certificate chain. Additionally, this onlyimpacts clients, or servers that have explicitly enabled clientauthentication.In OpenSSL 1.1.1 and 1.0.2, this only affects displaying diverse objects,such as X.509 certificates. This is assumed to not happen in such a waythat it would cause a Denial of Service, so these versions are considerednot affected by this issue in such a way that it would be cause for concern,and the severity is therefore considered low.

- Vulnerability: CVE-2023-0215

  - CVSS Score: N/A

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

- Vulnerability: CVE-2022-29404
  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.
- Vulnerability: CVE-2012-3526
  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.
- Vulnerability: CVE-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-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.

IP Address: 151.22.39.122

- Organization: edison
- 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: 151.101.1.195

- 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.kimscleaners.com/

No vulnerabilities found for this IP address.

IP Address: 109.168.22.85

- Organization: SEH SRL . - 6275212
- Operating System: Ubuntu
- Critical Vulnerabilities: 0
- High Vulnerabilities: 27
- Medium Vulnerabilities: 73
- Low Vulnerabilities: 4
- Total Vulnerabilities: 104

Services Running on IP Address

- Service: nginx
  - Port: 80
  - Version: 1.14.0
  - Location: https://demo-ricaricaev.seh.it/
- Service: nginx
  - Port: 443
  - Version: 1.14.0
  - Location: /
- Service: N/A
  - Port: 5060
  - Version: N/A
  - Location:
- Service: Apache httpd
  - Port: 8000
  - Version: 2.4.29
  - Location:
- Service: nginx
  - Port: 8080
  - Version: 1.14.0
  - Location: https://demo-ricaricaev.seh.it/
- Service: nginx
  - Port: 8443
  - 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-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-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-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-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-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-2020-11022
  - CVSS Score: 4.3
  - Description: In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
- Vulnerability: CVE-2020-11023
  - CVSS Score: 4.3
  - Description: In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
- Vulnerability: CVE-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-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-2021-39275
  - CVSS Score: 7.5
  - Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.
- Vulnerability: CVE-2022-28615
  - CVSS Score: 6.4
  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.
- Vulnerability: CVE-2022-30556
  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.
- Vulnerability: CVE-2022-22719
  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

- Vulnerability: CVE-2023-44487
  - 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-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-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-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-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-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-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: 46.28.2.183

- Organization: Serverplan network3
- Operating System: N/A
- Critical Vulnerabilities: 0
- High Vulnerabilities: 0
- Medium Vulnerabilities: 0
- Low Vulnerabilities: 0
- Total Vulnerabilities: 0

Services Running on IP Address

- Service: Apache httpd
  - Port: 443
  - Version: N/A
  - Location: /

No vulnerabilities found for this IP address.

IP Address: 3.120.219.35

- Organization: A100 ROW GmbH
- Operating System: N/A
- Critical Vulnerabilities: 0
- High Vulnerabilities: 0
- Medium Vulnerabilities: 0
- Low Vulnerabilities: 0
- Total Vulnerabilities: 0

Services Running on IP Address

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

No vulnerabilities found for this IP address.

IP Address: 3.125.77.225

- Organization: A100 ROW GmbH
- Operating System: N/A
- Critical Vulnerabilities: 0
- High Vulnerabilities: 0
- Medium Vulnerabilities: 0
- Low Vulnerabilities: 0
- Total Vulnerabilities: 0

Services Running on IP Address

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

No vulnerabilities found for this IP address.

IP Address: 51.178.13.239

- Organization: S.r.l. Bisy
- 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://51.178.13.239/
- Service: Apache httpd
  - Port: 443
  - Version: N/A
  - Location: /

No vulnerabilities found for this IP address.

IP Address: 109.168.22.86

- Organization: SEH SRL . - 6275212
- 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: 1.23.3
  - Location: https://ricaricaev.it/
- Service: nginx
  - Port: 443
  - Version: 1.23.3
  - Location: /

Vulnerabilities Found

- Vulnerability: CVE-2019-11358
  - CVSS Score: 4.3
  - Description: jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.
- Vulnerability: CVE-2020-11022
  - CVSS Score: 4.3
  - Description: In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
- Vulnerability: CVE-2020-11023
  - CVSS Score: 4.3
  - Description: In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

IP Address: 3.126.218.72

- 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: Apache httpd
  - Port: 443
  - Version: N/A
  - Location:

No vulnerabilities found for this IP address.

IP Address: 18.202.92.68

- 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://18.202.92.68:443/

No vulnerabilities found for this IP address.

IP Address: 89.197.73.20

- Organization: Virtual1 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: 5060
  - Version: N/A
  - Location:

No vulnerabilities found for this IP address.

IP Address: 3.127.119.45

- Organization: A100 ROW GmbH
- Operating System: N/A
- Critical Vulnerabilities: 0
- High Vulnerabilities: 0
- Medium Vulnerabilities: 0
- Low Vulnerabilities: 0
- Total Vulnerabilities: 0

Services Running on IP Address

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

No vulnerabilities found for this IP address.

IP Address: 156.54.148.62

- Organization: Telecom Italia S.p.A.
- Operating System: N/A
- Critical Vulnerabilities: 10
- High Vulnerabilities: 98
- Medium Vulnerabilities: 121
- Low Vulnerabilities: 4
- Total Vulnerabilities: 233

Services Running on IP Address

- Service: OpenSSH
  - Port: 22
  - Version: 7.2p2
  - Location:
- Service: nginx
  - Port: 80
  - Version: N/A
  - Location: /
- Service: nginx
  - Port: 443
  - Version: N/A
  - Location: /

Vulnerabilities Found

- Vulnerability: CVE-2018-10549
  - CVSS Score: 6.8
  - Description: An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. exif_read_data in ext/exif/exif.c has an out-of-bounds read for crafted JPEG data because exif_iif_add_value mishandles the case of a MakerNote that lacks a final '\{}0' character.
- Vulnerability: CVE-2018-10548
  - CVSS Score: 5
  - Description: An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. ext/ldap/ldap.c allows remote LDAP servers to cause a denial of service (NULL pointer dereference and application crash) because of mishandling of the ldap_get_dn return value.
- Vulnerability: CVE-2016-3141
  - CVSS Score: 7.5
  - Description: Use-after-free vulnerability in wddx.c in the WDDX extension in PHP before 5.5.33 and 5.6.x before 5.6.19 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact by triggering a wddx_deserialize call on XML data containing a crafted var element.

- Vulnerability: CVE-2018-10545
  - CVSS Score: 1.9
  - Description: An issue was discovered in PHP before 5.6.35, 7.0.x before 7.0.29, 7.1.x before 7.1.16, and 7.2.x before 7.2.4. Dumpable FPM child processes allow bypassing opcache access controls because fpm_unix.c makes a PR_SET_DUMPABLE prctl call, allowing one user (in a multiuser environment) to obtain sensitive information from the process memory of a second user's PHP applications by running gcore on the PID of the PHP-FPM worker process.
- Vulnerability: CVE-2018-10547
  - CVSS Score: 4.3
  - Description: An issue was discovered in ext/phar/phar_object.c in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. There is Reflected XSS on the PHAR 403 and 404 error pages via request data of a request for a .phar file. NOTE: this vulnerability exists because of an incomplete fix for CVE-2018-5712.
- Vulnerability: CVE-2018-10546
  - CVSS Score: 5
  - Description: An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. An infinite loop exists in ext/iconv/iconv.c because the iconv stream filter does not reject invalid multibyte sequences.
- Vulnerability: CVE-2017-7272
  - CVSS Score: 5.8
  - Description: PHP through 7.1.11 enables potential SSRF in applications that accept an fsockopen or pfsockopen hostname argument with an expectation that the port number is constrained. Because a :port syntax is recognized, fsockopen will use the port number that is specified in the hostname argument, instead of the port number in the second argument of the function.
- Vulnerability: CVE-2015-8387
  - CVSS Score: 7.5
  - Description: PCRE before 8.38 mishandles (?123) subroutine calls and related subroutine calls, which allows remote attackers to cause a denial of service (integer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.
- Vulnerability: CVE-2015-0232
  - CVSS Score: 6.8
  - Description: The exif_process_unicode function in ext/exif/exif.c in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free and application crash) via crafted EXIF data in a JPEG image.
- Vulnerability: CVE-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-2015-0235
  - CVSS Score: 10
  - Description: Heap-based buffer overflow in the __nss_hostname_digits_dots function in glibc 2.2, and other 2.x versions before 2.18, allows context-dependent attackers to execute arbitrary code via vectors related to the (1) gethostbyname or (2) gethostbyname2 function, aka "GHOST."
- Vulnerability: CVE-2016-3142
  - CVSS Score: 6.4
  - Description: The phar_parse_zipfile function in zip.c in the PHAR extension in PHP before 5.5.33 and 5.6.x before 5.6.19 allows remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read and application crash) by placing a PK\{}x05\{}x06 signature at an invalid location.
- Vulnerability: CVE-2014-5459
  - CVSS Score: 3.6
  - Description: The PEAR_REST class in REST.php in PEAR in PHP through 5.6.0 allows local users to write to arbitrary files via a symlink attack on a (1) rest.cachefile or (2) rest.cacheid file in /tmp/pear/cache/, related to the retrieveCacheFirst and useLocalCache functions.
- Vulnerability: CVE-2015-8835
  - CVSS Score: 7.5
  - Description: The make_http_soap_request function in ext/soap/php_http.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 does not properly retrieve keys, which allows remote attackers to cause a denial of service (NULL pointer dereference, type confusion, and application crash) or possibly execute arbitrary code via crafted serialized data representing a numerically indexed _cookies array, related to the SoapClient::__call method in ext/soap/soap.c.
- Vulnerability: CVE-2016-7418
  - CVSS Score: 5
  - Description: The php_wddx_push_element function in ext/wddx/wddx.c in PHP before 5.6.26 and 7.x before 7.0.11 allows remote attackers to cause a denial of service (invalid pointer access and out-of-bounds read) or possibly have unspecified other impact via an incorrect boolean element in a wddxPacket XML document, leading to mishandling in a wddx_deserialize call.
- Vulnerability: CVE-2016-7414
  - CVSS Score: 7.5
  - Description: The ZIP signature-verification feature in PHP before 5.6.26 and 7.x before 7.0.11 does not ensure that the uncompressed_filesize field is large enough, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via a crafted PHAR archive, related to ext/phar/util.c and ext/phar/zip.c.

- Vulnerability: CVE-2016-7416
  - CVSS Score: 5
  - Description: ext/intl/msgformat/msgformat_format.c in PHP before 5.6.26 and 7.x before 7.0.11 does not properly restrict the locale length provided to the Locale class in the ICU library, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a MessageFormatter::formatMessage call with a long first argument.
- Vulnerability: CVE-2016-7417
  - CVSS Score: 7.5
  - Description: ext/spl/spl_array.c in PHP before 5.6.26 and 7.x before 7.0.11 proceeds with SplArray unserialization without validating a return value and data type, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data.
- Vulnerability: CVE-2014-0185
  - CVSS Score: 7.2
  - Description: sapi/fpm/fpm/fpm_unix.c in the FastCGI Process Manager (FPM) in PHP before 5.4.28 and 5.5.x before 5.5.12 uses 0666 permissions for the UNIX socket, which allows local users to gain privileges via a crafted FastCGI client.
- Vulnerability: CVE-2016-7411
  - CVSS Score: 7.5
  - Description: ext/standard/var_unserializer.re in PHP before 5.6.26 mishandles object-deserialization failures, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via an unserialize call that references a partially constructed object.
- Vulnerability: CVE-2016-7412
  - CVSS Score: 6.8
  - Description: ext/mysqlnd/mysqlnd_wireprotocol.c in PHP before 5.6.26 and 7.x before 7.0.11 does not verify that a BIT field has the UNSIGNED_FLAG flag, which allows remote MySQL servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted field metadata.
- Vulnerability: CVE-2016-7413
  - CVSS Score: 7.5
  - Description: Use-after-free vulnerability in the wddx_stack_destroy function in ext/wddx/wddx.c in PHP before 5.6.26 and 7.x before 7.0.11 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a wddxPacket XML document that lacks an end-tag for a recordset field element, leading to mishandling in a wddx_deserialize call.
- Vulnerability: CVE-2015-6832
  - CVSS Score: 7.5
  - Description: Use-after-free vulnerability in the SPL unserialize implementation in ext/spl/spl_array.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 allows remote attackers to execute arbitrary code via crafted serialized data that triggers misuse of an array field.

- Vulnerability: CVE-2016-8670
  - CVSS Score: 7.5
  - Description: Integer signedness error in the dynamicGetbuf function in gd_io_dp.c in the GD Graphics Library (aka libgd) through 2.2.3, as used in PHP before 5.6.28 and 7.x before 7.0.13, allows remote attackers to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a crafted imagecreatefromstring call.
- Vulnerability: CVE-2015-8994
  - CVSS Score: 6.8
  - Description: An issue was discovered in PHP 5.x and 7.x, when the configuration uses apache2handler/mod_php or php-fpm with OpCache enabled. With 5.x after 5.6.28 or 7.x after 7.0.13, the issue is resolved in a non-default configuration with the opcache.validate_permission=1 setting. The vulnerability details are as follows. In PHP SAPIs where PHP interpreters share a common parent process, Zend OpCache creates a shared memory object owned by the common parent during initialization. Child PHP processes inherit the SHM descriptor, using it to cache and retrieve compiled script bytecode ("opcode" in PHP jargon). Cache keys vary depending on configuration, but filename is a central key component, and compiled opcode can generally be run if a script's filename is known or can be guessed. Many common shared-hosting configurations change EUID in child processes to enforce privilege separation among hosted users (for example using mod_ruid2 for the Apache HTTP Server, or php-fpm user settings). In these scenarios, the default Zend OpCache behavior defeats script file permissions by sharing a single SHM cache among all child PHP processes. PHP scripts often contain sensitive information: Think of CMS configurations where reading or running another user's script usually means gaining privileges to the CMS database.
- Vulnerability: CVE-2015-4148
  - CVSS Score: 5
  - Description: The do_soap_call function in ext/soap/soap.c in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 does not verify that the uri property is a string, which allows remote attackers to obtain sensitive information by providing crafted serialized data with an int data type, related to a "type confusion" issue.
- Vulnerability: CVE-2014-3587
  - CVSS Score: 4.3
  - Description: Integer overflow in the cdf_read_property_info function in cdf.c in file through 5.19, as used in the Fileinfo component in PHP before 5.4.32 and 5.5.x before 5.5.16, allows remote attackers to cause a denial of service (application crash) via a crafted CDF file. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1571.
- Vulnerability: CVE-2016-5773
  - CVSS Score: 7.5
  - Description: php_zip.c in the zip extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and application crash) via crafted serialized data containing a ZipArchive object.

- Vulnerability: CVE-2016-5772
  - CVSS Score: 7.5
  - Description: Double free vulnerability in the php_wddx_process_data function in wddx.c in the WDDX extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via crafted XML data that is mishandled in a wddx_deserialize call.
- Vulnerability: CVE-2016-5771
  - CVSS Score: 7.5
  - Description: spl_array.c in the SPL extension in PHP before 5.5.37 and 5.6.x before 5.6.23 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and application crash) via crafted serialized data.
- Vulnerability: CVE-2016-5770
  - CVSS Score: 7.5
  - Description: Integer overflow in the SplFileObject::fread function in spl_directory.c in the SPL extension in PHP before 5.5.37 and 5.6.x before 5.6.23 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large integer argument, a related issue to CVE-2016-5096.
- Vulnerability: CVE-2015-8935
  - CVSS Score: 4.3
  - Description: The sapi_header_op function in main/SAPI.c in PHP before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6 supports deprecated line folding without considering browser compatibility, which allows remote attackers to conduct cross-site scripting (XSS) attacks against Internet Explorer by leveraging (1) %0A%20 or (2) %0D%0A%20 mishandling in the header function.
- Vulnerability: CVE-2018-20783
  - CVSS Score: 5
  - Description: In PHP before 5.6.39, 7.x before 7.0.33, 7.1.x before 7.1.25, and 7.2.x before 7.2.13, a buffer over-read in PHAR reading functions may allow an attacker to read allocated or unallocated memory past the actual data when trying to parse a .phar file. This is related to phar_parse_pharfile in ext/phar/phar.c.
- Vulnerability: CVE-2015-4147
  - CVSS Score: 7.5
  - Description: The SoapClient::__call method in ext/soap/soap.c in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 does not verify that __default_headers is an array, which allows remote attackers to execute arbitrary code by providing crafted serialized data with an unexpected data type, related to a "type confusion" issue.
- Vulnerability: CVE-2016-5766
  - CVSS Score: 6.8

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

- Vulnerability: CVE-2015-2348
  - CVSS Score: 5
  - Description: The move_uploaded_file implementation in ext/standard/basic_functions.c in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 truncates a pathname upon encountering a \{}x00 character, which allows remote attackers to bypass intended extension restrictions and create files with unexpected names via a crafted second argument. NOTE: this vulnerability exists because of an incomplete fix for CVE-2006-7243.

- Vulnerability: CVE-2015-2305
  - CVSS Score: 6.8
  - Description: Integer overflow in the regcomp implementation in the Henry Spencer BSD regex library (aka rxspencer) alpha3.8.g5 on 32-bit platforms, as used in NetBSD through 6.1.5 and other products, might allow context-dependent attackers to execute arbitrary code via a large regular expression that leads to a heap-based buffer overflow.

- Vulnerability: CVE-2015-8838
  - CVSS Score: 4.3
  - Description: ext/mysqlnd/mysqlnd.c in PHP before 5.4.43, 5.5.x before 5.5.27, and 5.6.x before 5.6.11 uses a client SSL option to mean that SSL is optional, which allows man-in-the-middle attackers to spoof servers via a cleartext-downgrade attack, a related issue to CVE-2015-3152.

- Vulnerability: CVE-2016-4073
  - CVSS Score: 7.5
  - Description: Multiple integer overflows in the mbfl_strcut function in ext/mbstring/libmbfl/mbfl/mbfilter.c in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted mb_strcut call.

- Vulnerability: CVE-2016-4072
  - CVSS Score: 7.5
  - Description: The Phar extension in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 allows remote attackers to execute arbitrary code via a crafted filename, as demonstrated by mishandling of \{}0 characters by the phar_analyze_path function in ext/phar/phar.c.

- Vulnerability: CVE-2016-4071
  - CVSS Score: 7.5
  - Description: Format string vulnerability in the php_snmp_error function in ext/snmp/snmp.c in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 allows remote attackers to execute arbitrary code via format string specifiers in an SNMP::get call.

- Vulnerability: CVE-2016-4070
  - CVSS Score: 5

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

- Vulnerability: CVE-2015-4024
  - CVSS Score: 5
  - Description: Algorithmic complexity vulnerability in the multipart_buffer_headers function in main/rfc1867.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 allows remote attackers to cause a denial of service (CPU consumption) via crafted form data that triggers an improper order-of-growth outcome.
- Vulnerability: CVE-2018-14851
  - CVSS Score: 4.3
  - Description: exif_process_IFD_in_MAKERNOTE in ext/exif/exif.c in PHP before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted JPEG file.
- Vulnerability: CVE-2014-3538
  - CVSS Score: 5
  - Description: file before 5.19 does not properly restrict the amount of data read during a regex search, which allows remote attackers to cause a denial of service (CPU consumption) via a crafted file that triggers backtracking during processing of an awk rule. NOTE: this vulnerability exists because of an incomplete fix for CVE-2013-7345.
- Vulnerability: CVE-2015-0231
  - CVSS Score: 7.5
  - Description: Use-after-free vulnerability in the process_nested_data function in ext/standard/var_unserializer.re in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code via a crafted unserialize call that leverages improper handling of duplicate numerical keys within the serialized properties of an object. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-8142.
- Vulnerability: CVE-2015-2301
  - CVSS Score: 7.5
  - Description: Use-after-free vulnerability in the phar_rename_archive function in phar_object.c in PHP before 5.5.22 and 5.6.x before 5.6.6 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an attempted renaming of a Phar archive to the name of an existing file.
- 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-2013-6501

- CVSS Score: 4.6
- Description: The default soap.wsdl_cache_dir setting in (1) php.ini-production and (2) php.ini-development in PHP through 5.6.7 specifies the /tmp directory, which makes it easier for local users to conduct WSDL injection attacks by creating a file under /tmp with a predictable filename that is used by the get_sdl function in ext/soap/php_sdl.c.

- Vulnerability: CVE-2016-3074
  - CVSS Score: 7.5
  - Description: Integer signedness error in GD Graphics Library 2.1.1 (aka libgd or libgd2) allows remote attackers to cause a denial of service (crash) or potentially execute arbitrary code via crafted compressed gd2 data, which triggers a heap-based buffer overflow.
- 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-2014-2497
  - CVSS Score: 4.3
  - Description: The gdImageCreateFromXpm function in gdxpm.c in libgd, as used in PHP 5.4.26 and earlier, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted color table in an XPM file.
- Vulnerability: CVE-2014-3487
  - CVSS Score: 4.3
  - Description: The cdf_read_property_info function in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, does not properly validate a stream offset, which allows remote attackers to cause a denial of service (application crash) via a crafted CDF file.
- Vulnerability: CVE-2014-9426
  - CVSS Score: 7.5
  - Description: The apprentice_load function in libmagic/apprentice.c in the Fileinfo component in PHP through 5.6.4 attempts to perform a free operation on a stack-based character array, which allows remote attackers to cause a denial of service (memory corruption or application crash) or possibly have unspecified other impact via unknown vectors. NOTE: this is disputed by the vendor because the standard erealloc behavior makes the free operation unreachable
- Vulnerability: CVE-2018-5712
  - CVSS Score: 4.3
  - Description: An issue was discovered in PHP before 5.6.33, 7.0.x before 7.0.27, 7.1.x before 7.1.13, and 7.2.x before 7.2.1. There is Reflected XSS on the PHAR 404 error page via the URI of a request for a .phar file.
- Vulnerability: CVE-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-2016-5768
  - CVSS Score: 7.5
  - Description: Double free vulnerability in the _php_mb_regex_ereg_replace_exec function in php_mbregex.c in the mbstring extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) by leveraging a callback exception.

- Vulnerability: CVE-2016-5769
  - CVSS Score: 7.5
  - Description: Multiple integer overflows in mcrypt.c in the mcrypt extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 allow remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted length value, related to the (1) mcrypt_generic and (2) mdecrypt_generic functions.

- Vulnerability: CVE-2016-9137
  - CVSS Score: 7.5
  - Description: Use-after-free vulnerability in the CURLFile implementation in ext/curl/curl_file.c in PHP before 5.6.27 and 7.x before 7.0.12 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data that is mishandled during __wakeup processing.

- Vulnerability: CVE-2016-3185
  - CVSS Score: 6.4
  - Description: The make_http_soap_request function in ext/soap/php_http.c in PHP before 5.4.44, 5.5.x before 5.5.28, 5.6.x before 5.6.12, and 7.x before 7.0.4 allows remote attackers to obtain sensitive information from process memory or cause a denial of service (type confusion and application crash) via crafted serialized _cookies data, related to the SoapClient::__call method in ext/soap/soap.c.

- Vulnerability: CVE-2015-2787
  - CVSS Score: 7.5
  - Description: Use-after-free vulnerability in the process_nested_data function in ext/standard/var_unserializer.re in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 allows remote attackers to execute arbitrary code via a crafted unserialize call that leverages use of the unset function within an __wakeup function, a related issue to CVE-2015-0231.

- Vulnerability: CVE-2015-6831
  - CVSS Score: 7.5

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

- Vulnerability: CVE-2016-5116
  - CVSS Score: 6.4
  - Description: gd_xbm.c in the GD Graphics Library (aka libgd) before 2.2.0, as used in certain custom PHP 5.5.x configurations, allows context-dependent attackers to obtain sensitive information from process memory or cause a denial of service (stack-based buffer under-read and application crash) via a long name.
- Vulnerability: CVE-2015-6833
  - CVSS Score: 5
  - Description: Directory traversal vulnerability in the PharData class in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 allows remote attackers to write to arbitrary files via a .. (dot dot) in a ZIP archive entry that is mishandled during an extractTo call.
- Vulnerability: CVE-2015-6834
  - CVSS Score: 7.5
  - Description: Multiple use-after-free vulnerabilities in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 allow remote attackers to execute arbitrary code via vectors related to (1) the Serializable interface, (2) the SplObjectStorage class, and (3) the SplDoublyLinkedList class, which are mishandled during unserialization.
- Vulnerability: CVE-2015-6835
  - CVSS Score: 7.5
  - Description: The session deserializer in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 mishandles multiple php_var_unserialize calls, which allow remote attackers to execute arbitrary code or cause a denial of service (use-after-free) via crafted session content.
- Vulnerability: CVE-2015-6836
  - CVSS Score: 7.5
  - Description: The SoapClient __call method in ext/soap/soap.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 does not properly manage headers, which allows remote attackers to execute arbitrary code via crafted serialized data that triggers a "type confusion" in the serialize_function_call function.
- Vulnerability: CVE-2015-6837
  - CVSS Score: 5
  - Description: The xsl_ext_function_php function in ext/xsl/xsltprocessor.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13, when libxml2 before 2.9.2 is used, does not consider the possibility of a NULL valuePop return value before proceeding with a free operation during initial error checking, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted XML document, a different vulnerability than CVE-2015-6838.
- Vulnerability: CVE-2015-6838

- CVSS Score: 5
- Description: The xsl_ext_function_php function in ext/xsl/xsltprocessor.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13, when libxml2 before 2.9.2 is used, does not consider the possibility of a NULL valuePop return value before proceeding with a free operation after the principal argument loop, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted XML document, a different vulnerability than CVE-2015-6837.

- Vulnerability: CVE-2018-19520
  - CVSS Score: 6.5
  - Description: An issue was discovered in SDCMS 1.6 with PHP 5.x. app/admin/controller/themecontroller.php uses a check_bad function in an attempt to block certain PHP functions such as eval, but does not prevent use of preg_replace 'e' calls, allowing users to execute arbitrary code by leveraging access to admin template management.
- Vulnerability: CVE-2016-9934
  - CVSS Score: 5
  - Description: ext/wddx/wddx.c in PHP before 5.6.28 and 7.x before 7.0.13 allows remote attackers to cause a denial of service (NULL pointer dereference) via crafted serialized data in a wddxPacket XML document, as demonstrated by a PDORow string.
- Vulnerability: CVE-2016-7478
  - CVSS Score: 5
  - Description: Zend/zend_exceptions.c in PHP, possibly 5.x before 5.6.28 and 7.x before 7.0.13, allows remote attackers to cause a denial of service (infinite loop) via a crafted Exception object in serialized data, a related issue to CVE-2015-8876.
- Vulnerability: CVE-2017-7890
  - CVSS Score: 4.3
  - Description: The GIF decoding function gdImageCreateFromGifCtx in gd_gif_in.c in the GD Graphics Library (aka libgd), as used in PHP before 5.6.31 and 7.x before 7.1.7, does not zero colorMap arrays before use. A specially crafted GIF image could use the uninitialized tables to read ~700 bytes from the top of the stack, potentially disclosing sensitive information.
- Vulnerability: CVE-2017-11145
  - CVSS Score: 5
  - Description: In PHP before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7, an error in the date extension's timelib_meridian parsing code could be used by attackers able to supply date strings to leak information from the interpreter, related to ext/date/lib/parse_date.c out-of-bounds reads affecting the php_parse_date function. NOTE: the correct fix is in the e8b7698f5ee757ce2c8bd10a192a491a498f891c commit, not the bd77ac90d3bdf31ce2a5251ad92e9e75 gist.
- Vulnerability: CVE-2017-11144
  - CVSS Score: 5

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

- Vulnerability: CVE-2017-11147
  - CVSS Score: 6.4
  - Description: In PHP before 5.6.30 and 7.x before 7.0.15, the PHAR archive handler could be used by attackers supplying malicious archive files to crash the PHP interpreter or potentially disclose information due to a buffer over-read in the phar_parse_pharfile function in ext/phar/phar.c.
- Vulnerability: CVE-2015-3416
  - CVSS Score: 7.5
  - Description: The sqlite3VXPrintf function in printf.c in SQLite before 3.8.9 does not properly handle precision and width values during floating-point conversions, which allows context-dependent attackers to cause a denial of service (integer overflow and stack-based buffer overflow) or possibly have unspecified other impact via large integers in a crafted printf function call in a SELECT statement.
- Vulnerability: CVE-2015-3411
  - CVSS Score: 6.4
  - Description: PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 does not ensure that pathnames lack %00 sequences, which might allow remote attackers to read or write to arbitrary files via crafted input to an application that calls (1) a DOMDocument load method, (2) the xmlwriter_open_uri function, (3) the finfo_file function, or (4) the hash_hmac_file function, as demonstrated by a filename\{}0.xml attack that bypasses an intended configuration in which client users may read only .xml files.
- Vulnerability: CVE-2014-0207
  - CVSS Score: 4.3
  - Description: The cdf_read_short_sector function in cdf.c in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, allows remote attackers to cause a denial of service (assertion failure and application exit) via a crafted CDF file.
- Vulnerability: CVE-2018-17082
  - CVSS Score: 4.3
  - Description: The Apache2 component in PHP before 5.6.38, 7.0.x before 7.0.32, 7.1.x before 7.1.22, and 7.2.x before 7.2.10 allows XSS via the body of a "Transfer-Encoding: chunked" request, because the bucket brigade is mishandled in the php_handler function in sapi/apache2handler/sapi_apache2.c.
- Vulnerability: CVE-2019-9639
  - CVSS Score: 5
  - Description: An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_MAKERNOTE because of mishandling the data_len variable.

- Vulnerability: CVE-2019-9638
  - CVSS Score: 5
  - Description: An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_MAKERNOTE because of mishandling the maker_note->offset relationship to value_len.
- Vulnerability: CVE-2016-1903
  - CVSS Score: 6.4
  - Description: The gdImageRotateInterpolated function in ext/gd/libgd/gd_interpolation.c in PHP before 5.5.31, 5.6.x before 5.6.17, and 7.x before 7.0.2 allows remote attackers to obtain sensitive information or cause a denial of service (out-of-bounds read and application crash) via a large bgd_color argument to the imagerotate function.
- Vulnerability: CVE-2013-7456
  - CVSS Score: 6.8
  - Description: gd_interpolation.c in the GD Graphics Library (aka libgd) before 2.1.1, as used in PHP before 5.5.36, 5.6.x before 5.6.22, and 7.x before 7.0.7, allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted image that is mishandled by the imagescale function.
- Vulnerability: CVE-2015-0273
  - CVSS Score: 7.5
  - Description: Multiple use-after-free vulnerabilities in ext/date/php_date.c in PHP before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6 allow remote attackers to execute arbitrary code via crafted serialized input containing a (1) R or (2) r type specifier in (a) DateTimeZone data handled by the php_date_timezone_initialize_from_hash function or (b) DateTime data handled by the php_date_initialize_from_hash function.
- Vulnerability: CVE-2019-9637
  - CVSS Score: 5
  - Description: An issue was discovered in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. Due to the way rename() across filesystems is implemented, it is possible that file being renamed is briefly available with wrong permissions while the rename is ongoing, thus enabling unauthorized users to access the data.
- Vulnerability: CVE-2016-6289
  - CVSS Score: 6.8
  - Description: Integer overflow in the virtual_file_ex function in TSRM/tsrm_virtual_cwd.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a crafted extract operation on a ZIP archive.
- Vulnerability: CVE-2015-4602
  - CVSS Score: 10
  - Description: The __PHP_Incomplete_Class function in ext/standard/incomplete_class.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an unexpected data type, related to a "type confusion" issue.

- Vulnerability: CVE-2017-12868
  - CVSS Score: 7.5
  - Description: The secureCompare method in lib/SimpleSAML/Utils/Crypto.php in SimpleSAMLphp 1.14.13 and earlier, when used with PHP before 5.6, allows attackers to conduct session fixation attacks or possibly bypass authentication by leveraging missing character conversions before an XOR operation.
- Vulnerability: CVE-2015-4601
  - CVSS Score: 10
  - Description: PHP before 5.6.7 might allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an unexpected data type, related to "type confusion" issues in (1) ext/soap/php_encoding.c, (2) ext/soap/php_http.c, and (3) ext/soap/soap.c, a different issue than CVE-2015-4600.
- Vulnerability: CVE-2015-4600
  - CVSS Score: 10
  - Description: The SoapClient implementation in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an unexpected data type, related to "type confusion" issues in the (1) SoapClient::__getLastRequest, (2) SoapClient::__getLastResponse, (3) SoapClient::__getLastRequestHeaders, (4) SoapClient::__getLastResponseHeaders, (5) SoapClient::__getCookies, and (6) SoapClient::__setCookie methods.
- Vulnerability: CVE-2015-4603
  - CVSS Score: 10
  - Description: The exception::getTraceAsString function in Zend/zend_exceptions.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to execute arbitrary code via an unexpected data type, related to a "type confusion" issue.
- Vulnerability: CVE-2018-14883
  - CVSS Score: 5
  - Description: An issue was discovered in PHP before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8. An Integer Overflow leads to a heap-based buffer over-read in exif_thumbnail_extract of exif.c.
- Vulnerability: CVE-2015-4605
  - CVSS Score: 5
  - Description: The mcopy function in softmagic.c in file 5.x, as used in the Fileinfo component in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8, does not properly restrict a certain offset value, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted string that is mishandled by a "Python script text executable" rule.
- Vulnerability: CVE-2015-4604
  - CVSS Score: 5

  - Description: The mget function in softmagic.c in file 5.x, as used in the Fileinfo component in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8, does not properly maintain a certain pointer relationship, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted string that is mishandled by a "Python script text executable" rule.

- Vulnerability: CVE-2014-3597
  - CVSS Score: 6.8
  - Description: Multiple buffer overflows in the php_parserr function in ext/standard/dns.c in PHP before 5.4.32 and 5.5.x before 5.5.16 allow remote DNS servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted DNS record, related to the dns_get_record function and the dn_expand function. NOTE: this issue exists because of an incomplete fix for CVE-2014-4049.
- Vulnerability: CVE-2014-4670
  - CVSS Score: 4.6
  - Description: Use-after-free vulnerability in ext/spl/spl_dllist.c in the SPL component in PHP through 5.5.14 allows context-dependent attackers to cause a denial of service or possibly have unspecified other impact via crafted iterator usage within applications in certain web-hosting environments.
- Vulnerability: CVE-2014-9912
  - CVSS Score: 7.5
  - Description: The get_icu_disp_value_src_php function in ext/intl/locale/locale_methods.c in PHP before 5.3.29, 5.4.x before 5.4.30, and 5.5.x before 5.5.14 does not properly restrict calls to the ICU uresbund.cpp component, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a locale_get_display_name call with a long first argument.
- Vulnerability: CVE-2014-0237
  - CVSS Score: 5
  - Description: The cdf_unpack_summary_info function in cdf.c in the Fileinfo component in PHP before 5.4.29 and 5.5.x before 5.5.13 allows remote attackers to cause a denial of service (performance degradation) by triggering many file_printf calls.
- Vulnerability: CVE-2016-5093
  - CVSS Score: 7.5
  - Description: The get_icu_value_internal function in ext/intl/locale/locale_methods.c in PHP before 5.5.36, 5.6.x before 5.6.22, and 7.x before 7.0.7 does not ensure the presence of a ’\{}0’ character, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted locale_get_primary_language call.
- Vulnerability: CVE-2014-4049
  - CVSS Score: 5.1
  - Description: Heap-based buffer overflow in the php_parserr function in ext/standard/dns.c in PHP 5.6.0beta4 and earlier allows remote servers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted DNS TXT record, related to the dns_get_record function.

- Vulnerability: CVE-2015-8394
  - CVSS Score: 7.5
  - Description: PCRE before 8.38 mishandles the (?(<digits>) and (?(R<digits>) conditions, which allows remote attackers to cause a denial of service (integer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.
- Vulnerability: CVE-2016-5096
  - CVSS Score: 7.5
  - Description: Integer overflow in the fread function in ext/standard/file.c in PHP before 5.5.36 and 5.6.x before 5.6.22 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large integer in the second argument.
- Vulnerability: CVE-2014-9653
  - CVSS Score: 7.5
  - Description: readelf.c in file before 5.22, as used in the Fileinfo component in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5, does not consider that pread calls sometimes read only a subset of the available data, which allows remote attackers to cause a denial of service (uninitialized memory access) or possibly have unspecified other impact via a crafted ELF file.
- Vulnerability: CVE-2016-5094
  - CVSS Score: 7.5
  - Description: Integer overflow in the php_html_entities function in ext/standard/html.c in PHP before 5.5.36 and 5.6.x before 5.6.22 allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering a large output string from the htmlspecialchars function.
- Vulnerability: CVE-2016-5095
  - CVSS Score: 7.5
  - Description: Integer overflow in the php_escape_html_entities_ex function in ext/standard/html.c in PHP before 5.5.36 and 5.6.x before 5.6.22 allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering a large output string from a FILTER_SANITIZE_FULL_SPECIAL_CHARS filter_var call. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-5094.
- Vulnerability: CVE-2016-4543
  - CVSS Score: 7.5
  - Description: The exif_process_IFD_in_JPEG function in ext/exif/exif.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 does not validate IFD sizes, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted header data.
- Vulnerability: CVE-2016-4542
  - CVSS Score: 7.5
  - Description: The exif_process_IFD_TAG function in ext/exif/exif.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 does not properly construct spprintf arguments, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted header data.

- Vulnerability: CVE-2016-4541
  - CVSS Score: 7.5
  - Description: The grapheme_strpos function in ext/intl/grapheme/grapheme_string.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a negative offset.
- Vulnerability: CVE-2016-4540
  - CVSS Score: 7.5
  - Description: The grapheme_stripos function in ext/intl/grapheme/grapheme_string.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a negative offset.
- Vulnerability: CVE-2017-7963
  - CVSS Score: 5
  - Description: The GNU Multiple Precision Arithmetic Library (GMP) interfaces for PHP through 7.1.4 allow attackers to cause a denial of service (memory consumption and application crash) via operations on long strings. NOTE: the vendor disputes this, stating "There is no security issue here, because GMP safely aborts in case of an OOM condition. The only attack vector here is denial of service. However, if you allow attacker-controlled, unbounded allocations you have a DoS vector regardless of GMP's OOM behavior.
- Vulnerability: CVE-2014-3515
  - CVSS Score: 7.5
  - Description: The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.
- Vulnerability: CVE-2016-4544
  - CVSS Score: 7.5
  - Description: The exif_process_TIFF_in_JPEG function in ext/exif/exif.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 does not validate TIFF start data, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted header data.
- Vulnerability: CVE-2016-5399
  - CVSS Score: 6.8
  - Description: The bzread function in ext/bz2/bz2.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (out-of-bounds write) or execute arbitrary code via a crafted bz2 archive.
- Vulnerability: CVE-2019-9023
  - CVSS Score: 7.5

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

- Vulnerability: CVE-2019-9020
  - CVSS Score: 7.5
  - Description: An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. Invalid input to the function xmlrpc_decode() can lead to an invalid memory access (heap out of bounds read or read after free). This is related to xml_elem_parse_buf in ext/xmlrpc/libxmlrpc/xml_element.c.
- Vulnerability: CVE-2019-9021
  - CVSS Score: 7.5
  - Description: An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A heap-based buffer over-read in PHAR reading functions in the PHAR extension may allow an attacker to read allocated or unallocated memory past the actual data when trying to parse the file name, a different vulnerability than CVE-2018-20783. This is related to phar_detect_phar_fname_ext in ext/phar/phar.c.
- Vulnerability: CVE-2019-9024
  - CVSS Score: 5
  - Description: An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. xmlrpc_decode() can allow a hostile XMLRPC server to cause PHP to read memory outside of allocated areas in base64_decode_xmlrpc in ext/xmlrpc/libxmlrpc/base64.c.
- Vulnerability: CVE-2015-8389
  - CVSS Score: 7.5
  - Description: PCRE before 8.38 mishandles the /(?:|a|){100}x/ pattern and related patterns, which allows remote attackers to cause a denial of service (infinite recursion) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.
- Vulnerability: CVE-2013-7345
  - CVSS Score: 5
  - Description: The BEGIN regular expression in the awk script detector in magic/Magdir/commands in file before 5.15 uses multiple wildcards with unlimited repetitions, which allows context-dependent attackers to cause a denial of service (CPU consumption) via a crafted ASCII file that triggers a large amount of backtracking, as demonstrated via a file with many newline characters.
- Vulnerability: CVE-2016-6291
  - CVSS Score: 7.5

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

- Vulnerability: CVE-2016-6290
  - CVSS Score: 7.5
  - Description: ext/session/session.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 does not properly maintain a certain hash data structure, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via vectors related to session deserialization.
- Vulnerability: CVE-2016-6292
  - CVSS Score: 4.3
  - Description: The exif_process_user_comment function in ext/exif/exif.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted JPEG image.
- Vulnerability: CVE-2016-6295
  - CVSS Score: 7.5
  - Description: ext/snmp/snmp.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to cause a denial of service (use-after-free and application crash) or possibly have unspecified other impact via crafted serialized data, a related issue to CVE-2016-5773.
- Vulnerability: CVE-2016-6294
  - CVSS Score: 7.5
  - Description: The locale_accept_from_http function in ext/intl/locale/locale_methods.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 does not properly restrict calls to the ICU uloc_acceptLanguageFromHTTP function, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a call with a long argument.
- Vulnerability: CVE-2016-6297
  - CVSS Score: 6.8
  - Description: Integer overflow in the php_stream_zip_opener function in ext/zip/zip_stream.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a crafted zip:// URL.
- Vulnerability: CVE-2016-6296
  - CVSS Score: 7.5
  - Description: Integer signedness error in the simplestring_addn function in simplestring.c in xmlrpc-epi through 0.54.2, as used in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9, allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a long first argument to the PHP xmlrpc_encode_request function.

- Vulnerability: CVE-2014-5120
  - CVSS Score: 6.4
  - Description: gd_ctx.c in the GD component in PHP 5.4.x before 5.4.32 and 5.5.x before 5.5.16 does not ensure that pathnames lack %00 sequences, which might allow remote attackers to overwrite arbitrary files via crafted input to an application that calls the (1) imagegd, (2) imagegd2, (3) imagegif, (4) imagejpeg, (5) imagepng, (6) imagewbmp, or (7) imagewebp function.
- Vulnerability: CVE-2015-4642
  - CVSS Score: 10
  - Description: The escapeshellarg function in ext/standard/exec.c in PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 on Windows allows remote attackers to execute arbitrary OS commands via a crafted string to an application that accepts command-line arguments for a call to the PHP system function.
- Vulnerability: CVE-2015-1351
  - CVSS Score: 7.5
  - Description: Use-after-free vulnerability in the _zend_shared_memdup function in zend_shared_alloc.c in the OPcache extension in PHP through 5.6.7 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
- Vulnerability: CVE-2015-1352
  - CVSS Score: 5
  - Description: The build_tablename function in pgsql.c in the PostgreSQL (aka pgsql) extension in PHP through 5.6.7 does not validate token extraction for table names, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted name.
- Vulnerability: CVE-2015-4116
  - CVSS Score: 7.5
  - Description: Use-after-free vulnerability in the spl_ptr_heap_insert function in ext/spl/spl_heap.c in PHP before 5.5.27 and 5.6.x before 5.6.11 allows remote attackers to execute arbitrary code by triggering a failed SplMinHeap::compare operation.
- Vulnerability: CVE-2015-8865
  - CVSS Score: 7.5
  - Description: The file_check_mem function in funcs.c in file before 5.23, as used in the Fileinfo component in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5, mishandles continuation-level jumps, which allows context-dependent attackers to cause a denial of service (buffer overflow and application crash) or possibly execute arbitrary code via a crafted magic file.
- Vulnerability: CVE-2014-9705
  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the enchant_broker_request_dict function in ext/enchant/enchant.c in PHP before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6 allows remote attackers to execute arbitrary code via vectors that trigger creation of multiple dictionaries.
- Vulnerability: CVE-2015-8867

  - CVSS Score: 5
  - Description: The openssl_random_pseudo_bytes function in ext/openssl/openssl.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 incorrectly relies on the deprecated RAND_pseudo_bytes function, which makes it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors.

- Vulnerability: CVE-2015-8866
  - CVSS Score: 6.8
  - Description: ext/libxml/libxml.c in PHP before 5.5.22 and 5.6.x before 5.6.6, when PHP-FPM is used, does not isolate each thread from libxml_disable_entity_loader changes in other threads, which allows remote attackers to conduct XML External Entity (XXE) and XML Entity Expansion (XEE) attacks via a crafted XML document, a related issue to CVE-2015-5161.
- Vulnerability: CVE-2016-10712
  - CVSS Score: 5
  - Description: In PHP before 5.5.32, 5.6.x before 5.6.18, and 7.x before 7.0.3, all of the return values of stream_get_meta_data can be controlled if the input can be controlled (e.g., during file uploads). For example, a "$uri = stream_get_meta_data(fopen($file, "r"))['uri']" call mishandles the case where $file is data:text/plain;uri=eviluri, -- in other words, metadata can be set by an attacker.
- Vulnerability: CVE-2014-9709
  - CVSS Score: 5
  - Description: The GetCode_ function in gd_gif_in.c in GD 2.1.1 and earlier, as used in PHP before 5.5.21 and 5.6.x before 5.6.5, allows remote attackers to cause a denial of service (buffer over-read and application crash) via a crafted GIF image that is improperly handled by the gdImageCreateFromGif function.
- Vulnerability: CVE-2015-5589
  - CVSS Score: 10
  - Description: The phar_convert_to_other function in ext/phar/phar_object.c in PHP before 5.4.43, 5.5.x before 5.5.27, and 5.6.x before 5.6.11 does not validate a file pointer before a close operation, which allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via a crafted TAR archive that is mishandled in a Phar::convertToData call.
- Vulnerability: CVE-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-2016-9138
  - CVSS Score: 7.5
  - Description: PHP through 5.6.27 and 7.x through 7.0.12 mishandles property modification during __wakeup processing, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data, as demonstrated by Exception::__toString with DateInterval::__wakeup.

- Vulnerability: CVE-2018-7584
  - CVSS Score: 7.5
  - Description: In PHP through 5.6.33, 7.0.x before 7.0.28, 7.1.x through 7.1.14, and 7.2.x through 7.2.2, there is a stack-based buffer under-read while parsing an HTTP response in the php_stream_url_wrap_http_ex function in ext/standard/http_fopen_wrapper.c. This subsequently results in copying a large string.
- Vulnerability: CVE-2016-10397
  - CVSS Score: 5
  - Description: In PHP before 5.6.28 and 7.x before 7.0.13, incorrect handling of various URI components in the URL parser could be used by attackers to bypass hostname-specific URL checks, as demonstrated by evil.example.com:80#@good.example.com/ and evil.example.com:80?@good.example.com/ inputs to the parse_url function (implemented in the php_url_parse_ex function in ext/standard/url.c).
- Vulnerability: CVE-2015-8383
  - CVSS Score: 7.5
  - Description: PCRE before 8.38 mishandles certain repeated conditional groups, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.
- Vulnerability: CVE-2014-3669
  - CVSS Score: 7.5
  - Description: Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.
- Vulnerability: CVE-2018-5711
  - CVSS Score: 4.3
  - Description: gd_gif_in.c in the GD Graphics Library (aka libgd), as used in PHP before 5.6.33, 7.0.x before 7.0.27, 7.1.x before 7.1.13, and 7.2.x before 7.2.1, has an integer signedness error that leads to an infinite loop via a crafted GIF file, as demonstrated by a call to the imagecreatefromgif or imagecreatefromstring PHP function. This is related to GetCode_ and gdImageCreateFromGifCtx.
- Vulnerability: CVE-2015-8386
  - CVSS Score: 7.5
  - Description: PCRE before 8.38 mishandles the interaction of lookbehind assertions and mutually recursive subpatterns, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.
- Vulnerability: CVE-2017-11143
  - CVSS Score: 5

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

- Vulnerability: CVE-2016-10161
  - CVSS Score: 5
  - Description: The object_common1 function in ext/standard/var_unserializer.c in PHP before 5.6.30, 7.0.x before 7.0.15, and 7.1.x before 7.1.1 allows remote attackers to cause a denial of service (buffer over-read and application crash) via crafted serialized data that is mishandled in a finish_nested_data call.
- Vulnerability: CVE-2015-3412
  - CVSS Score: 5
  - Description: PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 does not ensure that pathnames lack %00 sequences, which might allow remote attackers to read arbitrary files via crafted input to an application that calls the stream_resolve_include_path function in ext/standard/streamsfuncs.c, as demonstrated by a filename\{}0.extension attack that bypasses an intended configuration in which client users may read files with only one specific extension.
- Vulnerability: CVE-2016-5767
  - CVSS Score: 6.8
  - Description: Integer overflow in the gdImageCreate function in gd.c in the GD Graphics Library (aka libgd) before 2.0.34RC1, as used in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8, allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted image dimensions.
- Vulnerability: CVE-2015-4599
  - CVSS Score: 10
  - Description: The SoapFault::__toString method in ext/soap/soap.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to obtain sensitive information, cause a denial of service (application crash), or possibly execute arbitrary code via an unexpected data type, related to a "type confusion" issue.
- Vulnerability: CVE-2015-4598
  - CVSS Score: 7.5
  - Description: PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 does not ensure that pathnames lack %00 sequences, which might allow remote attackers to read or write to arbitrary files via crafted input to an application that calls (1) a DOMDocument save method or (2) the GD imagepsloadfont function, as demonstrated by a filename\{}0.html attack that bypasses an intended configuration in which client users may write to only .html files.
- Vulnerability: CVE-2014-9652
  - CVSS Score: 5

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

- Vulnerability: CVE-2015-2783
  - CVSS Score: 5.8
  - Description: ext/phar/phar.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to obtain sensitive information from process memory or cause a denial of service (buffer over-read and application crash) via a crafted length value in conjunction with crafted serialized data in a phar archive, related to the phar_parse_metadata and phar_parse_pharfile functions.
- Vulnerability: CVE-2015-9253
  - CVSS Score: 6.8
  - Description: An issue was discovered in PHP 7.3.x before 7.3.0alpha3, 7.2.x before 7.2.8, and before 7.1.20. The php-fpm master process restarts a child process in an endless loop when using program execution functions (e.g., passthru, exec, shell_exec, or system) with a non-blocking STDIN stream, causing this master process to consume 100% of the CPU, and consume disk space with a large volume of error logs, as demonstrated by an attack by a customer of a shared-hosting facility.
- Vulnerability: CVE-2014-3981
  - CVSS Score: 3.3
  - Description: acinclude.m4, as used in the configure script in PHP 5.5.13 and earlier, allows local users to overwrite arbitrary files via a symlink attack on the /tmp/phpglibccheck file.
- Vulnerability: CVE-2017-9226
  - CVSS Score: 7.5
  - Description: An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A heap out-of-bounds write or read occurs in next_state_val() during regular expression compilation. Octal numbers larger than 0xff are not handled correctly in fetch_token() and fetch_token_in_cc(). A malformed regular expression containing an octal number in the form of '\{}700' would produce an invalid code point value larger than 0xff in next_state_val(), resulting in an out-of-bounds write memory corruption.
- Vulnerability: CVE-2017-9224
  - CVSS Score: 7.5
  - Description: An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A stack out-of-bounds read occurs in match_at() during regular expression searching. A logical error involving order of validation and access in match_at() could result in an out-of-bounds read from a stack buffer.
- Vulnerability: CVE-2016-5385
  - CVSS Score: 5.1

- Description: PHP through 7.0.8 does not attempt to address RFC 3875 section 4.1.18 namespace conflicts 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, as demonstrated by (1) an application that makes a getenv('HTTP_PROXY') call or (2) a CGI configuration of PHP, aka an "httpoxy" issue.

- Vulnerability: CVE-2015-5590
  - CVSS Score: 7.5
  - Description: Stack-based buffer overflow in the phar_fix_filepath function in ext/phar/phar.c in PHP before 5.4.43, 5.5.x before 5.5.27, and 5.6.x before 5.6.11 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large length value, as demonstrated by mishandling of an e-mail attachment by the imap PHP extension.
- Vulnerability: CVE-2014-0236
  - CVSS Score: 5
  - Description: file before 5.18, as used in the Fileinfo component in PHP before 5.6.0, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a zero root_storage value in a CDF file, related to cdf.c and readcdf.c.
- Vulnerability: CVE-2016-7132
  - CVSS Score: 5
  - Description: ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly have unspecified other impact via an invalid wddxPacket XML document that is mishandled in a wddx_deserialize call, as demonstrated by a stray element inside a boolean element, leading to incorrect pop processing.
- Vulnerability: CVE-2016-7131
  - CVSS Score: 5
  - Description: ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly have unspecified other impact via a malformed wddxPacket XML document that is mishandled in a wddx_deserialize call, as demonstrated by a tag that lacks a < (less than) character.
- Vulnerability: CVE-2016-7130
  - CVSS Score: 5
  - Description: The php_wddx_pop_element function in ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly have unspecified other impact via an invalid base64 binary value, as demonstrated by a wddx_deserialize call that mishandles a binary element in a wddxPacket XML document.
- Vulnerability: CVE-2019-6977
  - CVSS Score: 6.8

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

- Vulnerability: CVE-2014-3478
  - CVSS Score: 5
  - Description: Buffer overflow in the mconvert function in softmagic.c in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, allows remote attackers to cause a denial of service (application crash) via a crafted Pascal string in a FILE_PSTRING conversion.
- Vulnerability: CVE-2015-8873
  - CVSS Score: 5
  - Description: Stack consumption vulnerability in Zend/zend_exceptions.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 allows remote attackers to cause a denial of service (segmentation fault) via recursive method calls.
- Vulnerability: CVE-2015-8876
  - CVSS Score: 7.5
  - Description: Zend/zend_exceptions.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 does not validate certain Exception objects, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or trigger unintended method execution via crafted serialized data.
- Vulnerability: CVE-2015-8877
  - CVSS Score: 5
  - Description: The gdImageScaleTwoPass function in gd_interpolation.c in the GD Graphics Library (aka libgd) before 2.2.0, as used in PHP before 5.6.12, uses inconsistent allocate and free approaches, which allows remote attackers to cause a denial of service (memory consumption) via a crafted call, as demonstrated by a call to the PHP imagescale function.
- Vulnerability: CVE-2015-8874
  - CVSS Score: 5
  - Description: Stack consumption vulnerability in GD in PHP before 5.6.12 allows remote attackers to cause a denial of service via a crafted imagefilltoborder call.
- Vulnerability: CVE-2015-8393
  - CVSS Score: 5
  - Description: pcregrep in PCRE before 8.38 mishandles the -q option for binary files, which might allow remote attackers to obtain sensitive information via a crafted file, as demonstrated by a CGI script that sends stdout data to a client.
- Vulnerability: CVE-2015-8878
  - CVSS Score: 7.1

  - Description: main/php_open_temporary_file.c in PHP before 5.5.28 and 5.6.x before 5.6.12 does not ensure thread safety, which allows remote attackers to cause a denial of service (race condition and heap memory corruption) by leveraging an application that performs many temporary-file accesses.

- Vulnerability: CVE-2015-8879
  - CVSS Score: 5
  - Description: The odbc_bindcols function in ext/odbc/php_odbc.c in PHP before 5.6.12 mishandles driver behavior for SQL_WVARCHAR columns, which allows remote attackers to cause a denial of service (application crash) in opportunistic circumstances by leveraging use of the odbc_fetch_array function to access a certain type of Microsoft SQL Server table.
- Vulnerability: CVE-2015-3307
  - CVSS Score: 7.5
  - Description: The phar_parse_metadata function in ext/phar/phar.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service (heap metadata corruption) or possibly have unspecified other impact via a crafted tar archive.
- Vulnerability: CVE-2015-4021
  - CVSS Score: 5
  - Description: The phar_parse_tarfile function in ext/phar/tar.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 does not verify that the first character of a filename is different from the \{}0 character, which allows remote attackers to cause a denial of service (integer underflow and memory corruption) via a crafted entry in a tar archive.
- Vulnerability: CVE-2014-9425
  - CVSS Score: 7.5
  - Description: Double free vulnerability in the zend_ts_hash_graceful_destroy function in zend_ts_hash.c in the Zend Engine in PHP through 5.5.20 and 5.6.x through 5.6.4 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
- Vulnerability: CVE-2015-4022
  - CVSS Score: 7.5
  - Description: Integer overflow in the ftp_genlist function in ext/ftp/ftp.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 allows remote FTP servers to execute arbitrary code via a long reply to a LIST command, leading to a heap-based buffer overflow.
- Vulnerability: CVE-2015-4025
  - CVSS Score: 7.5
  - Description: PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 truncates a pathname upon encountering a \{}x00 character in certain situations, which allows remote attackers to bypass intended extension restrictions and access files or directories with unexpected names via a crafted argument to (1) set_include_path, (2) tempnam, (3) rmdir, or (4) readlink. NOTE: this vulnerability exists because of an incomplete fix for CVE-2006-7243.
- Vulnerability: CVE-2015-8391

  - CVSS Score: 9
  - Description: The pcre_compile function in pcre_compile.c in PCRE before 8.38 mishandles certain [: nesting, which allows remote attackers to cause a denial of service (CPU consumption) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.
- Vulnerability: CVE-2015-4026
  - CVSS Score: 7.5
  - Description: The pcntl_exec implementation in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 truncates a pathname upon encountering a \{}x00 character, which might allow remote attackers to bypass intended extension restrictions and execute files with unexpected names via a crafted first argument. NOTE: this vulnerability exists because of an incomplete fix for CVE-2006-7243.
- Vulnerability: CVE-2015-4643
  - CVSS Score: 7.5
  - Description: Integer overflow in the ftp_genlist function in ext/ftp/ftp.c in PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 allows remote FTP servers to execute arbitrary code via a long reply to a LIST command, leading to a heap-based buffer overflow. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-4022.
- Vulnerability: CVE-2014-9427
  - CVSS Score: 7.5
  - Description: sapi/cgi/cgi_main.c in the CGI component in PHP through 5.4.36, 5.5.x through 5.5.20, and 5.6.x through 5.6.4, when mmap is used to read a .php file, does not properly consider the mapping's length during processing of an invalid file that begins with a # character and lacks a newline character, which causes an out-of-bounds read and might (1) allow remote attackers to obtain sensitive information from php-cgi process memory by leveraging the ability to upload a .php file or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping.
- Vulnerability: CVE-2015-8390
  - CVSS Score: 7.5
  - Description: PCRE before 8.38 mishandles the [: and \{}\{} substrings in character classes, which allows remote attackers to cause a denial of service (uninitialized memory read) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.
- Vulnerability: CVE-2016-10158
  - CVSS Score: 5
  - Description: The exif_convert_any_to_int function in ext/exif/exif.c in PHP before 5.6.30, 7.0.x before 7.0.15, and 7.1.x before 7.1.1 allows remote attackers to cause a denial of service (application crash) via crafted EXIF data that triggers an attempt to divide the minimum representable negative integer by -1.
- Vulnerability: CVE-2016-10159
  - CVSS Score: 5

  - Description: Integer overflow in the phar_parse_pharfile function in ext/phar/phar.c in PHP before 5.6.30 and 7.0.x before 7.0.15 allows remote attackers to cause a denial of service (memory consumption or application crash) via a truncated manifest entry in a PHAR archive.
- Vulnerability: CVE-2014-3670
  - CVSS Score: 6.8
  - Description: The exif_ifd_make_value function in exif.c in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the exif_thumbnail function.
- Vulnerability: CVE-2019-9641
  - CVSS Score: 7.5
  - Description: An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_TIFF.
- Vulnerability: CVE-2015-3152
  - CVSS Score: 4.3
  - Description: Oracle MySQL before 5.7.3, Oracle MySQL Connector/C (aka libmysqlclient) before 6.1.3, and MariaDB before 5.5.44 use the --ssl option to mean that SSL is optional, which allows man-in-the-middle attackers to spoof servers via a cleartext-downgrade attack, aka a "BACKRONYM" attack.
- Vulnerability: CVE-2018-15132
  - CVSS Score: 5
  - Description: An issue was discovered in ext/standard/link_win32.c in PHP before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8. The linkinfo function on Windows doesn't implement the open_basedir check. This could be abused to find files on paths outside of the allowed directories.
- Vulnerability: CVE-2014-2270
  - CVSS Score: 4.3
  - Description: softmagic.c in file before 5.17 and libmagic allows context-dependent attackers to cause a denial of service (out-of-bounds memory access and crash) via crafted offsets in the softmagic of a PE executable.
- Vulnerability: CVE-2016-7124
  - CVSS Score: 7.5
  - Description: ext/standard/var_unserializer.c in PHP before 5.6.25 and 7.x before 7.0.10 mishandles certain invalid objects, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data that leads to a (1) __destruct call or (2) magic method call.
- Vulnerability: CVE-2016-7125
  - CVSS Score: 5
  - Description: ext/session/session.c in PHP before 5.6.25 and 7.x before 7.0.10 skips invalid session names in a way that triggers incorrect parsing, which allows remote attackers to inject arbitrary-type session data by leveraging control of a session name, as demonstrated by object injection.

- Vulnerability: CVE-2016-7126
  - CVSS Score: 7.5
  - Description: The imagetruecolortopalette function in ext/gd/gd.c in PHP before 5.6.25 and 7.x before 7.0.10 does not properly validate the number of colors, which allows remote attackers to cause a denial of service (select_colors allocation error and out-of-bounds write) or possibly have unspecified other impact via a large value in the third argument.
- Vulnerability: CVE-2016-7127
  - CVSS Score: 7.5
  - Description: The imagegammacorrect function in ext/gd/gd.c in PHP before 5.6.25 and 7.x before 7.0.10 does not properly validate gamma values, which allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact by providing different signs for the second and third arguments.
- Vulnerability: CVE-2014-1943
  - CVSS Score: 5
  - Description: Fine Free file before 5.17 allows context-dependent attackers to cause a denial of service (infinite recursion, CPU consumption, and crash) via a crafted indirect offset value in the magic of a file.
- Vulnerability: CVE-2016-7128
  - CVSS Score: 5
  - Description: The exif_process_IFD_in_TIFF function in ext/exif/exif.c in PHP before 5.6.25 and 7.x before 7.0.10 mishandles the case of a thumbnail offset that exceeds the file size, which allows remote attackers to obtain sensitive information from process memory via a crafted TIFF image.
- Vulnerability: CVE-2016-7129
  - CVSS Score: 7.5
  - Description: The php_wddx_process_data function in ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via an invalid ISO 8601 time value, as demonstrated by a wddx_deserialize call that mishandles a dateTime element in a wddxPacket XML document.
- Vulnerability: CVE-2016-2554
  - CVSS Score: 10
  - Description: Stack-based buffer overflow in ext/phar/tar.c in PHP before 5.5.32, 5.6.x before 5.6.18, and 7.x before 7.0.3 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted TAR archive.
- Vulnerability: CVE-2017-11628
  - CVSS Score: 6.8
  - Description: In PHP before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7, a stack-based buffer overflow in the zend_ini_do_op() function in Zend/zend_ini_parser.c could cause a denial of service or potentially allow executing code. NOTE: this is only relevant for PHP applications that accept untrusted input (instead of the system's php.ini file) for the parse_ini_string or parse_ini_file function, e.g., a web application for syntax validation of php.ini directives.

- Vulnerability: CVE-2014-3480
  - CVSS Score: 4.3
  - Description: The cdf_count_chain function in cdf.c in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, does not properly validate sector-count data, which allows remote attackers to cause a denial of service (application crash) via a crafted CDF file.
- Vulnerability: CVE-2017-12933
  - CVSS Score: 7.5
  - Description: The finish_nested_data function in ext/standard/var_unserializer.re in PHP before 5.6.31, 7.0.x before 7.0.21, and 7.1.x before 7.1.7 is prone to a buffer over-read while unserializing untrusted data. Exploitation of this issue can have an unspecified impact on the integrity of PHP.
- Vulnerability: CVE-2014-0238
  - CVSS Score: 5
  - Description: The cdf_read_property_info function in cdf.c in the Fileinfo component in PHP before 5.4.29 and 5.5.x before 5.5.13 allows remote attackers to cause a denial of service (infinite loop or out-of-bounds memory access) via a vector that (1) has zero length or (2) is too long.
- Vulnerability: CVE-2014-4721
  - CVSS Score: 2.6
  - Description: The phpinfo implementation in ext/standard/info.c in PHP before 5.4.30 and 5.5.x before 5.5.14 does not ensure use of the string data type for the PHP_AUTH_PW, PHP_AUTH_TYPE, PHP_AUTH_USER, and PHP_SELF variables, which might allow context-dependent attackers to obtain sensitive information from process memory by using the integer data type with crafted values, related to a "type confusion" vulnerability, as demonstrated by reading a private SSL key in an Apache HTTP Server web-hosting environment with mod_ssl and a PHP 5.3.x mod_php.
- Vulnerability: CVE-2014-9767
  - CVSS Score: 4.3
  - Description: Directory traversal vulnerability in the ZipArchive::extractTo function in ext/zip/php_zip.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 and ext/zip/ext_zip.cpp in HHVM before 3.12.1 allows remote attackers to create arbitrary empty directories via a crafted ZIP archive.
- Vulnerability: CVE-2015-2331
  - CVSS Score: 7.5
  - Description: Integer overflow in the _zip_cdir_new function in zip_dirent.c in libzip 0.11.2 and earlier, as used in the ZIP extension in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 and other products, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a ZIP archive that contains many entries, leading to a heap-based buffer overflow.
- Vulnerability: CVE-2016-4537
  - CVSS Score: 7.5

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

- Vulnerability: CVE-2016-4538
  - CVSS Score: 7.5
  - Description: The bcpowmod function in ext/bcmath/bcmath.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 modifies certain data structures without considering whether they are copies of the _zero_, _one_, or _two_ global variable, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted call.
- Vulnerability: CVE-2016-4539
  - CVSS Score: 7.5
  - Description: The xml_parse_into_struct function in ext/xml/xml.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 allows remote attackers to cause a denial of service (buffer under-read and segmentation fault) or possibly have unspecified other impact via crafted XML data in the second argument, leading to a parser level of zero.
- Vulnerability: CVE-2016-6207
  - CVSS Score: 4.3
  - Description: Integer overflow in the _gdContributionsAlloc function in gd_interpolation.c in GD Graphics Library (aka libgd) before 2.2.3 allows remote attackers to cause a denial of service (out-of-bounds memory write or memory consumption) via unspecified vectors.
- Vulnerability: CVE-2014-4698
  - CVSS Score: 4.6
  - Description: Use-after-free vulnerability in ext/spl/spl_array.c in the SPL component in PHP through 5.5.14 allows context-dependent attackers to cause a denial of service or possibly have unspecified other impact via crafted ArrayIterator usage within applications in certain web-hosting environments.
- Vulnerability: CVE-2015-3329
  - CVSS Score: 7.5
  - Description: Multiple stack-based buffer overflows in the phar_set_inode function in phar_internal.h in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allow remote attackers to execute arbitrary code via a crafted length value in a (1) tar, (2) phar, or (3) ZIP archive.
- Vulnerability: CVE-2020-11579
  - CVSS Score: 5
  - Description: An issue was discovered in Chadha PHPKB 9.0 Enterprise Edition. installer/test-connection.php (part of the installation process) allows a remote unauthenticated attacker to disclose local files on hosts running PHP before 7.2.16, or on hosts where the MySQL ALLOW LOCAL DATA INFILE option is enabled.
- Vulnerability: CVE-2016-6288
  - CVSS Score: 7.5

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

- Vulnerability: CVE-2015-3415
  - CVSS Score: 7.5
  - Description: The sqlite3VdbeExec function in vdbe.c in SQLite before 3.8.9 does not properly implement comparison operators, which allows context-dependent attackers to cause a denial of service (invalid free operation) or possibly have unspecified other impact via a crafted CHECK clause, as demonstrated by CHECK(0&O>O) in a CREATE TABLE statement.
- Vulnerability: CVE-2016-9935
  - CVSS Score: 7.5
  - Description: The php_wddx_push_element function in ext/wddx/wddx.c in PHP before 5.6.29 and 7.x before 7.0.14 allows remote attackers to cause a denial of service (out-of-bounds read and memory corruption) or possibly have unspecified other impact via an empty boolean element in a wddxPacket XML document.
- Vulnerability: CVE-2016-5114
  - CVSS Score: 6.4
  - Description: sapi/fpm/fpm/fpm_log.c in PHP before 5.5.31, 5.6.x before 5.6.17, and 7.x before 7.0.2 misinterprets the semantics of the snprintf return value, which allows attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read and buffer overflow) via a long string, as demonstrated by a long URI in a configuration with custom REQUEST_URI logging.
- Vulnerability: CVE-2018-19396
  - CVSS Score: 5
  - Description: ext/standard/var_unserializer.c in PHP 5.x through 7.1.24 allows attackers to cause a denial of service (application crash) via an unserialize call for the com, dotnet, or variant class.
- Vulnerability: CVE-2018-19395
  - CVSS Score: 5
  - Description: ext/standard/var.c in PHP 5.x through 7.1.24 on Windows allows attackers to cause a denial of service (NULL pointer dereference and application crash) because com and com_safearray_proxy return NULL in com_properties_get in ext/com_dotnet/com_handlers.c, as demonstrated by a serialize call on COM("WScript.Shell").
- Vulnerability: CVE-2014-3668
  - CVSS Score: 5
  - Description: Buffer overflow in the date_from_ISO8601 function in the mkgmtime implementation in libxmlrpc/xmlrpc.c in the XMLRPC extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) via (1) a crafted first argument to the xmlrpc_set_type function or (2) a crafted argument to the xmlrpc_decode function, related to an out-of-bounds read operation.
- Vulnerability: CVE-2015-4644

  - CVSS Score: 5
  - Description: The php_pgsql_meta_data function in pgsql.c in the PostgreSQL (aka pgsql) extension in PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 does not validate token extraction for table names, which might allow remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted name. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-1352.

- Vulnerability: CVE-2017-11142
  - CVSS Score: 7.8
  - Description: In PHP before 5.6.31, 7.x before 7.0.17, and 7.1.x before 7.1.3, remote attackers could cause a CPU consumption denial of service attack by injecting long form variables, related to main/php_variables.c.
- Vulnerability: CVE-2014-3710
  - CVSS Score: 5
  - Description: The donote function in readelf.c in file through 5.20, as used in the Fileinfo component in PHP 5.4.34, does not ensure that sufficient note headers are present, which allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted ELF file.
- Vulnerability: CVE-2016-4343
  - CVSS Score: 6.8
  - Description: The phar_make_dirstream function in ext/phar/dirstream.c in PHP before 5.6.18 and 7.x before 7.0.3 mishandles zero-size ././@LongLink files, which allows remote attackers to cause a denial of service (uninitialized pointer dereference) or possibly have unspecified other impact via a crafted TAR archive.
- Vulnerability: CVE-2016-4342
  - CVSS Score: 8.3
  - Description: ext/phar/phar_object.c in PHP before 5.5.32, 5.6.x before 5.6.18, and 7.x before 7.0.3 mishandles zero-length uncompressed data, which allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via a crafted (1) TAR, (2) ZIP, or (3) PHAR archive.
- Vulnerability: CVE-2015-2325
  - CVSS Score: 6.8
  - Description: The compile_branch function in PCRE before 8.37 allows context-dependent attackers to compile incorrect code, cause a denial of service (out-of-bounds heap read and crash), or possibly have other unspecified impact via a regular expression with a group containing a forward reference repeated a large number of times within a repeated outer group that has a zero minimum quantifier.
- Vulnerability: CVE-2015-2326
  - CVSS Score: 4.3
  - Description: The pcre_compile2 function in PCRE before 8.37 allows context-dependent attackers to compile incorrect code and cause a denial of service (out-of-bounds read) via regular expression with a group containing both a forward referencing subroutine call and a recursive back reference, as demonstrated by "((?+1)(\{}1))/".

- Vulnerability: CVE-2015-3414
  - CVSS Score: 7.5
  - Description: SQLite before 3.8.9 does not properly implement the dequoting of collation-sequence names, which allows context-dependent attackers to cause a denial of service (uninitialized memory access and application crash) or possibly have unspecified other impact via a crafted COLLATE clause, as demonstrated by COLLATE"""""""" at the end of a SELECT statement.
- Vulnerability: CVE-2015-7803
  - CVSS Score: 6.8
  - Description: The phar_get_entry_data function in ext/phar/util.c in PHP before 5.5.30 and 5.6.x before 5.6.14 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a .phar file with a crafted TAR archive entry in which the Link indicator references a file that does not exist.
- Vulnerability: CVE-2016-9933
  - CVSS Score: 5
  - Description: Stack consumption vulnerability in the gdImageFillToBorder function in gd.c in the GD Graphics Library (aka libgd) before 2.2.2, as used in PHP before 5.6.28 and 7.x before 7.0.13, allows remote attackers to cause a denial of service (segmentation violation) via a crafted imagefilltoborder call that triggers use of a negative color value.
- Vulnerability: CVE-2015-7804
  - CVSS Score: 6.8
  - Description: Off-by-one error in the phar_parse_zipfile function in ext/phar/zip.c in PHP before 5.5.30 and 5.6.x before 5.6.14 allows remote attackers to cause a denial of service (uninitialized pointer dereference and application crash) by including the / filename in a .zip PHAR archive.
- Vulnerability: CVE-2014-3479
  - CVSS Score: 4.3
  - Description: The cdf_check_stream_offset function in cdf.c in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, relies on incorrect sector-size data, which allows remote attackers to cause a denial of service (application crash) via a crafted stream offset in a CDF file.
- Vulnerability: CVE-2014-8142
  - CVSS Score: 7.5
  - Description: Use-after-free vulnerability in the process_nested_data function in ext/standard/var_unserializer.re in PHP before 5.4.36, 5.5.x before 5.5.20, and 5.6.x before 5.6.4 allows remote attackers to execute arbitrary code via a crafted unserialize call that leverages improper handling of duplicate keys within the serialized properties of an object, a different vulnerability than CVE-2004-1019.
- Vulnerability: CVE-2015-3330
  - CVSS Score: 6.8
  - Description: The php_handler function in sapi/apache2handler/sapi_apache2.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8, when the Apache HTTP Server 2.4.x is used, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via pipelined HTTP requests that result in a "deconfigured interpreter."

- Vulnerability: CVE-2017-16642
  - CVSS Score: 5
  - Description: In PHP before 5.6.32, 7.x before 7.0.25, and 7.1.x before 7.1.11, an error in the date extension's timelib_meridian handling of 'front of' and 'back of' directives could be used by attackers able to supply date strings to leak information from the interpreter, related to ext/date/lib/parse_date.c out-of-bounds reads affecting the php_parse_date function. NOTE: this is a different issue than CVE-2017-11145.

IP Address: 62.94.137.201

- Organization: EDISON 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: N/A
  - Port: 179
  - Version: N/A
  - Location:

No vulnerabilities found for this IP address.

IP Address: 151.22.38.13

- Organization: edison
- 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: 185.91.71.118

- Organization: Libraesva srl
- 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: Postfix smtpd
  - Port: 25
  - Version: N/A
  - Location:
- Service: Apache httpd
  - Port: 80
  - Version: N/A
  - Location: https://185.91.71.118/
- Service: net-snmp
  - Port: 161
  - Version: N/A
  - Location:
- Service: Postfix smtpd
  - Port: 465
  - Version: N/A
  - Location:
- Service: Postfix smtpd
  - Port: 587
  - Version: N/A
  - Location:

No vulnerabilities found for this IP address.

IP Address: 52.49.152.75

- 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: /

No vulnerabilities found for this IP address.

IP Address: 151.22.38.14

- Organization: edison
- 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: 151.22.38.252

- Organization: edison
- Operating System: N/A
- Critical Vulnerabilities: 0
- High Vulnerabilities: 0
- Medium Vulnerabilities: 0
- Low Vulnerabilities: 0
- Total Vulnerabilities: 0

Services Running on IP Address

- Service: Apache httpd
  - Port: 443
  - Version: N/A
  - Location: /

No vulnerabilities found for this IP address.