Report for Domain: edison.it

Generated by Apollo

September 10, 2024

Contents

1 Summary of Findings

Below are some key statistics from the data provided:

- **Number of IPs**: 90
- **Number of Domains**: 154
- **Number of Emails**: 16
- **Number of Resolved Hosts**: 52
- **Number of Mail Servers**: 4
- **Number of URLs**: 0

2 IP Addresses found

Below is the list of IP addresses found:

- 151.22.39.45
- 151.22.38.13
- 204.246.191.61
- 52.211.124.234
- 195.103.103.30
- 212.73.193.150
- 89.197.73.20
- 62.94.137.201
- 213.217.29.85
- 3.64.78.167
- 151.22.38.14
- 151.22.38.130
- 3.121.19.218
- 185.91.71.118
- 94.124.69.67
- 62.94.137.182
- 0.0.0.0
- 51.75.86.118
- 54.192.76.24
- 37.72.32.254
- 151.22.38.175
- 3.120.219.35
- 37.72.32.222
- 52.51.233.170
- 108.138.192.49
- 54.192.76.85
- 151.22.38.156
- 51.178.13.239
- 151.22.39.54
- 51.91.24.51
- 212.35.216.126
- 151.22.39.9
- 40.126.32.129

- 109.168.22.86
- 93.186.249.30
- 46.28.2.183
- 62.94.137.206
- 95.174.28.207
- 108.157.194.127
- 151.22.38.131
- 151.22.39.6
- 151.22.39.122
- 52.50.23.25
- 83.211.69.255
- 3.126.218.72
- 51.15.59.206
- 151.22.38.152
- 151.22.39.18
- 195.231.62.154
- 52.49.152.75
- 35.156.181.89
- 93.186.242.241
- 156.54.148.62
- 204.246.191.51
- 37.72.32.244
- 52.213.159.238
- 54.192.76.55
- 40.126.32.6
- 51.38.105.34
- 3.126.233.235
- 54.192.76.109
- 52.98.242.232
- 151.22.38.214
- 40.87.138.215
- 18.202.92.68
- 151.22.39.38
- 204.246.191.9
- 151.22.38.234
- 34.248.167.34

- 137.135.246.66
- 151.22.39.27
- 54.76.95.70
- 109.168.22.85
- 151.22.38.133
- 63.33.242.246
- 62.94.137.200
- 151.22.38.140
- 13.74.182.99
- 3.125.77.225
- 151.101.65.195
- 204.246.191.8
- 162.55.172.85
- 151.22.38.70
- 151.22.39.19
- 37.72.32.255
- 151.101.1.195
- 94.127.86.211
- 18.195.121.173
- 151.22.38.198
- 151.22.38.155

3 Domain found

Below is the list of Domain found:

- consipsl3.edison.it
- editoowanl01.corp.edison.it
- ediaw01.free.edison.it
- facilitysolutions.edison.it
- documentale-itg.edison.it
- bonus.edison.it
- edoc.edison.it
- gdc.edison.it
- gen-e.edison.it
- portaleproduttori2.edison.it
- webcon.edison.it
- vireoxmobile.edison.it
- da.edison.it
- cowprep.corp.edison.it
- hubatoa.edison.it
- crm.prep.edison.it
- enefcampus.edison.it
- uag.free.edison.it
- certauth.sso.edison.it
- desitest.corp.edison.it
- ediema.edison.it
- outlook.corp.edison.it
- portalesrm.edison.it
- mi045wlc5508dr.corp.edison.it
- nicesvil.edison.it
- password-reset.edison.it
- hubtest.edison.it
- efficienzaenergetica.edison.it
- open.edison.it
- dnf.edison.it
- cbctest.corp.edison.it
- *.edison.it
- eas.edison.it

- ediprdalvcms01.corp.edison.it
- extranet.edison.it
- editstpiteas01.corp.edison.it
- inge.edison.it
- trayport.edison.it
- collaudo-dof.edison.it
- mail.edison.it
- vpnclientleonardo.edison.it
- av.edison.it
- legacy.edison.it
- stories.efficienzaenergetica.edison.it
- mi045ise3305ced.corp.edison.it
- extranet2010.edison.it
- qlv.free.edison.it
- erm.corp.edison.it
- er-ta.edison.it
- wsnomitsrg.edison.it
- thorprep.corp.edison.it
- mi045ise3305dr.corp.edison.it
- fgt.egypt.edison.it
- smtppub.edison.it
- wsnomitsrgtest.edison.it
- niceprod.edison.it
- edireppiteas01.corp.edison.it
- vpn-fornitori.edison.it
- ebidtest.corp.edison.it
- enterpriseregistration.edison.it
- autodiscover.edison.it
- segnalazioni.edison.it
- edisonnextbrandcenter.edison.it
- cbc.corp.edison.it
- edito-test-01.corp.edison.it
- cmor.edison.it
- powerprocert.edison.it
- email.edison.it
- crmee.edison.it

- pec.edison.it
- stonesvil.edison.it
- hub.portal.edison.it
- hedgingportal.corp.edison.it
- free.edison.it
- thortestatoa.edison.it
- noi.edison.it
- hub.edison.it
- portaleproduttori1.edison.it
- adt.edison.it
- authsap.edison.it
- elearning.edison.it
- qvmobiletest.corp.edison.it
- admpowerprocert.edison.it
- gateway.edison.it
- fmw.edison.it
- indep2010.edison.it
- dep.edison.it
- chargeandgo.edison.it
- desi.corp.edison.it
- elp.edison.it
- monitoraggiomar.edison.it
- enterpriseregistration.egypt.edison.it
- daemobile.edison.it
- authsaptest.edison.it
- etools1.edison.it
- ediweb.edison.it
- powerpro.edison.it
- ediema01.corp.edison.it
- mi045wlc5508ced.corp.edison.it
- stonecert.edison.it
- corp.edison.it
- ssl.edison.it
- sip.edison.it
- collaudo-noi.edison.it
- sso.edison.it

- teleriscaldamento.edison.it
- ebid.corp.edison.it
- asid.edison.it
- lyncdiscover.edison.it
- admpowerpro.edison.it
- ediprdpiteas01.corp.edison.it
- enterpriseregistration.corp.edison.it
- lync.edison.it
- documentale-stoccaggio.edison.it
- indep.edison.it
- er.edison.it
- centraletorviscosa.edison.it
- edicerpiteas01.corp.edison.it
- edison.it
- ediprdenras11.corp.edison.it
- leonardo.edison.it
- energiachecambiatutto.edison.it
- vpnlondon.edison.it
- stone.edison.it
- pss.edison.it
- vpn.edison.it
- ssl-eesm-ot.edison.it
- ema.edison.it
- er-fa.edison.it
- edisonbrandcenter.edison.it
- 140anni.edison.it
- owebapp.edison.it
- areaclienti.prep.edison.it
- inwelldiary.edison.it
- lyncws.edison.it
- directorsdocuments.edison.it
- move.edison.it
- authsapdev.edison.it
- citrix.edison.it
- edisonfornature.edison.it
- portale.edison.it

- thorprod.corp.edison.it
- enterpriseregistration.fenice.edison.it
- dep2010.edison.it
- iag.free.edison.it
- etools2.edison.it
- mdm.free.edison.it
- elyx.edison.it
- softweb.edison.it
- dof.edison.it
- edisonmediacenter.edison.it
- monitoraggiomar-test.edison.it
- comparatoreofferte.edison.it
- spfk.edison.it

4 URLs found

Below is the list of URLs found:

- No URLs found

5 Domain Related to URLs Found

- No Domains or URLs found

6 Emails found

Below is the list of Emails found:

- lorenzo.matucci@edison.it
- servizioclienti@edison.it
- staffqualifiche@edison.it
- edisonenergia_faci@edison.it
- allacci_subentri@edison.it
- cristina.parenti@edison.it
- hr.onboarding@edison.it
- ufficiostampa@edison.it
- elena.distaso@edison.it
- massimiliano.cicalese@edison.it
- lucia.caltagirone@edison.it
- edisonnext@pec.edison.it
- sostenibilita@edison.it
- edison@pec.edison.it
- supporto.fornitori@edison.it
- jane.doe@edison.it

7 Resolved Hosts

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

- **140anni.edison.it** : 108.157.194.127
- **adt.edison.it** : 3.120.219.35
- **authsap.edison.it** : 3.125.77.225
- **authsapdev.edison.it** : 3.125.77.225
- **autodiscover.edison.it** : 52.98.242.232
- **centraletorviscosa.edison.it** : 35.156.181.89
- **chargeandgo.edison.it** : 109.168.22.86
- **comparatoreofferte.edison.it** : 3.120.219.35
- **consipsl3.edison.it** : 156.54.148.62
- **crm.prep.edison.it** : 151.22.38.152
- **crmee.edison.it** : 151.22.38.156
- **daemobile.edison.it** : 151.22.38.140
- **directorsdocuments.edison.it** : 40.87.138.215
- **dnf.edison.it** : 108.138.192.49
- **ediema.edison.it** : 151.22.38.234
- **edison.it** : 51.38.105.34
- **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** : 3.126.233.235
- **enefcampus.edison.it** : 51.91.24.51
- **enterpriseregistration.corp.edison.it** : 40.126.32.6
- **enterpriseregistration.edison.it** : 40.126.32.6
- **enterpriseregistration.fenice.edison.it** : 40.126.32.129
- **er-fa.edison.it** : 37.72.32.255
- **er-ta.edison.it** : 37.72.32.222
- **er.edison.it** : 37.72.32.254
- **fmw.edison.it** : 151.22.39.54
- **gateway.edison.it** : 151.22.38.133

- **gen-e.edison.it** : 93.186.242.241
- **iag.free.edison.it** : 151.22.38.70
- **mail.edison.it** : 151.22.38.175
- **monitoraggiomar-test.edison.it** : 63.33.242.246
- **monitoraggiomar.edison.it** : 34.248.167.34
- **open.edison.it** : 0.0.0.0
- **powerpro.edison.it** : 35.156.181.89
- **pss.edison.it** : 151.22.38.155
- **segnalazioni.edison.it** : 95.174.28.207
- **smtppub.edison.it** : 151.22.38.131
- **ssl-eesm-ot.edison.it** : 151.22.39.122
- **ssl.edison.it** : 151.22.38.13
- **stories.efficienzaenergetica.edison.it** : 151.101.65.195
- **vireoxmobile.edison.it** : 37.72.32.244
- **vpn-fornitori.edison.it** : 151.22.38.133
- **vpn.edison.it** : 151.22.38.14
- **vpnclientleonardo.edison.it** : 195.231.62.154
- **wsnomitsrg.edison.it** : 3.121.19.218
- **wsnomitsrgtest.edison.it** : 18.195.121.173

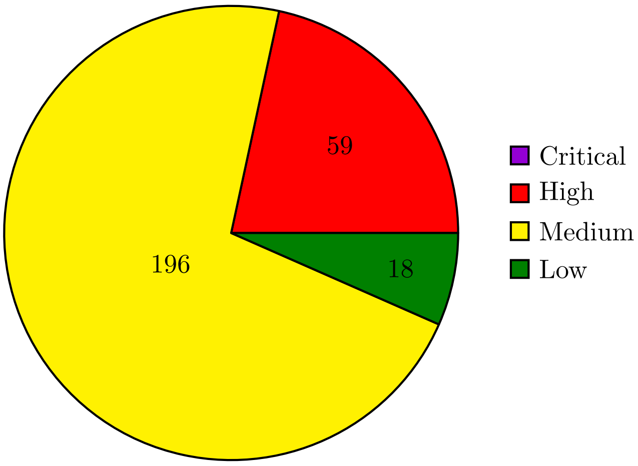
8 Server Mail found

Below is the list of Mail Server found:

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

9 Pie Chart of Vulnerabilities

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



10 Vulnerability Summary per IP

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

IP Address	Critical	High	Medium	Low
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
62.94.137.182	0	0	0	0
3.126.233.235	0	0	0	0
93.186.242.241	0	0	0	0
3.125.77.225	0	0	0	0
151.101.65.195	0	0	0	0
37.72.32.255	0	0	0	0
54.192.76.24	0	0	0	0
18.202.92.68	0	0	0	0
151.22.38.13	0	0	0	0
156.54.148.62	0	0	0	0
37.72.32.222	0	0	0	0
52.98.242.232	0	0	0	0
3.64.78.167	0	0	0	0
52.211.124.234	0	0	0	0
151.101.1.195	0	0	0	0
51.178.13.239	0	0	0	0
3.120.219.35	0	0	0	0
46.28.2.183	0	0	0	0
89.197.73.20	0	0	0	0
37.72.32.244	0	0	0	0
151.22.39.122	0	0	0	0
151.22.38.133	0	0	0	0
151.22.38.14	0	0	0	0
62.94.137.206	0	0	0	0
62.94.137.201	0	0	0	0
35.156.181.89	0	0	0	0
213.217.29.85	0	0	0	0
94.124.69.67	0	0	0	0
52.50.23.25	0	0	0	0
185.91.71.118	0	0	0	0

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

11 Shodan Results for IP Addresses

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

11.1 IP Address: 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.

11.2 IP Address: 54.76.95.70

- Organization: Amazon Technologies Inc.
- Operating System: N/A
- 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.a2a.eu/
- Service: Apache httpd
  - Port: 443
  - Version: 2.4.18
  - Location: https://www.grappanonino.com/

Vulnerabilities Found

- Vulnerability: CVE-2019-0220
  - CVSS Score: 5
  - Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.
- Vulnerability: CVE-2017-3169
  - CVSS Score: 7.5
  - Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.
- Vulnerability: CVE-2024-27316
  - CVSS Score: N/A
  - Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.
- Vulnerability: CVE-2017-7679

  - CVSS Score: 7.5
  - Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.
- Vulnerability: CVE-2013-2765
  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.
- Vulnerability: CVE-2020-1934
  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.
- Vulnerability: CVE-2018-17189
  - CVSS Score: 5
  - Description: In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 (mod_http2) connections.
- Vulnerability: CVE-2022-36760
  - CVSS Score: N/A
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.
- Vulnerability: CVE-2020-35452
  - CVSS Score: 6.8
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow
- Vulnerability: CVE-2017-9798
  - CVSS Score: 5
  - Description: Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.
- Vulnerability: CVE-2016-1546

  - CVSS Score: 4.3
  - Description: The Apache HTTP Server 2.4.17 and 2.4.18, when mod_http2 is enabled, does not limit the number of simultaneous stream workers for a single HTTP/2 connection, which allows remote attackers to cause a denial of service (stream-processing outage) via modified flow-control windows.

- Vulnerability: CVE-2022-29404
  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.
- Vulnerability: CVE-2021-33193
  - CVSS Score: 5
  - Description: A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.
- Vulnerability: CVE-2009-0796
  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.
- Vulnerability: CVE-2013-4365
  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.
- Vulnerability: CVE-2018-1333
  - CVSS Score: 5
  - Description: By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.18-2.4.30,2.4.33).
- Vulnerability: CVE-2022-22720
  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling
- Vulnerability: CVE-2018-11763
  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.17 to 2.4.34, by sending continuous, large SETTINGS frames a client can occupy a connection, server thread and CPU time without any connection timeout coming to effect. This affects only HTTP/2 connections. A possible mitigation is to not enable the h2 protocol.
- Vulnerability: CVE-2022-28330
  - CVSS Score: 5

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

- Vulnerability: CVE-2021-32791
  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.
- Vulnerability: CVE-2021-32792
  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using 'OIDCPreservePost On'.
- Vulnerability: CVE-2023-31122
  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.
- Vulnerability: CVE-2016-8612
  - CVSS Score: 3.3
  - Description: Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.
- Vulnerability: CVE-2024-38476
  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.
- Vulnerability: CVE-2024-38477
  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.
- Vulnerability: CVE-2024-38474
  - CVSS Score: N/A

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

- Vulnerability: CVE-2019-0196
  - CVSS Score: 5
  - Description: A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.
- Vulnerability: CVE-2019-0211
  - CVSS Score: 7.2
  - Description: In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.
- Vulnerability: CVE-2022-22721
  - CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.
- Vulnerability: CVE-2006-20001
  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.
- Vulnerability: CVE-2019-10092
  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.
- Vulnerability: CVE-2013-0941
  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

- Vulnerability: CVE-2019-17567
  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.
- Vulnerability: CVE-2017-15715
  - CVSS Score: 6.8
  - Description: In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.
- Vulnerability: CVE-2022-31813
  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.
- Vulnerability: CVE-2012-4001
  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.
- Vulnerability: CVE-2019-10098
  - CVSS Score: 5.8
  - Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.
- Vulnerability: CVE-2022-37436
  - CVSS Score: N/A
  - Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.
- Vulnerability: CVE-2016-5387
  - CVSS Score: 6.8
  - Description: The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.

- Vulnerability: CVE-2012-4360
  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
- Vulnerability: CVE-2021-40438
  - CVSS Score: 6.8
  - Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.
- Vulnerability: CVE-2011-1176
  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.
- Vulnerability: CVE-2022-23943
  - CVSS Score: 7.5
  - Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.
- Vulnerability: CVE-2020-1927
  - CVSS Score: 5.8
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.
- Vulnerability: CVE-2018-17199
  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.
- Vulnerability: CVE-2017-9788
  - CVSS Score: 6.4
  - Description: In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.
- Vulnerability: CVE-2017-15710

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

- Vulnerability: CVE-2016-4975
  - CVSS Score: 4.3
  - Description: Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).

- Vulnerability: CVE-2018-1302
  - CVSS Score: 4.3
  - Description: When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.

- Vulnerability: CVE-2018-1303
  - CVSS Score: 5
  - Description: A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache. The vulnerability is considered as low risk since mod_cache_socache is not widely used, mod_cache_disk is not concerned by this vulnerability.

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

- Vulnerability: CVE-2021-34798
  - CVSS Score: 5
  - Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

- Vulnerability: CVE-2023-25690
  - CVSS Score: N/A

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

- Vulnerability: CVE-2021-32786
  - CVSS Score: 5.8
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, ‘oidc_validate_redirect_url()‘ does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring ‘mod_auth_openidc‘ to only allow redirection whose destination matches a given regular expression.
- Vulnerability: CVE-2021-32785
  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache (‘OIDCCacheEncrypt off‘, ‘OIDCSessionType server-cache‘, ‘OIDCCacheType redis‘), ‘mod_auth_openidc‘ wrongly performed argument interpolation before passing Redis requests to ‘hiredis‘, which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the ‘hiredis‘ API. As a workaround, this vulnerability can be mitigated by setting ‘OIDCCacheEncrypt‘ to ‘on‘, as cache keys are cryptographically hashed before use when this option is enabled.
- Vulnerability: CVE-2011-2688
  - CVSS Score: 7.5
  - Description: SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module 3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL commands via the user field.
- Vulnerability: CVE-2021-44224

  - CVSS Score: 6.4
  - Description: A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).

- Vulnerability: CVE-2020-11985
  - CVSS Score: 4.3
  - Description: IP address spoofing when proxying using mod_remoteip and mod_rewrite For configurations using proxying with mod_remoteip and certain mod_rewrite rules, an attacker could spoof their IP address for logging and PHP scripts. Note this issue was fixed in Apache HTTP Server 2.4.24 but was retrospectively allocated a low severity CVE in 2020.
- Vulnerability: CVE-2021-44790
  - CVSS Score: 7.5
  - Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.
- Vulnerability: CVE-2013-0942
  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
- Vulnerability: CVE-2016-4979
  - CVSS Score: 5
  - Description: The Apache HTTP Server 2.4.18 through 2.4.20, when mod_http2 and mod_ssl are enabled, does not properly recognize the "SSLVerifyClient require" directive for HTTP/2 request authorization, which allows remote attackers to bypass intended access restrictions by leveraging the ability to send multiple requests over a single connection and aborting a renegotiation.
- Vulnerability: CVE-2012-3526
  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.
- Vulnerability: CVE-2018-1301
  - CVSS Score: 4.3
  - Description: A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.

- Vulnerability: CVE-2021-26690
  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service
- Vulnerability: CVE-2021-26691
  - CVSS Score: 7.5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow
- Vulnerability: CVE-2022-26377
  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.
- Vulnerability: CVE-2007-4723
  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.
- Vulnerability: CVE-2023-45802
  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.
- Vulnerability: CVE-2022-28614
  - CVSS Score: 5
  - Description: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.
- Vulnerability: CVE-2020-13938
  - CVSS Score: 2.1

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

- Vulnerability: CVE-2009-2299
  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.
- Vulnerability: CVE-2018-1283
  - CVSS Score: 3.5
  - Description: In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to forward its session data to CGI applications (SessionEnv on, not the default), a remote user may influence their content by using a "Session" header. This comes from the "HTTP_SESSION" variable name used by mod_session to forward its data to CGIs, since the prefix "HTTP_" is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications.
- Vulnerability: CVE-2019-10082
  - CVSS Score: 6.4
  - Description: In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.
- Vulnerability: CVE-2018-1312
  - CVSS Score: 6.8
  - Description: In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.
- Vulnerability: CVE-2016-8740
  - CVSS Score: 5
  - Description: The mod_http2 module in the Apache HTTP Server 2.4.17 through 2.4.23, when the Protocols configuration includes h2 or h2c, does not restrict request-header length, which allows remote attackers to cause a denial of service (memory consumption) via crafted CONTINUATION frames in an HTTP/2 request.
- Vulnerability: CVE-2016-8743
  - CVSS Score: 5
  - Description: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.
- Vulnerability: CVE-2024-40898
  - CVSS Score: N/A

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

- Vulnerability: CVE-2019-0217
  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.
- Vulnerability: CVE-2021-39275
  - CVSS Score: 7.5
  - Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.
- Vulnerability: CVE-2022-28615
  - CVSS Score: 6.4
  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.
- Vulnerability: CVE-2022-30556
  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.
- Vulnerability: CVE-2022-22719
  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.
- Vulnerability: CVE-2019-0220
  - CVSS Score: 5
  - Description: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.
- Vulnerability: CVE-2017-3169
  - CVSS Score: 7.5
  - Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.
- Vulnerability: CVE-2024-27316

  - CVSS Score: N/A
  - Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.
- Vulnerability: CVE-2017-7679
  - CVSS Score: 7.5
  - Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.
- Vulnerability: CVE-2013-2765
  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.
- Vulnerability: CVE-2020-1934
  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.
- Vulnerability: CVE-2018-17189
  - CVSS Score: 5
  - Description: In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 (mod_http2) connections.
- Vulnerability: CVE-2022-36760
  - CVSS Score: N/A
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.
- Vulnerability: CVE-2020-35452
  - CVSS Score: 6.8
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow
- Vulnerability: CVE-2017-9798
  - CVSS Score: 5

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

- Vulnerability: CVE-2016-1546
  - CVSS Score: 4.3
  - Description: The Apache HTTP Server 2.4.17 and 2.4.18, when mod_http2 is enabled, does not limit the number of simultaneous stream workers for a single HTTP/2 connection, which allows remote attackers to cause a denial of service (stream-processing outage) via modified flow-control windows.
- Vulnerability: CVE-2022-29404
  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.
- Vulnerability: CVE-2021-33193
  - CVSS Score: 5
  - Description: A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.
- Vulnerability: CVE-2009-0796
  - CVSS Score: 2.6
  - Description: Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.
- Vulnerability: CVE-2013-4365
  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.
- Vulnerability: CVE-2018-1333
  - CVSS Score: 5
  - Description: By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.18-2.4.30,2.4.33).
- Vulnerability: CVE-2022-22720
  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- Vulnerability: CVE-2018-11763
  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.17 to 2.4.34, by sending continuous, large SETTINGS frames a client can occupy a connection, server thread and CPU time without any connection timeout coming to effect. This affects only HTTP/2 connections. A possible mitigation is to not enable the h2 protocol.
- Vulnerability: CVE-2022-28330
  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.
- Vulnerability: CVE-2021-32791
  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider.
    In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.
- Vulnerability: CVE-2021-32792
  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using ‘OIDCPreservePost On‘.
- Vulnerability: CVE-2023-31122
  - CVSS Score: N/A
  - Description: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.
- Vulnerability: CVE-2016-8612
  - CVSS Score: 3.3
  - Description: Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.
- Vulnerability: CVE-2024-38476
  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.
- Vulnerability: CVE-2024-38477
  - CVSS Score: N/A

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

- Vulnerability: CVE-2024-38474
  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.
- Vulnerability: CVE-2019-0196
  - CVSS Score: 5
  - Description: A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.
- Vulnerability: CVE-2019-0211
  - CVSS Score: 7.2
  - Description: In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.
- Vulnerability: CVE-2022-22721
  - CVSS Score: 5.8
  - Description: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.
- Vulnerability: CVE-2006-20001
  - CVSS Score: N/A
  - Description: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.This issue affects Apache HTTP Server 2.4.54 and earlier.
- Vulnerability: CVE-2019-10092
  - CVSS Score: 4.3
  - Description: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.
- Vulnerability: CVE-2013-0941
  - CVSS Score: 2.1

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

- Vulnerability: CVE-2019-17567
  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.
- Vulnerability: CVE-2017-15715
  - CVSS Score: 6.8
  - Description: In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.
- Vulnerability: CVE-2022-31813
  - CVSS Score: 7.5
  - Description: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.
- Vulnerability: CVE-2012-4001
  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.
- Vulnerability: CVE-2019-10098
  - CVSS Score: 5.8
  - Description: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.
- Vulnerability: CVE-2022-37436
  - CVSS Score: N/A
  - Description: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.
- Vulnerability: CVE-2016-5387
  - CVSS Score: 6.8

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

- Vulnerability: CVE-2012-4360
  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
- Vulnerability: CVE-2021-40438
  - CVSS Score: 6.8
  - Description: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.
- Vulnerability: CVE-2011-1176
  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.
- Vulnerability: CVE-2022-23943
  - CVSS Score: 7.5
  - Description: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.
- Vulnerability: CVE-2020-1927
  - CVSS Score: 5.8
  - Description: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.
- Vulnerability: CVE-2018-17199
  - CVSS Score: 5
  - Description: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.
- Vulnerability: CVE-2017-9788
  - CVSS Score: 6.4

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

- Vulnerability: CVE-2017-15710
  - CVSS Score: 5
  - Description: In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.
- Vulnerability: CVE-2016-4975
  - CVSS Score: 4.3
  - Description: Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).
- Vulnerability: CVE-2018-1302
  - CVSS Score: 4.3
  - Description: When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.
- Vulnerability: CVE-2018-1303
  - CVSS Score: 5
  - Description: A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache. The vulnerability is considered as low risk since mod_cache_socache is not widely used, mod_cache_disk is not concerned by this vulnerability.
- Vulnerability: CVE-2017-3167
  - CVSS Score: 7.5
  - Description: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.

- Vulnerability: CVE-2021-34798
  - CVSS Score: 5
  - Description: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.
- Vulnerability: CVE-2023-25690
  - CVSS Score: N/A
  - Description: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:RewriteEngine onRewriteRule "/̂here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]ProxyPassReverse /here/ http://example.com:8080/Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.
- Vulnerability: CVE-2021-32786
  - CVSS Score: 5.8
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, ‘oidc_validate_redirect_url()‘ does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring ‘mod_auth_openidc‘ to only allow redirection whose destination matches a given regular expression.
- Vulnerability: CVE-2021-32785
  - CVSS Score: 4.3
  - Description: mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache (‘OIDCCacheEncrypt off‘, ‘OIDCSessionType server-cache‘, ‘OIDCCacheType redis‘), ‘mod_auth_openidc‘ wrongly performed argument interpolation before passing Redis requests to ‘hiredis‘, which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the ‘hiredis‘ API. As a workaround, this vulnerability can be mitigated by setting ‘OIDCCacheEncrypt‘ to ‘on‘, as cache keys are cryptographically hashed before use when this option is enabled.
- Vulnerability: CVE-2011-2688

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

- Vulnerability: CVE-2021-44224
  - CVSS Score: 6.4
  - Description: A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).

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

- Vulnerability: CVE-2021-44790
  - CVSS Score: 7.5
  - Description: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

- Vulnerability: CVE-2013-0942
  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- Vulnerability: CVE-2016-4979
  - CVSS Score: 5
  - Description: The Apache HTTP Server 2.4.18 through 2.4.20, when mod_http2 and mod_ssl are enabled, does not properly recognize the "SSLVerifyClient require" directive for HTTP/2 request authorization, which allows remote attackers to bypass intended access restrictions by leveraging the ability to send multiple requests over a single connection and aborting a renegotiation.

- Vulnerability: CVE-2012-3526
  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

- Vulnerability: CVE-2018-1301

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

- Vulnerability: CVE-2021-26690
  - CVSS Score: 5
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service
- Vulnerability: CVE-2021-26691
  - CVSS Score: 7.5
  - Description: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow
- Vulnerability: CVE-2022-26377
  - CVSS Score: 5
  - Description: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.
- Vulnerability: CVE-2007-4723
  - CVSS Score: 7.5
  - Description: Directory traversal vulnerability in Ragnarok Online Control Panel 4.3.4a, when the Apache HTTP Server is used, allows remote attackers to bypass authentication via directory traversal sequences in a URI that ends with the name of a publicly available page, as demonstrated by a "/...../" sequence and an account_manage.php/login.php final component for reaching the protected account_manage.php page.
- Vulnerability: CVE-2023-45802
  - CVSS Score: N/A
  - Description: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.This was found by the reporter during testing ofCVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.Users are recommended to upgrade to version 2.4.58, which fixes the issue.
- Vulnerability: CVE-2022-28614
  - CVSS Score: 5

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

- Vulnerability: CVE-2020-13938
  - CVSS Score: 2.1
  - Description: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows
- Vulnerability: CVE-2009-2299
  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.
- Vulnerability: CVE-2018-1283
  - CVSS Score: 3.5
  - Description: In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to forward its session data to CGI applications (SessionEnv on, not the default), a remote user may influence their content by using a "Session" header. This comes from the "HTTP_SESSION" variable name used by mod_session to forward its data to CGIs, since the prefix "HTTP_" is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications.
- Vulnerability: CVE-2019-10082
  - CVSS Score: 6.4
  - Description: In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.
- Vulnerability: CVE-2018-1312
  - CVSS Score: 6.8
  - Description: In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.
- Vulnerability: CVE-2016-8740
  - CVSS Score: 5
  - Description: The mod_http2 module in the Apache HTTP Server 2.4.17 through 2.4.23, when the Protocols configuration includes h2 or h2c, does not restrict request-header length, which allows remote attackers to cause a denial of service (memory consumption) via crafted CONTINUATION frames in an HTTP/2 request.
- Vulnerability: CVE-2016-8743
  - CVSS Score: 5

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

- Vulnerability: CVE-2024-40898
  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.
- Vulnerability: CVE-2019-0217
  - CVSS Score: 6
  - Description: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.
- Vulnerability: CVE-2021-39275
  - CVSS Score: 7.5
  - Description: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.
- Vulnerability: CVE-2022-28615
  - CVSS Score: 6.4
  - Description: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.
- Vulnerability: CVE-2022-30556
  - CVSS Score: 5
  - Description: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.
- Vulnerability: CVE-2022-22719
  - CVSS Score: 5
  - Description: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

11.3 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-2013-2765
  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.
- Vulnerability: CVE-2024-38476
  - CVSS Score: N/A

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

- Vulnerability: CVE-2024-38477
  - CVSS Score: N/A
  - Description: null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request.Users are recommended to upgrade to version 2.4.60, which fixes this issue.
- Vulnerability: CVE-2024-38474
  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.
- Vulnerability: CVE-2024-40898
  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.
- Vulnerability: CVE-2011-1176
  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.
- Vulnerability: CVE-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-2009-2299
  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.
- Vulnerability: CVE-2023-43622
  - 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-2024-27316
  - CVSS Score: N/A
  - Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.
- Vulnerability: CVE-2013-4365
  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.
- Vulnerability: CVE-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-2012-3526
  - CVSS Score: 5
  - Description: The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.
- Vulnerability: CVE-2012-4360
  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
- Vulnerability: CVE-2013-0941
  - CVSS Score: 2.1
  - Description: EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.
- Vulnerability: CVE-2013-0942
  - CVSS Score: 4.3
  - Description: Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
- Vulnerability: CVE-2012-4001
  - CVSS Score: 5
  - Description: The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.
- Vulnerability: CVE-2013-2765
  - CVSS Score: 5
  - Description: The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.
- Vulnerability: CVE-2024-38476
  - CVSS Score: N/A
  - Description: Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution viabackend applications whose response headers are malicious or exploitable.Users are recommended to upgrade to version 2.4.60, which fixes this issue.
- Vulnerability: CVE-2024-38477

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

- Vulnerability: CVE-2024-38474
  - CVSS Score: N/A
  - Description: Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts indirectories permitted by the configuration but not directly reachable by anyURL or source disclosure of scripts meant to only to be executed as CGI.Users are recommended to upgrade to version 2.4.60, which fixes this issue.Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.
- Vulnerability: CVE-2024-40898
  - CVSS Score: N/A
  - Description: SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests.Users are recommended to upgrade to version 2.4.62 which fixes this issue.
- Vulnerability: CVE-2011-1176
  - CVSS Score: 4.3
  - Description: The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.
- Vulnerability: CVE-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-2009-2299
  - CVSS Score: 5
  - Description: The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.
- Vulnerability: CVE-2023-43622
  - 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-2024-27316
  - CVSS Score: N/A
  - Description: HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.
- Vulnerability: CVE-2013-4365
  - CVSS Score: 7.5
  - Description: Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.
- Vulnerability: CVE-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-2012-3526
  - CVSS Score: 5

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

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

11.4 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.

11.5 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.

11.6 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: 80
  - Version: N/A
  - Location: https://edisonenergia.it/
- Service: N/A
  - Port: 443
  - Version: N/A
  - Location:

No vulnerabilities found for this IP address.

11.7 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/
- Service: N/A
  - Port: 8443
  - Version: N/A
  - Location: /

No vulnerabilities found for this IP address.

11.8 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.

11.9 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://resumedrafter.com/
- Service: N/A
  - Port: 443
  - Version: N/A
  - Location: /

No vulnerabilities found for this IP address.

11.10 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.

11.11 IP Address: 54.192.76.24

- Organization: Amazon.com, Inc.
- Operating System: N/A
- Critical Vulnerabilities: 0
- High Vulnerabilities: 0
- Medium Vulnerabilities: 0
- Low Vulnerabilities: 0
- Total Vulnerabilities: 0

Services Running on IP Address

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

No vulnerabilities found for this IP address.

11.12 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.

11.13 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.

11.14 IP Address: 156.54.148.62

- Organization: Telecom Italia 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: OpenSSH
  - Port: 22
  - Version: 7.2p2
  - Location:
- Service: nginx
  - Port: 80
  - Version: N/A
  - Location: https://consipsl3.edison.it/
- Service: nginx
  - Port: 443
  - Version: N/A
  - Location: http://consipsl3.edison.it/luce/login

No vulnerabilities found for this IP address.

11.15 IP Address: 37.72.32.222

- Organization: Edison Rinnovabili
- 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.

11.16 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.

11.17 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.

11.18 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.

11.19 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://benbrown.ca/
- Service: N/A
  - Port: 443
  - Version: N/A
  - Location: /

No vulnerabilities found for this IP address.

11.20 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.

11.21 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.

11.22 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: 80
  - Version: N/A
  - Location: /
- Service: Apache httpd
  - Port: 443
  - Version: N/A
  - Location: /

No vulnerabilities found for this IP address.

11.23 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.

11.24 IP Address: 37.72.32.244

- Organization: Edison Rinnovabili
- 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.

11.25 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.

11.26 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: 10443
  - Version: N/A
  - Location: /

No vulnerabilities found for this IP address.

11.27 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.

11.28 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.

11.29 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.

11.30 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.

11.31 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: 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.

11.32 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.

11.33 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: 80
  - Version: N/A
  - Location: https://www.service.eau.veolia.fr/
- Service: N/A
  - Port: 443
  - Version: N/A
  - Location: /

No vulnerabilities found for this IP address.

11.34 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.