Out-of-date Version (Apache)

CRITICAL

|  |  |  |
| --- | --- | --- |
| Certainty | : |  |
| URL | : | <https://zero.webappsecurity.com/> |
| Identified Version | : | 2.2.6 |
| Latest Version | : | 2.2.34 (in this branch) |
| Vulnerability Database | : | Result is based on 07/27/2023 20:30:00 vulnerability database content. |

CLASSIFICATION

|  |  |
| --- | --- |
| PCI DSS 3.2 | [6.2](https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss) |
| OWASP 2013 | [A9](http://www.owasp.org/index.php/Top_10_2013-A9) |
| OWASP 2017 | [A9](https://www.owasp.org/index.php/Top_10_2017-A9) |
| CWE | [829](http://cwe.mitre.org/data/definitions/829.html) |
| CAPEC | [310](http://capec.mitre.org/data/definitions/310.html) |
| HIPAA | [164.308(A)(1)(I)](http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf) |
| ISO27001 | [A.14.1.2](https://www.netsparker.com/compliance-reports/iso27001/control-objectives-and-controls/#A-14-1-2) |

Vulnerability Details

Netsparker identified you are using an out-of-date version of Apache.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

Remedy

Please upgrade your installation of Apache to the latest stable version.

Remedy References

[Downloading the Apache HTTP Server](https://httpd.apache.org/download.cgi)

Known Vulnerabilities in this Version

Apache HTTP Server CVE-2016-8743 Vulnerability

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.

Affected Versions

2.2.0 to 2.2.31

External References

[CVE-2016-8743](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-8743)

Apache HTTP Server CVE-2016-5387 Vulnerability

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](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-5387)"; in other words, this is not a CVE ID for a vulnerability.

Affected Versions

2.2.0 to 2.2.31

External References

[CVE-2016-5387](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-5387)

Apache HTTP Server Integer Overflow or Wraparound Vulnerability

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.

Affected Versions

2.0 to 2.4.53

External References

[CVE-2022-28615](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-28615)

Apache HTTP Server Insufficient Verification of Data Authenticity Vulnerability

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.

Affected Versions

2.0 to 2.4.53

External References

[CVE-2022-31813](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-31813)

Apache HTTP Server CVE-2012-0053 Vulnerability

protocol.c in the Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header information during construction of Bad Request (aka 400) error documents, which allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a (1) long or (2) malformed header in conjunction with crafted web script.

Affected Versions

2.2.0 to 2.2.21

External References

[CVE-2012-0053](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0053)

Apache HTTP Server CVE-2012-0883 Vulnerability

envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the LD\_LIBRARY\_PATH, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of apachectl.

Affected Versions

2.2.0 to 2.2.22

External References

[CVE-2012-0883](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0883)

Apache HTTP Server CVE-2013-1862 Vulnerability

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

Affected Versions

2.2.0 to 2.2.24

External References

[CVE-2013-1862](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1862)

Apache HTTP Server CVE-2013-1896 Vulnerability

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

Affected Versions

2.2.0 to 2.2.24

External References

[CVE-2013-1896](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1896)

Apache HTTP Server CVE-2013-6438 Vulnerability

The dav\_xml\_get\_cdata function in main/util.c in the mod\_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.

Affected Versions

2.2.0 to 2.2.26

External References

[CVE-2013-6438](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-6438)

Apache HTTP Server Uncontrolled Resource Consumption Vulnerability

The deflate\_in\_filter function in mod\_deflate.c in the mod\_deflate module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.

Affected Versions

2.2.0 to 2.2.28

External References

[CVE-2014-0118](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0118)

Apache HTTP Server Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') Vulnerability

Race condition in the mod\_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status\_handler function in modules/generators/mod\_status.c and the lua\_ap\_scoreboard\_worker function in modules/lua/lua\_request.c.

Affected Versions

2.2.0 to 2.2.28

External References

[CVE-2014-0226](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0226)

Apache HTTP Server CVE-2012-0031 Vulnerability

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

Affected Versions

2.2.0 to 2.2.21

External References

[CVE-2012-0031](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0031)

Apache HTTP Server Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

mod\_proxy\_ftp in Apache 2.2.x before 2.2.7-dev, 2.0.x before 2.0.62-dev, and 1.3.x before 1.3.40-dev does not define a charset, which allows remote attackers to conduct cross-site scripting (XSS) attacks using UTF-7 encoding.

Affected Versions

2.2.0 to 2.2.7

External References

[CVE-2008-0005](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-0005)

Apache HTTP Server Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

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

Affected Versions

2.2.0 to 2.2.22

External References

[CVE-2008-0455](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-0455)

Apache HTTP Server Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') Vulnerability

CRLF injection vulnerability in the mod\_negotiation module in the Apache HTTP Server 2.2.6 and earlier in the 2.2.x series, 2.0.61 and earlier in the 2.0.x series, and 1.3.39 and earlier in the 1.3.x series allows remote authenticated users to inject arbitrary HTTP headers and conduct HTTP response splitting attacks by uploading a file with a multi-line name containing HTTP header sequences and a file extension, which leads to injection within a (1) "406 Not Acceptable" or (2) "300 Multiple Choices" HTTP response when the extension is omitted in a request for the file.

Affected Versions

2.2.0 to 2.2.11

External References

[CVE-2008-0456](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-0456)

Apache HTTP Server Allocation of Resources Without Limits or Throttling Vulnerability

The ap\_proxy\_http\_process\_response function in mod\_proxy\_http.c in the mod\_proxy module in the Apache HTTP Server 2.0.63 and 2.2.8 does not limit the number of forwarded interim responses, which allows remote HTTP servers to cause a denial of service (memory consumption) via a large number of interim responses.

Affected Versions

2.2.0 to 2.2.8

External References

[CVE-2008-2364](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-2364)

Apache HTTP Server Uncontrolled Resource Consumption Vulnerability

The mod\_deflate module in Apache httpd 2.2.11 and earlier compresses large files until completion even after the associated network connection is closed, which allows remote attackers to cause a denial of service (CPU consumption).

Affected Versions

2.2.0 to 2.2.11

External References

[CVE-2009-1891](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1891)

Apache HTTP Server Other Vulnerability

The mod\_proxy\_ftp module in the Apache HTTP Server allows remote attackers to bypass intended access restrictions and send arbitrary commands to an FTP server via vectors related to the embedding of these commands in the Authorization HTTP header, as demonstrated by a certain module in VulnDisco Pack Professional 8.11.

Affected Versions

2.2.0 to 2.2.13

External References

[CVE-2009-3095](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3095)

Apache HTTP Server NULL Pointer Dereference Vulnerability

The ap\_proxy\_ftp\_handler function in modules/proxy/proxy\_ftp.c in the mod\_proxy\_ftp module in the Apache HTTP Server 2.0.63 and 2.2.13 allows remote FTP servers to cause a denial of service (NULL pointer dereference and child process crash) via a malformed reply to an EPSV command.

Affected Versions

2.2.0 to 2.2.13

External References

[CVE-2009-3094](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3094)

Apache HTTP Server Uncontrolled Resource Consumption Vulnerability

The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than [CVE-2007-0086](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-0086).

Affected Versions

2.2.0 to 2.2.19

External References

[CVE-2011-3192](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3192)

Apache HTTP Server Allocation of Resources Without Limits or Throttling Vulnerability

Stack consumption vulnerability in the fnmatch implementation in apr\_fnmatch.c in the Apache Portable Runtime (APR) library before 1.4.3 and the Apache HTTP Server before 2.2.18, and in fnmatch.c in libc in NetBSD 5.1, OpenBSD 4.8, FreeBSD, Apple Mac OS X 10.6, Oracle Solaris 10, and Android, allows context-dependent attackers to cause a denial of service (CPU and memory consumption) via \*? sequences in the first argument, as demonstrated by attacks against mod\_autoindex in httpd.

Affected Versions

2.2.0 to 2.2.18

External References

[CVE-2011-0419](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0419)

Apache HTTP Server Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

The ap\_read\_request function in server/protocol.c in the Apache HTTP Server 2.2.x before 2.2.15, when a multithreaded MPM is used, does not properly handle headers in subrequests in certain circumstances involving a parent request that has a body, which might allow remote attackers to obtain sensitive information via a crafted request that triggers access to memory locations associated with an earlier request.

Affected Versions

2.2.0 to 2.2.14

External References

[CVE-2010-0434](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0434)

Apache HTTP Server CVE-2014-0098 Vulnerability

The log\_cookie function in mod\_log\_config.c in the mod\_log\_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.

Affected Versions

2.2.0 to 2.2.26

External References

[CVE-2014-0098](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0098)

Apache HTTP Server CVE-2009-2699 Vulnerability

The Solaris pollset feature in the Event Port backend in poll/unix/port.c in the Apache Portable Runtime (APR) library before 1.3.9, as used in the Apache HTTP Server before 2.2.14 and other products, does not properly handle errors, which allows remote attackers to cause a denial of service (daemon hang) via unspecified HTTP requests, related to the prefork and event MPMs.

Affected Versions

2.2.0 to 2.2.13

External References

[CVE-2009-2699](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2699)

Apache HTTP Improper Initialization Server Vulnerability

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.

Affected Versions

0.8.11 to 2.4.52

External References

[CVE-2022-22719](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22719)

Apache HTTP Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') Server Vulnerability

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

Affected Versions

0.8.11 to 2.4.52

External References

[CVE-2022-22720](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22720)

Apache Denial of service in mod\_lua r:parsebody Vulnerability

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.

Affected Versions

0.8.11 to 2.4.53

External References

[CVE-2022-29404](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29404)

Apache read beyond bounds via ap\_rwrite() Vulnerability

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.

Affected Versions

0.8.11 to 2.4.53

External References

[CVE-2022-28614](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-28614)

Apache read beyond bounds in mod\_isapi Vulnerability

Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod\_isapi module.

Affected Versions

0.8.11 to 2.4.53

External References

[CVE-2022-28330](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-28330)

Apache HTTP Server Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

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.

Affected Versions

2.0 to 2.4.53

External References

[CVE-2022-30556](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30556)

Apache HTTP Server Integer Overflow or Wraparound Vulnerability

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.

Affected Versions

2.0 to 2.4.52

External References

[CVE-2022-22721](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22721)

Apache HTTP Server Out-of-bounds Write Vulnerability

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.

Affected Versions

2.0 to 2.4.48

External References

[CVE-2021-39275](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-39275)

Apache HTTP Server CVE-2013-5704 Vulnerability

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

Affected Versions

2.2.2 to 2.2.6

External References

[CVE-2013-5704](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-5704)

Apache HTTP Server Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Cross-site scripting (XSS) vulnerability in the (1) mod\_imap module in the Apache HTTP Server 1.3.0 through 1.3.39 and 2.0.35 through 2.0.61 and the (2) mod\_imagemap module in the Apache HTTP Server 2.2.0 through 2.2.6 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

Affected Versions

2.2.0 to 2.2.6

External References

[CVE-2007-5000](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-5000)

Apache HTTP Server Numeric Errors Vulnerability

Off-by-one error in the apr\_brigade\_vprintf function in Apache APR-util before 1.3.5 on big-endian platforms allows remote attackers to obtain sensitive information or cause a denial of service (application crash) via crafted input.

Affected Versions

2.2.0 to 2.2.11

External References

[CVE-2009-1956](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1956)

Apache HTTP Server NULL Pointer Dereference Vulnerability

mod\_auth\_openidc is an authentication and authorization module for the Apache 2.x HTTP server that implements the OpenID Connect Relying Party functionality. In versions 2.0.0 through 2.4.13.1, when `OIDCStripCookies` is set and a crafted cookie supplied, a NULL pointer dereference would occur, resulting in a segmentation fault. This could be used in a Denial-of-Service attack and thus presents an availability risk. Version 2.4.13.2 contains a patch for this issue. As a workaround, avoid using `OIDCStripCookies`.

Affected Versions

2.0.0 to 2.4.13

External References

[CVE-2023-28625](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-28625)

Apache HTTP Server Interpretation Conflict Vulnerability

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.

Affected Versions

2.0 to 2.4.54

External References

[CVE-2022-37436](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-37436)

Apache HTTP Server Uncontrolled Resource Consumption Vulnerability

[CVE-2009-1890](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1890) httpd: mod\_proxy reverse proxy DoS (infinite loop)

Affected Versions

2.2.0 to 2.2.11

External References

[CVE-2009-1890](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1890)

Apache HTTP Server Out-of-bounds Write Vulnerability

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.

Affected Versions

2.0 to 2.4.54

External References

[CVE-2006-20001](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-20001)

Apache HTTP Server Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

[CVE-2008-2939](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-2939) httpd: mod\_proxy\_ftp globbing XSS

Affected Versions

2.2.6

External References

[CVE-2008-2939](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-2939)

Apache HTTP Server Server-Side Request Forgery (SSRF) Vulnerability

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.

Affected Versions

0.8.11 to 2.4.48

External References

[CVE-2021-40438](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40438)

Apache HTTP Server NULL Pointer Dereference Vulnerability

Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

Affected Versions

0.8.11 to 2.4.48

External References

[CVE-2021-34798](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34798)

Apache HTTP Server Out-of-bounds Write Vulnerability

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.

Affected Versions

0.8.11 to 2.4.51

External References

[CVE-2021-44790](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-44790)

Apache HTTP Server Resource Management Errors Vulnerability

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

Affected Versions

2.2.6

External References

[CVE-2014-0231](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0231)

Apache HTTP Server Improper Input Validation Vulnerability

The lua\_websocket\_read function in lua\_request.c in the mod\_lua module in the Apache HTTP Server through 2.4.12 allows remote attackers to cause a denial of service (child-process crash) by sending a crafted WebSocket Ping frame after a Lua script has called the wsupgrade function.

Affected Versions

2.2 to 2.2.6

External References

[CVE-2015-0228](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0228)

Apache HTTP Server Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Multiple cross-site scripting (XSS) vulnerabilities in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via vectors involving hostnames and URIs in the (1) mod\_imagemap, (2) mod\_info, (3) mod\_ldap, (4) mod\_proxy\_ftp, and (5) mod\_status modules.

Affected Versions

2.2.6

External References

[CVE-2012-3499](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3499)

Apache HTTP Server Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Multiple cross-site scripting (XSS) vulnerabilities in the balancer\_handler function in the manager interface in mod\_proxy\_balancer.c in the mod\_proxy\_balancer module in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via a crafted string.

Affected Versions

2.2.6

External References

[CVE-2012-4558](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4558)

Apache HTTP Server Resource Management Errors Vulnerability

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

Affected Versions

2.2 to 2.2.6

External References

[CVE-2014-0231](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0231)

Apache HTTP Server DEPRECATED: Code Vulnerability

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

Affected Versions

2.2 to 2.2.6

External References

[CVE-2015-3183](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-3183)

Apache HTTP Server Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Multiple cross-site scripting (XSS) vulnerabilities in the make\_variant\_list function in mod\_negotiation.c in the mod\_negotiation module in the Apache HTTP Server 2.4.x before 2.4.3, when the MultiViews option is enabled, allow remote attackers to inject arbitrary web script or HTML via a crafted filename that is not properly handled during construction of a variant list.

Affected Versions

2.2.6

External References

[CVE-2012-2687](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2687)

Apache HTTP Server Other Vulnerability

The (1) mod\_cache and (2) mod\_dav modules in the Apache HTTP Server 2.2.x before 2.2.16 allow remote attackers to cause a denial of service (process crash) via a request that lacks a path.

Affected Versions

2.2.6 to 2.2.15

External References

[CVE-2010-1452](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1452)

Apache HTTP Server Improper Input Validation Vulnerability

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

Affected Versions

2.2.6

External References

[CVE-2011-3368](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3368)

Apache HTTP Server Numeric Errors Vulnerability

Integer overflow in the ap\_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod\_setenvif module is enabled, allows local users to gain privileges via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, leading to a heap-based buffer overflow.

Affected Versions

2.2.6

External References

[CVE-2011-3607](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3607)

Apache HTTP Server CVE-2010-0425 Vulnerability

modules/arch/win32/mod\_isapi.c in mod\_isapi in the Apache HTTP Server 2.0.37 through 2.0.63, 2.2.0 through 2.2.14, and 2.3.x before 2.3.7, when running on Windows, does not ensure that request processing is complete before calling isapi\_unload for an ISAPI .dll module, which allows remote attackers to execute arbitrary code via unspecified vectors related to a crafted request, a reset packet, and "orphaned callback pointers."

Affected Versions

2.2.6 to 2.2.14

External References

[CVE-2010-0425](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0425)

Apache HTTP Server Other Vulnerability

The ap\_proxy\_ajp\_request function in mod\_proxy\_ajp.c in mod\_proxy\_ajp in the Apache HTTP Server 2.2.x before 2.2.15 does not properly handle certain situations in which a client sends no request body, which allows remote attackers to cause a denial of service (backend server outage) via a crafted request, related to use of a 500 error code instead of the appropriate 400 error code.

Affected Versions

2.2.6

External References

[CVE-2010-0408](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0408)

Apache HTTP Server Resource Management Errors Vulnerability

The Apache HTTP Server 1.x and 2.x allows remote attackers to cause a denial of service (daemon outage) via partial HTTP requests, as demonstrated by Slowloris, related to the lack of the mod\_reqtimeout module in versions before 2.2.15.

Affected Versions

2.2 to 2.2.6

External References

[CVE-2007-6750](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6750)

Apache HTTP Server Resource Management Errors Vulnerability

The Apache HTTP Server 1.x and 2.x allows remote attackers to cause a denial of service (daemon outage) via partial HTTP requests, as demonstrated by Slowloris, related to the lack of the mod\_reqtimeout module in versions before 2.2.15.

Affected Versions

2.2.6

External References

[CVE-2007-6750](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6750)

Apache HTTP Server Improper Input Validation Vulnerability

The ap\_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod\_setenvif module is enabled, does not restrict the size of values of environment variables, which allows local users to cause a denial of service (memory consumption or NULL pointer dereference) via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, related to (1) the "len +=" statement and (2) the apr\_pcalloc function call, a different vulnerability than [CVE-2011-3607](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3607).

Affected Versions

2.2.6

External References

[CVE-2011-4415](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4415)

Apache HTTP Server Improper Input Validation Vulnerability

The mod\_proxy module in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x before 2.2.18, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers by using the HTTP/0.9 protocol with a malformed URI containing an initial @ (at sign) character. NOTE: this vulnerability exists because of an incomplete fix for [CVE-2011-3368](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3368).

Affected Versions

2.2.6

External References

[CVE-2011-3639](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3639)

Apache HTTP Server Improper Input Validation Vulnerability

The mod\_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an @ (at sign) character and a : (colon) character in invalid positions. NOTE: this vulnerability exists because of an incomplete fix for [CVE-2011-3368](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3368).

Affected Versions

2.2.6

External References

[CVE-2011-4317](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4317)

Apache HTTP Server Configuration Vulnerability

The Apache HTTP Server 2.2.11 and earlier 2.2 versions does not properly handle Options=IncludesNOEXEC in the AllowOverride directive, which allows local users to gain privileges by configuring (1) Options Includes, (2) Options +Includes, or (3) Options +IncludesNOEXEC in a .htaccess file, and then inserting an exec element in a .shtml file.

Affected Versions

2.2 to 2.2.6

External References

[CVE-2009-1195](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1195)

Apache HTTP Server Configuration Vulnerability

The Apache HTTP Server 2.2.11 and earlier 2.2 versions does not properly handle Options=IncludesNOEXEC in the AllowOverride directive, which allows local users to gain privileges by configuring (1) Options Includes, (2) Options +Includes, or (3) Options +IncludesNOEXEC in a .htaccess file, and then inserting an exec element in a .shtml file.

Affected Versions

2.2.6 to 2.2.10

External References

[CVE-2009-1195](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1195)

Apache HTTP Server Cryptographic Issues Vulnerability

The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0, mod\_ssl in the Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a "plaintext injection" attack, aka the "Project Mogul" issue.

Affected Versions

2.2 to 2.2.6

External References

[CVE-2009-3555](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3555)

Apache HTTP Server Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

Apache HTTP Server, when running on Linux with a document root on a Windows share mounted using smbfs, allows remote attackers to obtain unprocessed content such as source files for .php programs via a trailing "\" (backslash), which is not handled by the intended AddType directive.

Affected Versions

2.2.6

External References

[CVE-2007-6514](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6514)

Apache HTTP Server Resource Management Errors Vulnerability

The balancer\_handler function in mod\_proxy\_balancer in the Apache HTTP Server 2.2.0 through 2.2.6, when a threaded Multi-Processing Module is used, allows remote authenticated users to cause a denial of service (child process crash) via an invalid bb variable.

Affected Versions

2.2.6

External References

[CVE-2007-6422](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6422)

Apache HTTP Server Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Cross-site scripting (XSS) vulnerability in mod\_status in the Apache HTTP Server 2.2.0 through 2.2.6, 2.0.35 through 2.0.61, and 1.3.2 through 1.3.39, when the server-status page is enabled, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

Affected Versions

2.2.6

External References

[CVE-2007-6388](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6388)

Apache HTTP Server Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Cross-site scripting (XSS) vulnerability in balancer-manager in mod\_proxy\_balancer in the Apache HTTP Server 2.2.0 through 2.2.6 allows remote attackers to inject arbitrary web script or HTML via the (1) ss, (2) wr, or (3) rr parameters, or (4) the URL.

Affected Versions

2.2.6

External References

[CVE-2007-6421](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6421)

Apache HTTP Server Resource Management Errors Vulnerability

\*\* DISPUTED \*\* Unspecified vulnerability in mod\_proxy\_balancer for Apache HTTP Server 2.2.x before 2.2.7-dev, when running on Windows, allows remote attackers to trigger memory corruption via a long URL. NOTE: the vendor could not reproduce this issue.

Affected Versions

2.2.6

External References

[CVE-2007-6423](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6423)

Apache HTTP Server Cross-Site Request Forgery (CSRF) Vulnerability

Cross-site request forgery (CSRF) vulnerability in the balancer-manager in mod\_proxy\_balancer for Apache HTTP Server 2.2.x allows remote attackers to gain privileges via unspecified vectors.

Affected Versions

2.2.6

External References

[CVE-2007-6420](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6420)

Apache HTTP Server Out-of-bounds Read Vulnerability

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.

Affected Versions

2.2 to 2.2.6

External References

[CVE-2018-1303](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1303)

Apache HTTP Server NULL Pointer Dereference Vulnerability

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.

Affected Versions

2.2 to 2.2.6

External References

[CVE-2018-1302](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1302)

Apache HTTP Server Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

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.

Affected Versions

2.2 to 2.2.6

External References

[CVE-2018-1301](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1301)

Apache HTTP Server Improper Neutralization of CRLF Sequences ('CRLF Injection') Vulnerability

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).

Affected Versions

2.2.6

External References

[CVE-2016-4975](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-4975)

Apache HTTP Server Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

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.

Affected Versions

2.2.0 to 2.2.6

External References

[CVE-2017-7679](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-7679)

Apache HTTP Server Improper Input Validation Vulnerability

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.

Affected Versions

2.2 to 2.2.6

External References

[CVE-2017-9788](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-9788)

Apache HTTP Server Use After Free Vulnerability

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.

Affected Versions

2.2 to 2.2.6

External References

[CVE-2017-9798](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-9798)

Apache HTTP Server Improper Input Validation Vulnerability

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.

Affected Versions

2.2 to 2.2.6

External References

[CVE-2016-8612](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-8612)