Apache HTTP Server 2.4 vulnerabilities

This page lists all security vulnerabilities fixed in released versions of Apache HTTP Server 2.4. Each vulnerability is given a security impact rating by the Apache security team - please note that this rating may well vary from platform to platform. We also list the versions the flaw is known to affect, and where a flaw has not been verified list the version with a question mark.

Please note that if a vulnerability is shown below as being fixed in a "-dev" release then this means that a fix has been applied to the development source tree and will be part of an upcoming full release.

Please send comments or corrections for these vulnerabilities to the Security Team.

The initial GA release, Apache httpd 2.4.1, includes fixes for all vulnerabilities which have been resolved in Apache httpd 2.2.22 and all older releases. Consult the Apache httpd 2.2 vulnerabilities list for more information.

Fixed in Apache HTTP Server 2.4.67

important: Apache HTTP Server: http2: double free and possible RCE on early reset (CVE-2026-23918)

Double Free and possible RCE vulnerability in Apache HTTP Server with the HTTP/2 protocol.

This issue affects Apache HTTP Server: 2.4.66.

Users are recommended to upgrade to version 2.4.67, which fixes the issue.

Acknowledgements:

- finder: Bartlomiej Dmitruk, striga.ai
- finder: Stanislaw Strzalkowski, isec.pl

Reported to security team	2025-12-10
fixed in r1930444	2025-12-11
Update 2.4.67 released	2026-05-04
Affects	2.4.66

moderate: Apache HTTP Server: mod_rewrite elevation of privileges via ap_expr (CVE-2026-24072)

An escalation of privilege bug in various modules in Apache HTTP 2.4.66 and earlier allows local .htaccess authors to read files with the privileges of the httpd user.

Users are recommended to upgrade to version 2.4.67, which fixes this issue.

Acknowledgements: finder: y7syeu

Report received	2026-01-20
Update 2.4.67 released	2026-05-04
Affects	through 2.4.66

low: Apache HTTP Server: buffer overflow in mod_proxy_ajp via ajp_msg_check_header() (CVE-2026-28780)

Heap-based Buffer Overflow vulnerability in mod_proxy_ajp of Apache HTTP Server.

If mod_proxy_ajp connects to a malicious AJP server this AJP server can send a malicious AJP message back to mod_proxy_ajp and cause it to write 4 attacker controlled bytes after the end of a heap based buffer.

This issue affects Apache HTTP Server: through 2.4.66.

Users are recommended to upgrade to version 2.4.67, which fixes the issue.

Acknowledgements:

- finder: Andrew Lacambra
- finder: Elhanan Haenel
- finder: Tianshuo Han (<hantianshuo233@gmail.com>)
- finder: Tristan Madani

Reported to security team	2026-02-04
Reported to security team	2026-03-18
Reported to security team	2026-02-28
Update 2.4.67 released	2026-05-04
Affects	through 2.4.66

low: Apache HTTP Server: mod_md unrestricted OCSP response (CVE-2026-29168)

Allocation of Resources Without Limits or Throttling vulnerability in Apache HTTP Server's mod_md via OCSP response data.

This issue affects Apache HTTP Server: from 2.4.30 through 2.4.66.

Users are recommended to upgrade to version 2.4.67, which fixes the issue.

Acknowledgements: finder: Pavel Kohout, Aisle Research, Aisle.com

Reported to security team	2026-03-02
Update 2.4.67 released	2026-05-04
Affects	2.4.30 through 2.4.66

low: Apache HTTP Server: mod_dav_lock indirect lock crash (CVE-2026-29169)

A NULL pointer dereference in mod_dav_lock in Apache HTTP Server 2.4.66 and earlier may allow an attacker to crash the server with a malicious request.mod_dav_lock is not used internally by mod_dav or mod_dav_fs.

The only known use-case for mod_dav_lock was mod_dav_svn from Apache Subversion earlier than version 1.2.0.

Users are recommended to upgrade to version 2.4.67, which fixes this issue, or remove mod_dav_lock.

Acknowledgements: finder: Pavel Kohout, Aisle Research, Aisle.com

Report received	2026-03-04
Update 2.4.67 released	2026-05-04
Affects	through 2.4.66

moderate: Apache HTTP Server: mod_auth_digest timing attack (CVE-2026-33006)

A timing attack against mod_auth_digest in Apache HTTP Server 2.4.66 allows a bypass of Digest authentication by a remote attacker.

Users are recommended to upgrade to version 2.4.67, which fixes this issue.

Acknowledgements: finder: Nitescu Lucian

Report received	2026-03-09
Update 2.4.67 released	2026-05-04
Affects	through 2.4.66

low: Apache HTTP Server: mod_authn_socache crash (CVE-2026-33007)

A NULL pointer dereference in the mod_authn_socache in Apache HTTP Server 2.4.66 and earlier allows an unauthenticated remote user to crash a child process in a caching forward proxy configuration.

Users are recommended to upgrade to version 2.4.67, which fixes this issue.

Acknowledgements:

- finder: Pavel Kohout, Aisle Research, Aisle.com
- finder: Arkadi Vainbrand

Report received	2026-03-04
Update 2.4.67 released	2026-05-04
fixed in 2.4.x by r1933358	2026-05-04
Affects	2.4.0 through 2.4.66

low: Apache HTTP Server: multiple modules: HTTP response splitting forwarding malicious status line (CVE-2026-33523)

HTTP response splitting vulnerability in multiple Apache HTTP Server modules with untrusted or compromised backend servers.

This issue affects Apache HTTP Server: from through 2.4.66.

Users are recommended to upgrade to version 2.4.67, which fixes the issue.

Acknowledgements:

- finder: Haruki Oyama (Waseda University)
- finder: Merih Mengisteab
- finder: Dawit Jeong

Reported to security team	2026-03-05
Update 2.4.67 released	2026-05-04
Affects	2.4.0 through 2.4.66

low: Apache HTTP Server: Off-by-one OOB reads in AJP getter functions (CVE-2026-33857)

Out-of-bounds Read vulnerability in mod_proxy_ajp of

Apache HTTP Server.

This issue affects Apache HTTP Server: through 2.4.66.

Users are recommended to upgrade to version 2.4.67, which fixes the issue.

Acknowledgements: finder: Elhanan Haenel

Reported	2026-03-20
Update 2.4.67 released	2026-05-04
Affects	through 2.4.66

low: Apache HTTP Server: mod_proxy_ajp: Heap Buffer Over-Read Due to Missing Null-Termination Check (ajp_msg_get_string) (CVE-2026-34032)

Improper Null Termination, Out-of-bounds Read vulnerability in Apache HTTP Server.

This issue affects Apache HTTP Server: through 2.4.66.

Users are recommended to upgrade to version 2.4.67, which fixes the issue.

Acknowledgements:

- finder: Tianshuo Han (<hantianshuo233@gmail.com>)
- finder: Jérôme Djouder

Report received	2026-03-01
Update 2.4.67 released	2026-05-04
Affects	through 2.4.66

low: Apache HTTP Server: mod_proxy_ajp: Heap Over-Read and memory disclosure in ajp_parse_data() (CVE-2026-34059)

Buffer Over-read vulnerability in Apache HTTP Server.

This issue affects Apache HTTP Server: through 2.4.66.

Users are recommended to upgrade to version 2.4.67, which fixes the issue.

Acknowledgements: finder: Elhanan Haenel

Report received	2026-03-20

Update 2.4.67 released	2026-05-04
Affects	through 2.4.66

Fixed in Apache HTTP Server 2.4.66

low: Apache HTTP Server: mod_md (ACME), unintended retry intervals (CVE-2025-55753)

An integer overflow in the case of failed ACME certificate renewal leads, after a number of failures (~30 days in default configurations), to the backoff timer becoming 0. Attempts to renew the certificate then are repeated without delays until it succeeds.

This issue affects Apache HTTP Server: from 2.4.30 before 2.4.66.

Users are recommended to upgrade to version 2.4.66, which fixes the issue.

Acknowledgements: finder: Aisle Research

Reported to security team	2025-08-15
Update 2.4.66 released	2025-12-04
Affects	2.4.30 before 2.4.66

moderate: Apache HTTP Server: Server Side Includes adds query string to #exec cmd=... (CVE-2025-58098)

Apache HTTP Server 2.4.65 and earlier with Server Side Includes (SSI) enabled and mod_cgid (but not mod_cgi) passes the shell-escaped query string to #exec cmd="..." directives.

This issue affects Apache HTTP Server before 2.4.66.

Users are recommended to upgrade to version 2.4.66, which fixes the issue.

Acknowledgements: finder: Anthony Parfenov (United Rentals, Inc.)

Reported to security team	2025-08-21
Update 2.4.66 released	2025-12-04
Affects	before 2.4.66

moderate: Apache HTTP Server: NTLM Leakage on Windows through UNC SSRF (CVE-2025-59775)

Server-Side Request Forgery (SSRF) vulnerability

in Apache HTTP Server on Windows

with AllowEncodedSlashes On and MergeSlashes Off allows to potentially leak NTLM

hashes to a malicious server via SSRF and malicious requests or content

Users are recommended to upgrade to version 2.4.66, which fixes the issue.

Acknowledgements: finder: Orange Tsai (@orange_8361) from DEVCORE

Reported to security team	2025-09-10
Update 2.4.66 released	2025-12-04
Affects	through 2.4.65

low: Apache HTTP Server: CGI environment variable override (CVE-2025-65082)

Improper Neutralization of Escape, Meta, or Control Sequences vulnerability in Apache HTTP Server through environment variables set via the Apache configuration unexpectedly superseding variables calculated by the server for CGI programs.

This issue affects Apache HTTP Server from 2.4.0 through 2.4.65.

Users are recommended to upgrade to version 2.4.66 which fixes the issue.

Acknowledgements: finder: Mattias Åsander (Umeå University)

Reported to security team	2025-11-14
Update 2.4.66 released	2025-12-04
Affects	2.4.0 through 2.4.65

moderate: Apache HTTP Server: mod_userdir+suexec bypass via AllowOverride FileInfo (CVE-2025-66200)

mod_userdir+suexec bypass via AllowOverride FileInfo vulnerability in Apache HTTP Server. Users with access to use the RequestHeader directive in htaccess can cause some CGI scripts to run under an unexpected userid.

This issue affects Apache HTTP Server: from 2.4.7 through 2.4.65.

Users are recommended to upgrade to version 2.4.66, which fixes the issue.

Acknowledgements: finder: Mattias Åsander (Umeå University)

Reported to security team	2025-11-19
Update 2.4.66 released	2025-12-04
Affects	2.4.7 through 2.4.65

Fixed in Apache HTTP Server 2.4.65

moderate: Apache HTTP Server: 'RewriteCond expr' always evaluates to true in 2.4.64 (CVE-2025-54090)

A bug in Apache HTTP Server 2.4.64 results in all "RewriteCond expr ..." tests evaluating as "true".

Users are recommended to upgrade to version 2.4.65, which fixes the issue.

Reported to security team	2025-07-16
Update 2.4.65 released	2025-07-23
Affects	2.4.64

Fixed in Apache HTTP Server 2.4.64

moderate: Apache HTTP Server: HTTP response splitting (CVE-2024-42516)

HTTP response splitting in the core of Apache HTTP Server allows an attacker who can manipulate the Content-Type response headers of applications hosted or proxied by the server can split the HTTP response.

This vulnerability was described as CVE-2023-38709 but the patch included in Apache HTTP Server 2.4.59 did not address the issue.

Users are recommended to upgrade to version 2.4.64, which fixes this issue.

Reported to security team	2024-07-18
Update 2.4.64 released	2025-07-10
Affects	2.4.0 through 2.4.63

low: Apache HTTP Server: SSRF with mod_headers setting Content-Type header (CVE-2024-43204)

SSRF in Apache HTTP Server with mod_proxy loaded allows an attacker to send outbound proxy requests to a URL controlled by the attacker. Requires an unlikely configuration where mod_headers is configured to modify the Content-Type request or response header with a value provided in the HTTP request.

Users are recommended to upgrade to version 2.4.64 which fixes this issue.

Acknowledgements: finder: xiaojunjie@安恒信息杭州市滨江区技能大师工作室

Reported to security team	2024-08-07
2.4.x revision	2025-07-07
Update 2.4.64 released	2025-07-10
Affects	2.4.0 through 2.4.63

moderate: Apache HTTP Server: SSRF on Windows due to UNC paths (CVE-2024-43394)

Server-Side Request Forgery (SSRF) in Apache HTTP Server on Windows allows to potentially leak NTLM hashes to a malicious server via

mod_rewrite or apache expressions that pass unvalidated request input.

This issue affects Apache HTTP Server: from 2.4.0 through 2.4.63.

Note: The Apache HTTP Server Project will be setting a higher bar for accepting vulnerability reports regarding SSRF via UNC paths.

The server offers limited protection against administrators directing the server to open UNC paths.

Windows servers should limit the hosts they will connect over via SMB based on the nature of NTLM authentication.

Acknowledgements: finder: Kainan Zhang (@4xpl0r3r) from Fortinet

Reported to security team	2024-08-10
Update 2.4.64 released	2025-07-10
Affects	2.4.0 through 2.4.63

low: Apache HTTP Server: mod_ssl error log variable escaping (CVE-2024-47252)

Insufficient escaping of user-supplied data in mod_ssl in Apache HTTP Server 2.4.63 and earlier allows an untrusted SSL/TLS client to insert escape characters into log files in some configurations.

In a logging configuration where CustomLog is used with "%{varname}x" or "%{varname}c" to log variables provided by mod_ssl such as SSL_TLS_SNI, no escaping is performed by either mod_log_config or mod_ssl and unsanitized data provided by the client may appear in log files.

Acknowledgements: finder: John Runyon

Reported to security team	2024-09-18
Update 2.4.64 released	2025-07-10
Affects	2.4 through 2.4.63

moderate: Apache HTTP Server: mod_ssl access control bypass with session resumption (CVE-2025-23048)

In some mod_ssl configurations on Apache HTTP Server 2.4.35 through to 2.4.62, an access control bypass by trusted clients is possible using TLS 1.3 session resumption.

Configurations are affected when mod_ssl is configured for multiple virtual hosts, with each restricted to a different set of trusted client certificates (for example with a different SSLCACertificateFile/Path setting). In such a case, a client trusted to access one virtual host may be able to access another virtual host, if SSLStrictSNIVHostCheck is not enabled in either virtual host.

Acknowledgements: finder: Sven Hebrok, Felix Cramer, Tim Storm, Maximilian Radoy, and Juraj Somorovsky at Paderborn University

Reported to security team	2024-11-25
Update 2.4.64 released	2025-07-10
Affects	2.4.35 through 2.4.63

low: Apache HTTP Server: mod_proxy_http2 denial of service (CVE-2025-49630)

In certain proxy configurations, a denial of service attack against Apache HTTP Server versions 2.4.26 through to 2.4.63 can be triggered by untrusted clients causing an assertion in mod_proxy_http2.

Configurations affected are a reverse proxy is configured for an HTTP/2 backend, with ProxyPreserveHost set to "on".

Acknowledgements: finder: Anthony CORSIEZ

Report received	2025-06-04

Update 2.4.64 released	2025-07-10
Affects	2.4.26 through 2.4.63

moderate: Apache HTTP Server: mod_ssl TLS upgrade attack (CVE-2025-49812)

In some mod_ssl configurations on Apache HTTP Server versions through to 2.4.63, an HTTP desynchronisation attack allows a man-in-the-middle attacker to hijack an HTTP session via a TLS upgrade.

Only configurations using "SSLEngine optional" to enable TLS upgrades are affected. Users are recommended to upgrade to version 2.4.64, which removes support for TLS upgrade.

Acknowledgements:

- finder: Robert Merget (Technology Innovation Institute)
- finder: Nurullah Erinola (Ruhr University Bochum)
- finder: Marcel Maehren (Ruhr University Bochum)
- finder: Lukas Knittel (Ruhr University Bochum)
- finder: Sven Hebrok (Paderborn University)
- finder: Marcus Brinkmann (Ruhr University Bochum)
- finder: Juraj Somorovsky (Paderborn University)
- finder: Jörg Schwenk (Ruhr University Bochum)

Report received	2025-04-22
Update 2.4.64 released	2025-07-10
Affects	through 2.4.63

moderate: Apache HTTP Server: HTTP/2 DoS by Memory Increase (CVE-2025-53020)

Late Release of Memory after Effective Lifetime vulnerability in Apache HTTP Server.

This issue affects Apache HTTP Server: from 2.4.17 up to 2.4.63.

Users are recommended to upgrade to version 2.4.64, which fixes the issue.

Acknowledgements: finder: Gal Bar Nahum

Reported to security team	2025-06-18
fix developed	2025-06-19
Update 2.4.64 released	2025-07-10
Affects	2.4.17 through 2.4.63

Fixed in Apache HTTP Server 2.4.62

important: Apache HTTP Server: source code disclosure with handlers configured via AddType (CVE-2024-40725)

A partial fix for CVE-2024-39884 in the core of Apache HTTP Server 2.4.61 ignores some use of the legacy content-type based configuration of handlers. "AddType" and similar configuration, under some circumstances where files are requested indirectly, result in source code disclosure of local content. For example, PHP scripts may be served instead of interpreted.

Users are recommended to upgrade to version 2.4.62, which fixes this issue.

Reported to security team	2024-07-09
fixed by r1919249 in 2.4.x	2024-07-15
Update 2.4.62 released	2024-07-17
Affects	2.4.60 through 2.4.61

important: Apache HTTP Server: SSRF with mod_rewrite in server/vhost context on Windows (CVE-2024-40898)

SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTLM hashes to a malicious server via SSRF and malicious requests.

Users are recommended to upgrade to version 2.4.62 which fixes this issue.

Acknowledgements:

- finder: Smi1e (DBAPPSecurity Ltd.)
- finder: xiaojunjie (DBAPPSecurity Ltd.)

Reported to security team	2024-07-12
fixed by r1919248 in 2.4.x	2024-07-15
Update 2.4.62 released	2024-07-17
Affects	2.4.0 through 2.4.61

Fixed in Apache HTTP Server 2.4.61

important: Apache HTTP Server: source code disclosure with handlers configured via AddType (CVE-2024-39884)

A regression in the core of Apache HTTP Server 2.4.60 ignores some use of the legacy content-type based configuration of handlers. "AddType" and similar configuration, under some circumstances where files are requested indirectly, result in source code disclosure of local content. For example, PHP scripts may be served instead of interpreted.

Users are recommended to upgrade to version 2.4.61, which fixes this issue.

Reported to security team	2024-07-01
fixed by r1918839 in 2.4.x	2024-07-03
Update 2.4.61 released	2024-07-03
Affects	2.4.60

Fixed in Apache HTTP Server 2.4.60

low: Apache HTTP Server: DoS by Null pointer in websocket over HTTP/2 (CVE-2024-36387)

Serving WebSocket protocol upgrades over a HTTP/2 connection could result in a Null Pointer dereference, leading to a crash of the server process, degrading performance.

Acknowledgements: finder: Marc Stern (<marc.stern@approach-cyber.com>)

fixed in r1918003 in trunk	2024-05-27
fixed by r1918557 in 2.4.x	2024-07-01
Update 2.4.60 released	2024-07-01
Affects	2.4.55 through 2.4.59

important: Apache HTTP Server on WIndows UNC SSRF (CVE-2024-38472)

SSRF in Apache HTTP Server on Windows allows to potentially leak NTLM hashes to a malicious server via SSRF and malicious requests or content

Users are recommended to upgrade to version 2.4.60 which fixes this issue. Note: Existing configurations that access UNC paths will have to configure new directive "UNCList" to allow access during request processing.

Acknowledgements: finder: Orange Tsai (@orange_8361) from DEVCORE

Reported to security team	2024-04-01
fixed by r1918558 in 2.4.x	2024-07-01
Update 2.4.60 released	2024-07-01
Affects	2.4.0 through 2.4.59

moderate: Apache HTTP Server proxy encoding problem (CVE-2024-38473)

Encoding problem in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows request URLs with incorrect encoding to be sent to backend services, potentially bypassing authentication via crafted requests. This affects configurations where mechanisms other than ProxyPass/ProxyPassMatch or RewriteRule with the 'P' flag are used to configure a request to be proxied, such as SetHandler or inadvertent proxying via CVE-2024-39573. Note that these alternate mechanisms may be used within .htaccess.

Users are recommended to upgrade to version 2.4.60, which fixes this issue.

Acknowledgements: finder: Orange Tsai (@orange_8361) from DEVCORE

Reported to security team	2024-04-01
fixed by r1918559, r1918666, r1918600, r1918625, r1918668 in 2.4.x	2024-07-01
Update 2.4.60 released	2024-07-01
Affects	2.4.0 through 2.4.59

important: Apache HTTP Server weakness with encoded question marks in backreferences (CVE-2024-38474)

Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts in directories

permitted by the configuration but not directly reachable by any URL 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.

Acknowledgements: finder: Orange Tsai (@orange_8361) from DEVCORE

Reported to security team	2024-04-01
fixed by r1918561 in 2.4.x	2024-07-01
Update 2.4.60 released	2024-07-01
Affects	2.4.0 through 2.4.59

important: Apache HTTP Server weakness in mod_rewrite when first segment of substitution matches filesystem path. (CVE-2024-38475)

Improper escaping of output in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to map URLs to filesystem locations that are permitted to be served by the server but are not intentionally/directly reachable by any URL, resulting in code execution or source code disclosure.

Substitutions in server context that use a backreferences or variables as the first segment of the substitution are affected. Some unsafe RewiteRules will be broken by this change and the rewrite flag "UnsafePrefixStat" can be used to opt back in once ensuring the substitution is appropriately constrained.

Acknowledgements: finder: Orange Tsai (@orange_8361) from DEVCORE

Reported to security team	2024-04-01
fixed by r1918561 in 2.4.x	2024-07-01
Update 2.4.60 released	2024-07-01
Affects	2.4.0 through 2.4.59

important: Apache HTTP Server may use exploitable/malicious backend application output to run local handlers via internal redirect (CVE-2024-38476)

Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution via backend applications whose response headers are malicious or exploitable.

Note: Some legacy uses of the 'AddType' directive to connect a request to a handler must be ported to 'SetHandler' after this fix.

Users are recommended to upgrade to version 2.4.60, which fixes this issue.

Acknowledgements: finder: Orange Tsai (@orange_8361) from DEVCORE

Reported to security team	2024-04-01
fixed by r1918560 in 2.4.x	2024-07-01

Update 2.4.60 released	2024-07-01
Affects	2.4.0 through 2.4.59

important: Apache HTTP Server: Crash resulting in Denial of Service in mod_proxy via a malicious request (CVE-2024-38477)

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.

Acknowledgements: finder: Orange Tsai (@orange_8361) from DEVCORE

Reported	2024-04-01
fixed by r1918607 in 2.4.x	2024-07-01
Update 2.4.60 released	2024-07-01
Affects	2.4.0 through 2.4.59

moderate: Apache HTTP Server: mod_rewrite proxy handler substitution (CVE-2024-39573)

Potential SSRF in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to cause unsafe RewriteRules to unexpectedly setup URL's to be handled by mod_proxy.

Users are recommended to upgrade to version 2.4.60, which fixes this issue.

Acknowledgements: finder: Orange Tsai (@orange_8361) from DEVCORE

Reported to security team	2024-04-01
Update 2.4.60 released	2024-07-01
Affects	2.4.0 through 2.4.59

Fixed in Apache HTTP Server 2.4.59

moderate: Apache HTTP Server: HTTP response splitting (CVE-2023-38709)

Faulty input validation in the core of Apache allows malicious or exploitable backend/content generators to split HTTP responses.

This issue affects Apache HTTP Server: through 2.4.58.

Acknowledgements: finder: Orange Tsai (@orange_8361) from DEVCORE

Reported to security team	2023-06-26
Update 2.4.59 released	2024-04-04
Affects	through 2.4.58

low: Apache HTTP Server: HTTP Response Splitting in multiple modules (CVE-2024-24795)

HTTP Response splitting in multiple modules in Apache HTTP Server allows an attacker that can inject malicious response headers into backend applications to cause an HTTP desynchronization attack.

Users are recommended to upgrade to version 2.4.59, which fixes this issue.

Acknowledgements:

- finder: Keran Mu, Tsinghua University and Zhongguancun Laboratory.
- finder: Jianjun Chen, Tsinghua University and Zhongguancun Laboratory.

Reported to security team	2023-09-06
Update 2.4.59 released	2024-04-04
Affects	2.4.0 through 2.4.58

moderate: Apache HTTP Server: HTTP/2 DoS by memory exhaustion on endless continuation frames (CVE-2024-27316)

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.

Acknowledgements: finder: Bartek Nowotarski (https://nowotarski.info/)

Reported to security team	2024-02-22
Update 2.4.59 released	2024-04-04
Affects	2.4.17 through 2.4.58

Fixed in Apache HTTP Server 2.4.58

low: mod_macro buffer over-read (CVE-2023-31122)

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

Acknowledgements: finder: David Shoon (github/davidshoon)

Update 2.4.58 released	2023-10-19
Affects	through 2.4.57

low: Apache HTTP Server: DoS in HTTP/2 with initial windows size 0 (CVE-2023-43622)

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.

Acknowledgements:

- finder: Prof. Sven Dietrich (City University of New York)
- finder: Isa Jafarov (City University of New York)
- finder: Prof. Heejo Lee (Korea University)
- finder: Choongin Lee (Korea University)

Reported to security team	2023-09-15
Update 2.4.58 released	2023-10-19
Affects	2.4.55 through 2.4.57

moderate: Apache HTTP Server: HTTP/2 stream memory not reclaimed right away on RST (CVE-2023-45802)

When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.

This was found by the reporter during testing of CVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.

Users are recommended to upgrade to version 2.4.58, which fixes the issue.

Acknowledgements:

- finder: Will Dormann of Vul Labs
- finder: David Warren of Vul Labs

Reported to security team	2023-10-12
Update 2.4.58 released	2023-10-19
Affects	2.4.17 through 2.4.57

Fixed in Apache HTTP Server 2.4.56

important: HTTP request splitting with mod_rewrite and mod_proxy (CVE-2023-25690)

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 on

RewriteRule "^/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.

Acknowledgements: finder: Lars Krapf of Adobe

Reported to security team	2023-02-02
fixed by r1908095 in 2.4.x	2023-03-07
Update 2.4.56 released	2023-03-07
Affects	2.4.0 through 2.4.55

moderate: Apache HTTP Server: mod_proxy_uwsgi HTTP response splitting (CVE-2023-27522)

HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.

Special characters in the origin response header can truncate/split the response forwarded to the client.

Acknowledgements: finder: Dimas Fariski Setyawan Putra (nyxsorcerer)

Reported to security team	2023-01-29
fixed by r1908094 in 2.4.x	2023-03-07
Update 2.4.56 released	2023-03-07
Affects	2.4.30 through 2.4.55

Fixed in Apache HTTP Server 2.4.55

moderate: mod_dav out of bounds read, or write of zero byte (CVE-2006-20001)

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.

Described in first edition of "The Art of Software Security Assessment"	2006-10-31
Reported to security team	2022-08-10
Update 2.4.55 released	2023-01-17
Affects	2.4 through 2.4.54

moderate: Apache HTTP Server: mod_proxy_ajp Possible request smuggling (CVE-2022-36760)

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.

Acknowledgements: finder: ZeddYu_Lu from Qi'anxin Research Institute of Legendsec at Qi'anxin Group

Reported to security team	2022-07-12
Update 2.4.55 released	2023-01-17
Affects	2.4 through 2.4.54

moderate: Apache HTTP Server: mod_proxy prior to 2.4.55 allows a backend to trigger HTTP response splitting (CVE-2022-37436)

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.

Acknowledgements: finder: Dimas Fariski Setyawan Putra (@nyxsorcerer)

Reported to security team	2022-07-14
Update 2.4.55 released	2023-01-17
Affects	before 2.4.55

Fixed in Apache HTTP Server 2.4.54

moderate: mod_proxy_ajp: Possible request smuggling (CVE-2022-26377)

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.

Acknowledgements: Ricter Z @ 360 Noah Lab

Reported to security team	2022-03-02
Update 2.4.54 released	2022-06-08
Affects	<=2.4.53

low: read beyond bounds in mod_isapi (CVE-2022-28330)

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

Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue

Update 2.4.54 released	2022-06-08
Affects	<=2.4.53

low: read beyond bounds via ap_rwrite() (CVE-2022-28614)

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.

Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue

Update released in 2.4.54	2022-06-08
Affects	<=2.4.53

low: Read beyond bounds in ap_strcmp_match() (CVE-2022-28615)

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.

Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue

Update 2.4.54 released	2022-06-08
Affects	<=2.4.53

low: Denial of service in mod_lua r:parsebody (CVE-2022-29404)

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.

Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue

Update 2.4.54 released	2022-06-08
Affects	<=2.4.53

low: mod_sed denial of service (CVE-2022-30522)

If Apache HTTP Server 2.4.53 is configured to do transformations with mod_sed in contexts where the input to mod_sed may be very large, mod_sed may make excessively large memory allocations and trigger an abort.

Acknowledgements: This issue was found by Brian Moussalli from the JFrog Security Research team

Update 2.4.54 released	2022-06-08
Affects	2.4.53

low: Information Disclosure in mod_lua with websockets (CVE-2022-30556)

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.

Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue

Update 2.4.54 released	2022-06-08
Affects	<=2.4.53

low: mod_proxy X-Forwarded-For dropped by hop-by-hop mechanism (CVE-2022-31813)

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.

Acknowledgements: The Apache HTTP Server project would like to thank Gaetan Ferry (Synacktiv) for reporting this issue

Update 2.4.54 released	2022-06-08
Affects	<=2.4.53

Fixed in Apache HTTP Server 2.4.53

moderate: mod_lua Use of uninitialized value of in r:parsebody (CVE-2022-22719)

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.

Acknowledgements: Chamal De Silva

Reported to security team	2021-12-18
fixed by r1898694 in 2.4.x	2022-03-07
Update 2.4.53 released	2022-03-14
Affects	<=2.4.52

important: HTTP request smuggling vulnerability in Apache HTTP Server 2.4.52 and earlier (CVE-2022-22720)

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

Acknowledgements: James Kettle <james.kettle portswigger.net>

Reported to security team	2021-12-17
fixed by r1898692 in 2.4.x	2022-03-07
Update 2.4.53 released	2022-03-14
Affects	<=2.4.52

low: core: Possible buffer overflow with very large or unlimited LimitXMLRequestBody (CVE-2022-22721)

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.

Acknowledgements: Anonymous working with Trend Micro Zero Day Initiative

Reported to security team	2021-12-16
fixed by r1898693 in 2.4.x	2022-03-07
Update 2.4.53 released	2022-03-14
Affects	<=2.4.52

important: mod_sed: Read/write beyond bounds (CVE-2022-23943)

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.

Acknowledgements: Ronald Crane (Zippenhop LLC)

Reported to security team	2022-01-13
fixed by r1898695, r1898772 in 2.4.x	2022-03-09
Update 2.4.53 released	2022-03-14
Affects	<=2.4.52

Fixed in Apache HTTP Server 2.4.52

moderate: Possible NULL dereference or SSRF in forward proxy configurations in Apache HTTP Server 2.4.51 and earlier (CVE-2021-44224)

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).

Acknowledgements:

- 漂亮鼠
- TengMA(@Te3t123)

Reported to security team	2021-11-18
fixed by r1895955, r1896044 in 2.4.x	2021-12-14
Update 2.4.52 released	2021-12-20
Affects	>=2.4.7, <=2.4.51

important: Possible buffer overflow when parsing multipart content in mod_lua of Apache HTTP Server 2.4.51 and earlier (CVE-2021-44790)

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.

Acknowledgements: Chamal

Reported to security team	2021-12-07
Fixed by r1896039 in 2.4.x	2021-12-16
Update 2.4.52 released	2021-12-20
Affects	<=2.4.51

Fixed in Apache HTTP Server 2.4.51

critical: Path Traversal and Remote Code Execution in Apache HTTP Server 2.4.49 and 2.4.50 (incomplete fix of CVE-2021-41773) (CVE-2021-42013)

It was found that the fix for CVE-2021-41773 in Apache HTTP Server 2.4.50 was insufficient. An attacker could use a path traversal attack to map URLs to files outside the directories configured by Alias-like directives.

If files outside of these directories are not protected by the usual default configuration "require all denied", these requests can succeed. If CGI scripts are also enabled for these aliased pathes, this could allow for remote code execution.

This issue only affects Apache 2.4.49 and Apache 2.4.50 and not earlier versions.

Acknowledgements:

- Reported by Juan Escobar from Dreamlab Technologies
- Reported by Fernando Muñoz from NULL Life CTF Team
- Reported by Shungo Kumasaka
- Reported by Nattapon Jongcharoen

Reported to security team	2021-10-06
fixed by r1893977, r1893980, r1893982 in 2.4.x	2021-10-07
Update 2.4.51 released	2021-10-07
Affects	2.4.50, 2.4.49

Fixed in Apache HTTP Server 2.4.50

moderate: null pointer dereference in h2 fuzzing (CVE-2021-41524)

While fuzzing the 2.4.49 httpd, a new null pointer dereference was detected during HTTP/2 request processing,

allowing an external source to DoS the server. This requires a specially crafted request.

The vulnerability was recently introduced in version 2.4.49. No exploit is known to the project.

Acknowledgements: Apache httpd team would like to thank LI ZHI XIN from NSFocus Security Team for reporting this issue.

Reported to security team	2021-09-17
fixed by r1893655 in 2.4.x	2021-09-26
Update 2.4.50 released	2021-10-04
Affects	2.4.49

critical: Path traversal and file disclosure vulnerability in Apache HTTP Server 2.4.49 (CVE-2021-41773)

A flaw was found in a change made to path normalization in Apache HTTP Server 2.4.49. An attacker could use a path traversal attack to map URLs to files outside the directories configured by Alias-like directives.

If files outside of these directories are not protected by the usual default configuration "require all denied", these requests can succeed. If CGI scripts are also enabled for these aliased pathes, this could allow for remote code execution.

This issue is known to be exploited in the wild.

This issue only affects Apache 2.4.49 and not earlier versions.

Acknowledgements: This issue was reported by Ash Daulton along with the cPanel Security Team

Reported to security team	2021-09-29
fixed by r1893775 in 2.4.x	2021-10-01
Update 2.4.50 released	2021-10-04
Affects	2.4.49

Fixed in Apache HTTP Server 2.4.49

moderate: Request splitting via HTTP/2 method injection and mod_proxy (CVE-2021-33193)

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.

Acknowledgements: Reported by James Kettle of PortSwigger

Reported to security team	2021-05-11
Issue public	2021-08-06
Update 2.4.49 released	2021-09-16
Affects	<=2.4.48, !<2.4.17

moderate: NULL pointer dereference in httpd core (CVE-2021-34798)

Malformed requests may cause the server to dereference a NULL pointer.

This issue affects Apache HTTP Server 2.4.48 and earlier.

Acknowledgements: The issue was discovered by the Apache HTTP security team

Update 2.4.49 released	2021-09-16
Affects	<=2.4.48

moderate: mod_proxy_uwsgi out of bound read (CVE-2021-36160)

A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS).

This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48 (inclusive).

Acknowledgements: LI ZHI XIN from NSFocus Security Team

Reported to security team	2021-04-26
Update 2.4.49 release	2021-09-16
Affects	<=2.4.48, !<2.4.30

low: ap_escape_quotes buffer overflow (CVE-2021-39275)

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.

Acknowledgements: ClusterFuzz

Update 2.4.49 released	2021-09-16
Affects	<=2.4.48

important: mod_proxy SSRF (CVE-2021-40438)

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.

Acknowledgements: The issue was discovered by the Apache HTTP security team while analysing CVE-2021-36160

Update 2.4.49 released	2021-09-16
Affects	<=2.4.48

Fixed in Apache HTTP Server 2.4.48

moderate: mod_proxy_wstunnel tunneling of non Upgraded connections (CVE-2019-17567)

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.

Acknowledgements: Reported by Mikhail Egorov (<0ang3el gmail.com>)

Reported to security team	2019-10-05
Issue public	2021-06-01
Update 2.4.48 released	2021-06-01
Affects	2.4.46, 2.4.43, 2.4.41, 2.4.39, 2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6

moderate: Improper Handling of Insufficient Privileges (CVE-2020-13938)

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

Acknowledgements: Discovered by Ivan Zhakov

Reported to security team	2021-01-26
Issue public	2021-06-01
Update 2.4.48 released	2021-06-01
Affects	2.4.46, 2.4.43, 2.4.41, 2.4.39, 2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.4.0

low: mod_proxy_http NULL pointer dereference (CVE-2020-13950)

Apache HTTP Server versions 2.4.41 to 2.4.46 mod_proxy_http can be made to crash (NULL pointer dereference) with specially crafted requests using both Content-Length and Transfer-Encoding headers, leading to a Denial of Service

Acknowledgements: Reported by Marc Stern (<marc.stern@approach-cyber.com>)

Reported to security team	2020-09-11
Issue public	2021-06-01
Update 2.4.48 released	2021-06-01
Affects	2.4.46, 2.4.43, 2.4.41

low: mod_auth_digest possible stack overflow by one nul byte (CVE-2020-35452)

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

Acknowledgements: This issue was discovered and reported by GHSL team member @antonio-morales (Antonio Morales)

Reported to security team	2020-11-11
Issue public	2021-06-01
Update 2.4.48 released	2021-06-01
Affects	2.4.46, 2.4.43, 2.4.41, 2.4.39, 2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.4.0

low: mod_session NULL pointer dereference (CVE-2021-26690)

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

Acknowledgements: This issue was discovered and reported by GHSL team member @antonio-morales (Antonio Morales)

Reported to security team	2021-02-08
Issue public	2021-06-01
Update 2.4.48 released	2021-06-01
Affects	2.4.46, 2.4.43, 2.4.41, 2.4.39, 2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.4.0

low: mod_session response handling heap overflow (CVE-2021-26691)

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

Acknowledgements: Discovered internally Christophe Jaillet

Reported to security team	2021-03-01
Issue public	2021-06-01
Update 2.4.48 released	2021-06-01
Affects	2.4.46, 2.4.43, 2.4.41, 2.4.39, 2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.4.0

moderate: Unexpected URL matching with 'MergeSlashes OFF' (CVE-2021-30641)

Apache HTTP Server versions 2.4.39 to 2.4.46 Unexpected matching behavior with 'MergeSlashes OFF'

Acknowledgements: Discovered by Christoph Anton Mitterer

Reported to security team	2021-04-14
Issue public	2021-06-01

Update 2.4.48 released	2021-06-01
Affects	2.4.46, 2.4.43, 2.4.41, 2.4.39

important: NULL pointer dereference on specially crafted HTTP/2 request (CVE-2021-31618)

Apache HTTP Server protocol handler for the HTTP/2 protocol checks received request headers against the size limitations as configured for the server and used for the HTTP/1 protocol as well. On violation of these restrictions and HTTP response is sent to the client with a status code indicating why the request was rejected.

This rejection response was not fully initialised in the HTTP/2 protocol handler if the offending header was the very first one received or appeared in a a footer. This led to a NULL pointer dereference on initialised memory, crashing reliably the child process. Since such a triggering HTTP/2 request is easy to craft and submit, this can be exploited to DoS the server.

This issue affected mod_http2 1.15.17 and Apache HTTP Server version 2.4.47 only. Apache HTTP Server 2.4.47 was never released.

Acknowledgements: Apache HTTP server would like to thank LI ZHI XIN from NSFoucs for reporting this.

Reported to security team	2021-04-22
Issue public	2021-06-01
Update 2.4.48 released	2021-06-01
Affects	2.4.47

Fixed in Apache HTTP Server 2.4.44

important: Push Diary Crash on Specifically Crafted HTTP/2 Header (CVE-2020-9490)

In 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.

Acknowledgements: Felix Wilhelm of Google Project Zero

Reported to security team	2020-04-24
Issue public	2020-08-07
Update 2.4.44 released	2020-08-07
Affects	2.4.43, 2.4.39, 2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.30, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20

moderate: mod_proxy_uwsgi buffer overflow (CVE-2020-11984)

In Apache HTTP Server versions 2.4.32 to 2.4.43, mod_proxy_uwsgi has a information disclosure and possible RCE

Acknowledgements: Discovered by Felix Wilhelm of Google Project Zero

Reported to security team	2020-07-22
Issue public	2020-08-07
Update 2.4.44 released	2020-08-07
Affects	2.4.39, 2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33

moderate: Push Diary Crash on Specifically Crafted HTTP/2 Header (CVE-2020-11993)

In 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.

Acknowledgements: Felix Wilhelm of Google Project Zero

Reported to security team	2020-06-16
Issue public	2020-08-07
Update 2.4.44 released	2020-08-07
Affects	2.4.43, 2.4.39, 2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.30, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20

Fixed in Apache HTTP Server 2.4.42

low: mod_rewrite CWE-601 open redirect (CVE-2020-1927)

In Apache HTTP Server versions 2.4.0 to 2.4.41 some mod_rewrite configurations vulnerable to open redirect.

Acknowledgements: The issue was discovered by Fabrice Perez

Reported to security team	2019-12-05
Issue public	2020-04-01
Update 2.4.42 released	2020-04-01
Affects	2.4.41, 2.4.40, 2.4.39, 2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.30, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.4.0

low: mod_proxy_ftp use of uninitialized value (CVE-2020-1934)

in Apache HTTP Server versions 2.4.0 to 2.4.41, mod_proxy_ftp use of uninitialized value with malicious FTP backend.

Acknowledgements: The issue was discovered by Chamal De Silva

Reported to security team	2020-01-03
Issue public	2020-04-01
Update 2.4.42 released	2020-04-01
Affects	2.4.41, 2.4.40, 2.4.39, 2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.30, 2.4.29,

	2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.4.0

Fixed in Apache HTTP Server 2.4.41

moderate: mod_http2, DoS attack by exhausting h2 workers. (CVE-2019-9517)

A malicious client could perform a DoS attack by flooding a connection with requests and basically never reading responses on the TCP connection. Depending on h2 worker dimensioning, it was possible to block those with relatively few connections.

Acknowledgements: The issue was discovered by Jonathan Looney of Netflix.

Reported to security team	2019-04-10
Issue public	2019-08-14
Update 2.4.41 released	2019-08-14
Affects	2.4.39, 2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.32, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20

moderate: mod_http2, memory corruption on early pushes (CVE-2019-10081)

HTTP/2 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.

Acknowledgements: The issue was discovered by Craig Young of Tripwire VERT, <vuln-report@secur3.us>.

Reported to security team	2019-04-10
Issue public	2019-08-14
Update 2.4.41 released	2019-08-14
Affects	2.4.39, 2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.32, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20

moderate: mod_http2, read-after-free in h2 connection shutdown (CVE-2019-10082)

Using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.

Acknowledgements: The issue was discovered by Craig Young of Tripwire VERT, <vuln-report@secur3.us>.

Reported to security team	2019-04-12
Issue public	2019-08-14
Update 2.4.41 released	2019-08-14
Affects	2.4.39, 2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.32, 2.4.29, 2.4.28, 2.4.27,

	2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18

low: Limited cross-site scripting in mod_proxy error page (CVE-2019-10092)

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 malfomed 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. We have taken this opportunity to also remove request data from many other in-built error messages. Note however this issue did not affect them directly and their output was already escaped to prevent cross-site scripting attacks.

Acknowledgements: This issue was reported by Matei "Mal" Badanoiu

Reported to security team	2019-07-09
Issue public	2019-08-14
Update 2.4.41 released	2019-08-14
Affects	2.4.39, 2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.30, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.4.0

moderate: CVE-2019-10097 mod_remoteip: Stack buffer overflow and NULL pointer dereference (CVE-2019-10097)

When mod_remoteip was configured to use a trusted intermediary proxy server using the "PROXY" protocol, a specially crafted PROXY header could trigger a stack buffer overflow or NULL pointer deference. This vulnerability could only be triggered by a trusted proxy and not by untrusted HTTP clients.

Acknowledgements: The issue was discovered by Daniel McCarney <cpu@letsencrypt.org> Let's Encrypt / Internet Security Research Group (ISRG)

Reported to security team	2019-07-23
Issue public	2019-08-14
Update 2.4.41 released	2019-08-14
Affects	2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33

low: mod_rewrite potential open redirect (CVE-2019-10098)

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.

Acknowledgements: The issue was discovered by Yukitsugu Sasaki

Reported to security team	2019-03-26
Issue public	2019-08-14
Update 2.4.41 released	2019-08-14
Affects	2.4.39, 2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.30, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18,

	2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.4.0

Fixed in Apache HTTP Server 2.4.39

low: mod_http2, read-after-free on a string compare (CVE-2019-0196)

Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparision when determining the method of a request and thus process the request incorrectly.

Acknowledgements: The issue was discovered by Craig Young, <vuln-report@secur3.us>.

Reported to security team	2019-01-29
Issue public	2019-04-01
Update 2.4.39 released	2019-04-01
Affects	2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.30, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17

low: mod_http2, possible crash on late upgrade (CVE-2019-0197)

When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. A server that never enabled the h2 protocol or that only enabled it for https: and did not configure the "H2Upgrade on" is unaffected by this.

Acknowledgements: The issue was discovered by Stefan Eissing, greenbytes.de.

Reported to security team	2019-01-29
Issue public	2019-04-01
Update 2.4.39 released	2019-04-01
Affects	2.4.38, 2.4.37, 2.4.35, 2.4.34

important: Apache HTTP Server privilege escalation from modules' scripts (CVE-2019-0211)

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.

Acknowledgements: The issue was discovered by Charles Fol.

Reported to security team	2019-02-22
Issue public	2019-04-01
Update 2.4.39 released	2019-04-01
Affects	2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.30, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17

important: mod_ssl access control bypass (CVE-2019-0215)

In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in mod_ssl when using per-location client certificate verification with TLSv1.3 allowed a client supporting Post-Handshake Authentication to bypass configured access control restrictions.

Acknowledgements: The issue was discovered by Michael Kaufmann.

Reported to security team	2019-01-23
Issue public	2019-04-01
Update 2.4.39 released	2019-04-01
Affects	2.4.38, 2.4.37

important: mod_auth_digest access control bypass (CVE-2019-0217)

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.

Acknowledgements: The issue was discovered by Simon Kappel.

Reported to security team	2019-01-29
Issue public	2019-04-01
Update 2.4.39 released	2019-04-01
Affects	2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.30, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.4.0

low: Apache httpd URL normalization inconsistency (CVE-2019-0220)

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.

Acknowledgements: The issue was discovered by Bernhard Lorenz <bernhard.lorenz@alphastrike.io> of Alpha Strike Labs GmbH.

Reported to security team	2019-01-20
Issue public	2019-04-01
Update 2.4.39 released	2019-04-01
Affects	2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.30, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.4.0

Fixed in Apache HTTP Server 2.4.38

low: DoS for HTTP/2 connections via slow request bodies (CVE-2018-17189)

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 connections. A possible mitigation is to not enable the h2 protocol.

Acknowledgements: The issue was discovered by Gal Goldshtein of F5 Networks.

Reported to security team	2018-10-16
Issue public	2019-01-22
Update 2.4.38 released	2019-02-28
Affects	2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.30, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17

low: mod_session_cookie does not respect expiry time (CVE-2018-17199)

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.

Acknowledgements: The issue was discovered by Diego Angulo from ImExHS.

Reported to security team	2018-10-08
Issue public	2019-01-22
Update 2.4.38 released	2019-02-28
Affects	2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.30, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.4.0

important: mod_ssl 2.4.37 remote DoS when used with OpenSSL 1.1.1 (CVE-2019-0190)

A bug exists in the way mod_ssl handled client renegotiations. A remote attacker could send a carefully crafted request that would cause mod_ssl to enter a loop leading to a denial of service. This bug can be only triggered with Apache HTTP Server version 2.4.37 when using OpenSSL version 1.1.1 or later, due to an interaction in changes to handling of renegotiation attempts.

Acknowledgements: The issue was discovered through user bug reports.

Reported to security team	2019-01-01
Issue public	2019-01-22
Update 2.4.38 released	2019-02-28
Affects	2.4.37

Fixed in Apache HTTP Server 2.4.35

low: DoS for HTTP/2 connections by continuous SETTINGS (CVE-2018-11763)

By sending continous SETTINGS frames of maximum size an ongoing HTTP/2 connection could be kept busy and would never time out. This can be abused for a DoS on the server. This only affect a server that has enabled the h2 protocol.

Acknowledgements: The issue was discovered by Gal Goldshtein of F5 Networks.

Reported to security team	2018-07-18
Issue public	2018-09-25
Update 2.4.35 released	2018-09-29
Affects	2.4.34, 2.4.33, 2.4.30, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18

Fixed in Apache HTTP Server 2.4.34

low: DoS for HTTP/2 connections by crafted requests (CVE-2018-1333)

By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. This issue only affects servers that have configured and enabled HTTP/2 support, which is not the default

Acknowledgements: The issue was discovered by Craig Young of Tripwire VERT.

Reported to security team	2018-05-08
Issue public	2018-07-18
Update 2.4.34 released	2018-07-15
Affects	2.4.33, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18

moderate: mod_md, DoS via Coredumps on specially crafted requests (CVE-2018-8011)

By specially crafting HTTP requests, the mod_md challenge handler would dereference a NULL pointer and cause the child process to segfault. This could be used to DoS the server.

Acknowledgements: The issue was discovered by Daniel Caminada <daniel.caminada@ergon.ch>.

Reported to security team	2018-06-29
Issue public	2018-07-18
Update 2.4.34 released	2018-07-15
Affects	2.4.33

Fixed in Apache HTTP Server 2.4.33

low: Out of bound write in mod_authnz_ldap when using too small Accept-Language values (CVE-2017-15710)

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.

Acknowledgements: The Apache HTTP Server security team would like to thank Alex Nichols and Jakob Hirsch for reporting this issue.

Reported to security team	2017-12-07
Issue public	2018-03-21
Update 2.4.33 released	2018-03-21
Affects	2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1

low: <FilesMatch> bypass with a trailing newline in the file name (CVE-2017-15715)

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.

Acknowledgements: The issue was discovered by Elar Lang - security.elarlang.eu

Reported to security team	2017-11-24
Issue public	2018-03-21
Update 2.4.33 released	2018-03-21
Affects	2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1

moderate: Tampering of mod_session data for CGI applications (CVE-2018-1283)

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. The severity is set to Moderate because "SessionEnv on" is not a default nor common configuration, it should be considered more severe when this is the case though, because of the possible remote exploitation.

Acknowledgements: The issue was discovered internally by the Apache HTTP Server team.

Reported to security team	2017-11-14
Issue public	2018-03-21
Update 2.4.33 released	2018-03-21

Affects	2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1

low: Possible out of bound access after failure in reading the HTTP request (CVE-2018-1301)

A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.33, 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.

Acknowledgements: The issue was discovered by Robert Swiecki, bug found by honggfuzz.

Reported to security team	2018-01-23
Issue public	2018-03-21
Update 2.4.33 released	2018-03-21
Affects	2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1

low: Possible write of after free on HTTP/2 stream shutdown (CVE-2018-1302)

When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.33 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerabilty 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.

Acknowledgements: The issue was discovered by Robert Swiecki, bug found by honggfuzz.

Reported to security team	2018-01-23
Issue public	2018-03-21
Update 2.4.33 released	2018-03-21
Affects	2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17

low: Possible out of bound read in mod_cache_socache (CVE-2018-1303)

A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.33 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.

Acknowledgements: The issue was discovered by Robert Swiecki, bug found by honggfuzz.

Reported to security team	2018-01-23

Issue public	2018-03-21
Update 2.4.33 released	2018-03-21
Affects	2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6

low: Weak Digest auth nonce generation in mod_auth_digest (CVE-2018-1312)

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.

Acknowledgements: The issue was discovered by Nicolas Daniels.

Reported to security team	2013-03-05
Issue public	2018-03-21
Update 2.4.33 released	2018-03-21
Affects	2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1

Fixed in Apache HTTP Server 2.4.28

low: Use-after-free when using <Limit > with an unrecognized method in .htaccess ("OptionsBleed") (CVE-2017-9798)

When an unrecognized HTTP Method is given in an <Limit {method}> directive in an .htaccess file, and that .htaccess file is processed by the corresponding request, the global methods table is corrupted in the current worker process, resulting in erratic behaviour. This behavior may be avoided by listing all unusual HTTP Methods in a global httpd.conf RegisterHttpMethod directive in httpd release 2.4.25 and later. To permit other .htaccess directives while denying the <Limit > directive, see the AllowOverrideList directive. Source code patch (2.4) is at; CVE-2017-9798-patch-2.4.patch Source code patch (2.2) is at; CVE-2017-9798-patch-2.2.patch Note 2.2 is end-of-life, no further release with this fix is planned. Users are encouraged to migrate to 2.4.28 or later for this and other fixes.

Acknowledgements: We would like to thank Hanno Böck for reporting this issue.

Reported to security team	2017-07-12
Issue public	2017-09-18
Update 2.4.28 released	2017-10-05
Update 2.2.35-never released	--
Affects	2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.2.34, 2.2.32, 2.2.31, 2.2.29, 2.2.27, 2.2.26, 2.2.25, 2.2.24, 2.2.23, 2.2.22, 2.2.21, 2.2.20, 2.2.19, 2.2.18, 2.2.17, 2.2.16, 2.2.15, 2.2.14, 2.2.13,

	2.2.12, 2.2.11, 2.2.10, 2.2.9, 2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0

Fixed in Apache HTTP Server 2.4.27

important: Uninitialized memory reflection in mod_auth_digest (CVE-2017-9788)

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.

Acknowledgements: We would like to thank Robert Święcki for reporting this issue.

Reported to security team	2017-06-28
Issue public	2017-07-11
Update 2.4.27 released	2017-07-11
Update 2.2.34 released	2017-07-11
Affects	2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.2.32, 2.2.31, 2.2.29, 2.2.27, 2.2.26, 2.2.25, 2.2.24, 2.2.23, 2.2.22, 2.2.21, 2.2.20, 2.2.19, 2.2.18, 2.2.17, 2.2.16, 2.2.15, 2.2.14, 2.2.13, 2.2.12, 2.2.11, 2.2.10, 2.2.9, 2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0

important: Read after free in mod_http2 (CVE-2017-9789)

When under stress, closing many connections, the HTTP/2 handling code would sometimes access memory after it has been freed, resulting in potentially erratic behaviour.

Acknowledgements: We would like to thank Robert Święcki for reporting this issue.

Reported to security team	2017-06-30
Issue public	2017-07-11
Update 2.4.27 released	2017-07-11
Affects	2.4.26

Fixed in Apache HTTP Server 2.4.26

important: ap_get_basic_auth_pw() Authentication Bypass (CVE-2017-3167)

Use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed. Third-party module writers SHOULD use ap_get_basic_auth_components(), available in 2.2.34 and 2.4.26, instead of ap_get_basic_auth_pw(). Modules which call the legacy ap_get_basic_auth_pw() during the authentication phase MUST either immediately authenticate the user after the call, or else stop the

request immediately with an error response, to avoid incorrectly authenticating the current request.

Acknowledgements: We would like to thank Emmanuel Dreyfus for reporting this issue.

Reported to security team	2017-02-06
Issue public	2017-06-19
Update 2.4.26 released	2017-06-19
Update 2.2.34 released	2017-07-11
Affects	2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.2.32, 2.2.31, 2.2.29, 2.2.27, 2.2.26, 2.2.25, 2.2.24, 2.2.23, 2.2.22, 2.2.21, 2.2.20, 2.2.19, 2.2.18, 2.2.17, 2.2.16, 2.2.15, 2.2.14, 2.2.13, 2.2.12, 2.2.11, 2.2.10, 2.2.9, 2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0

important: mod_ssl Null Pointer Dereference (CVE-2017-3169)

mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.

Acknowledgements: We would like to thank Vasileios Panopoulos and AdNovum Informatik AG for reporting this issue.

Reported to security team	2016-12-05
Issue public	2017-06-19
Update 2.4.26 released	2017-06-19
Update 2.2.34 released	2017-07-11
Affects	2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.2.32, 2.2.31, 2.2.29, 2.2.27, 2.2.26, 2.2.25, 2.2.24, 2.2.23, 2.2.22, 2.2.21, 2.2.20, 2.2.19, 2.2.18, 2.2.17, 2.2.16, 2.2.15, 2.2.14, 2.2.13, 2.2.12, 2.2.11, 2.2.10, 2.2.9, 2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0

important: mod_http2 Null Pointer Dereference (CVE-2017-7659)

A maliciously constructed HTTP/2 request could cause mod_http2 to dereference a NULL pointer and crash the server process.

Acknowledgements: We would like to thank Robert Święcki for reporting this issue.

Reported to security team	2016-11-18
Issue public	2017-06-19
Update 2.4.26 released	2017-06-19
Affects	2.4.25

important: ap_find_token() Buffer Overread (CVE-2017-7668)

The HTTP strict parsing changes added in 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.

Acknowledgements: We would like to thank Javier Jiménez (javijmor@gmail.com) for reporting this issue.

Reported to security team	2017-05-06
Issue public	2017-06-19
Update 2.4.26 released	2017-06-19
Update 2.2.34 released	2017-07-11
Affects	2.4.25, 2.2.32

important: mod_mime Buffer Overread (CVE-2017-7679)

mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

Acknowledgements: We would like to thank ChenQin and Hanno Böck for reporting this issue.

Reported to security team	2015-11-15
Issue public	2017-06-19
Update 2.4.26 released	2017-06-19
Update 2.2.34 released	2017-07-11
Affects	2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.2.32, 2.2.31, 2.2.29, 2.2.27, 2.2.26, 2.2.25, 2.2.24, 2.2.23, 2.2.22, 2.2.21, 2.2.20, 2.2.19, 2.2.18, 2.2.17, 2.2.16, 2.2.15, 2.2.14, 2.2.13, 2.2.12, 2.2.11, 2.2.10, 2.2.9, 2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0

Fixed in Apache HTTP Server 2.4.25

low: Padding Oracle in Apache mod_session_crypto (CVE-2016-0736)

Prior to Apache HTTP release 2.4.25, mod_sessioncrypto was encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This made it vulnerable to padding oracle attacks, particularly with CBC. An authentication tag (SipHash MAC) is now added to prevent such attacks.

Acknowledgements: We would like to thank individuals at the RedTeam Pentesting GmbH for reporting this issue.

Reported to security team	2016-01-20
Issue public	2016-12-20
Update 2.4.25 released	2016-12-20
Affects	2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4,

	2.4.3, 2.4.2, 2.4.1

low: DoS vulnerability in mod_auth_digest (CVE-2016-2161)

Malicious input to mod_auth_digest will cause the server to crash, and each instance continues to crash even for subsequently valid requests.

Acknowledgements: We would like to thank Maksim Malyutin for reporting this issue.

Reported to security team	2016-07-11
Issue public	2016-12-20
Update 2.4.25 released	2016-12-20
Affects	2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1

moderate: mod_userdir CRLF injection (CVE-2016-4975)

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.

Acknowledgements: The issue was discovered by Sergey Bobrov

Reported to security team	2016-07-24
Issue public	2018-08-14
Update 2.4.25 released	2016-12-20
Update 2.2.32 released	2017-01-13
Affects	2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.2.31, 2.2.29, 2.2.27, 2.2.26, 2.2.25, 2.2.24, 2.2.23, 2.2.22, 2.2.21, 2.2.20, 2.2.19, 2.2.18, 2.2.17, 2.2.16, 2.2.15, 2.2.14, 2.2.13, 2.2.12, 2.2.11, 2.2.10, 2.2.9, 2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0

n/a: HTTP_PROXY environment variable "httpoxy" mitigation (CVE-2016-5387)

HTTP_PROXY is a well-defined environment variable in a CGI process, which collided with a number of libraries which failed to avoid colliding with this CGI namespace. A mitigation is provided for the httpd CGI environment to avoid populating the "HTTP_PROXY" variable from a "Proxy:" header, which has never been registered by IANA. This workaround and patch are documented in the ASF Advisory at asf-httpoxy-response.txt and incorporated in the 2.4.25 and 2.2.32 releases. Note: This is not assigned an httpd severity, as it is a defect in other software which overloaded well-established CGI environment variables, and does not reflect an error in HTTP server software.

Acknowledgements: We would like to thank Dominic Scheirlinck and Scott Geary of Vend for reporting and proposing a fix for this issue.

Reported to security team	2016-07-02
Issue public	2016-07-18
Update 2.4.25 released	2016-12-20
Update 2.2.32 released	2016-07-18
Affects	2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.2.31, 2.2.29, 2.2.27, 2.2.26, 2.2.25, 2.2.24, 2.2.23, 2.2.22, 2.2.21, 2.2.20, 2.2.19, 2.2.18, 2.2.17, 2.2.16, 2.2.15, 2.2.14, 2.2.13, 2.2.12, 2.2.11, 2.2.10, 2.2.9, 2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0

low: HTTP/2 CONTINUATION denial of service (CVE-2016-8740)

The HTTP/2 protocol implementation (mod_http2) had an incomplete handling of the LimitRequestFields directive. This allowed an attacker to inject unlimited request headers into the server, leading to eventual memory exhaustion.

Acknowledgements: We would like to thank Naveen Tiwari and CDF/SEFCOM at Arizona State University to reporting this issue.

Reported to security team	2016-11-22
Issue public	2016-12-04
Update 2.4.25 released	2016-12-20
Affects	2.4.23, 2.4.20, 2.4.18, 2.4.17

important: Apache HTTP Request Parsing Whitespace Defects (CVE-2016-8743)

Apache HTTP Server, prior to release 2.4.25 (and 2.2.32), accepted a broad pattern of unusual whitespace patterns from the user-agent, including bare CR, FF, VTAB in parsing the request line and request header lines, as well as HTAB in parsing the request line. Any bare CR present in request lines was treated as whitespace and remained in the request field member "the_request", while a bare CR in the request header field name would be honored as whitespace, and a bare CR in the request header field value was retained the input headers array. Implied additional whitespace was accepted in the request line and prior to the ':' delimiter of any request header lines.

RFC7230 Section 3.5 calls out some of these whitespace exceptions, and section 3.2.3 eliminated and clarified the role of implied whitespace in the grammer of this specification. Section 3.1.1 requires exactly one single SP between the method and request-target, and between the request-target and HTTP-version, followed immediately by a CRLF sequence. None of these fields permit any (unencoded) CTL character whatsoever. Section 3.2.4 explicitly disallowed any whitespace from the request header field prior to the ':' character, while Section 3.2 disallows all CTL characters in the request header line other than the HTAB character as whitespace.

These defects represent a security concern when httpd is participating in any chain of proxies or interacting with back-end application servers, either through mod_proxy or using conventional CGI mechanisms. In each case where one agent accepts such CTL characters and does not treat them as whitespace, there is the

possiblity in a proxy chain of generating two responses from a server behind the uncautious proxy agent. In a sequence of two requests, this results in request A to the first proxy being interpreted as requests A + A' by the backend server, and if requests A and B were submitted to the first proxy in a keepalive connection, the proxy may interpret response A' as the response to request B, polluting the cache or potentially serving the A' content to a different downstream user-agent.

These defects are addressed with the release of Apache HTTP Server 2.4.25 and coordinated by a new directive; HttpProtocolOptions Strict which is the default behavior of 2.4.25 and later.

By toggling from 'Strict' behavior to 'Unsafe' behavior, some of the restrictions may be relaxed to allow some invalid HTTP/1.1 clients to communicate with the server, but this will reintroduce the possibility of the problems described in this assessment. Note that relaxing the behavior to 'Unsafe' will still not permit raw CTLs other than HTAB (where permitted), but will allow other RFC requirements to not be enforced, such as exactly two SP characters in the request line.

Acknowledgements: We would like to thank David Dennerline at IBM Security's X-Force Researchers as well as Régis Leroy for each reporting this issue.

Reported to security team	2016-02-10
Issue public	2016-12-20
Update 2.4.25 released	2016-12-20
Update 2.2.32 released	2017-01-13
Affects	2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.2.31, 2.2.29, 2.2.27, 2.2.26, 2.2.25, 2.2.24, 2.2.23, 2.2.22, 2.2.21, 2.2.20, 2.2.19, 2.2.18, 2.2.17, 2.2.16, 2.2.15, 2.2.14, 2.2.13, 2.2.12, 2.2.11, 2.2.10, 2.2.9, 2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0

low: IP address spoofing when proxying using mod_remoteip and mod_rewrite (CVE-2020-11985)

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.

Acknowledgements:

Reported to security team	2016-10-13
Issue public	2020-08-07
Update 2.4.25 released	2020-08-07
Affects	2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1

Fixed in Apache HTTP Server 2.4.23

important: TLS/SSL X.509 client certificate auth bypass with HTTP/2 (CVE-2016-4979)

For configurations enabling support for HTTP/2, SSL client certificate validation was not enforced if configured, allowing clients unauthorized access to protected resources over HTTP/2. This issue affected releases 2.4.18 and 2.4.20 only.

Acknowledgements: This issue was reported by Erki Aring.

Reported to security team	2016-06-30
Issue public	2016-07-05
Update 2.4.23 released	2016-07-05
Affects	2.4.20, 2.4.18

Fixed in Apache HTTP Server 2.4.20

low: mod_http2: denial of service by thread starvation (CVE-2016-1546)

By manipulating the flow control windows on streams, a client was able to block server threads for long times, causing starvation of worker threads. Connections could still be opened, but no streams where processed for these. This issue affected HTTP/2 support in 2.4.17 and 2.4.18.

Acknowledgements: This issue was reported by Noam Mazor.

Reported to security team	2016-02-02
Issue public	2016-04-11
Update 2.4.20 released	2016-04-11
Affects	2.4.18, 2.4.17

Fixed in Apache HTTP Server 2.4.16

low: mod_lua: Crash in websockets PING handling (CVE-2015-0228)

A stack recursion crash in the mod_lua module was found. A Lua script executing the r:wsupgrade() function could crash the process if a malicious client sent a carefully crafted PING request. This issue affected releases 2.4.7 through 2.4.12 inclusive.

Acknowledgements: This issue was reported by Guido Vranken.

Reported to security team	2015-01-28
Issue public	2015-02-04
Update 2.4.16 released	2015-07-15
Affects	2.4.12, 2.4.10, 2.4.9, 2.4.7

low: Crash in ErrorDocument 400 handling (CVE-2015-0253)

A crash in ErrorDocument handling was found. If ErrorDocument 400 was configured pointing to a local URL-path with the INCLUDES filter active, a NULL dereference would occur when handling the error, causing the child process to crash. This issue affected the 2.4.12 release only.

Reported to security team	2015-02-03
Issue public	2015-03-05
Update 2.4.16 released	2015-07-15

Affects	2.4.12

low: HTTP request smuggling attack against chunked request parser (CVE-2015-3183)

An HTTP request smuggling attack was possible due to a bug in parsing of chunked requests. A malicious client could force the server to misinterpret the request length, allowing cache poisoning or credential hijacking if an intermediary proxy is in use.

Acknowledgements: This issue was reported by Régis Leroy.

Reported to security team	2015-04-04
Issue public	2015-06-09
Update 2.4.16 released	2015-07-15
Update 2.2.31 released	2015-07-16
Affects	2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.2.29, 2.2.27, 2.2.26, 2.2.25, 2.2.24, 2.2.23, 2.2.22, 2.2.21, 2.2.20, 2.2.19, 2.2.18, 2.2.17, 2.2.16, 2.2.15, 2.2.14, 2.2.13, 2.2.12, 2.2.11, 2.2.10, 2.2.9, 2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0

low: ap_some_auth_required API unusable (CVE-2015-3185)

A design error in the "ap_some_auth_required" function renders the API unusuable in httpd 2.4.x. In particular the API is documented to answering if the request required authentication but only answers if there are Require lines in the applicable configuration. Since 2.4.x Require lines are used for authorization as well and can appear in configurations even when no authentication is required and the request is entirely unrestricted. This could lead to modules using this API to allow access when they should otherwise not do so. API users should use the new ap_some_authn_required API added in 2.4.16 instead.

Acknowledgements: This issue was reported by Ben Reser.

Reported to security team	2013-08-05
Issue public	2015-06-09
Update 2.4.16 released	2015-07-15
Affects	2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.5, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.4.0

Fixed in Apache HTTP Server 2.4.12

low: HTTP Trailers processing bypass (CVE-2013-5704)

HTTP trailers could be used to replace HTTP headers late during request processing, potentially undoing or otherwise confusing modules that examined or modified request headers earlier. This fix adds the "MergeTrailers" directive to restore legacy behavior.

Acknowledgements: This issue was reported by Martin Holst Swende.

Reported to security team	2013-09-06

Issue public	2013-10-19
Update 2.4.12 released	2015-01-30
Update 2.2.29 released	2014-09-03
Affects	2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.2.27, 2.2.26, 2.2.25, 2.2.24, 2.2.23, 2.2.22, 2.2.21, 2.2.20, 2.2.19, 2.2.18, 2.2.17, 2.2.16, 2.2.15, 2.2.14, 2.2.13, 2.2.12, 2.2.11, 2.2.10, 2.2.9, 2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0

low: mod_cache crash with empty Content-Type header (CVE-2014-3581)

A NULL pointer deference was found in mod_cache. A malicious HTTP server could cause a crash in a caching forward proxy configuration. This crash would only be a denial of service if using a threaded MPM.

Reported to security team	2014-09-08
Issue public	2014-09-08
Update 2.4.12 released	2015-01-30
Affects	2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1

low: mod_proxy_fcgi out-of-bounds memory read (CVE-2014-3583)

An out-of-bounds memory read was found in mod_proxy_fcgi. A malicious FastCGI server could send a carefully crafted response which could lead to a crash when reading past the end of a heap memory or stack buffer. This issue affects version 2.4.10 only.

Acknowledgements: This issue was reported by Teguh P. Alko.

Reported to security team	2014-09-17
Issue public	2014-11-12
Update 2.4.12 released	2015-01-30
Affects	2.4.10

low: mod_lua multiple "Require" directive handling is broken (CVE-2014-8109)

Fix handling of the Require line in mod_lau when a LuaAuthzProvider is used in multiple Require directives with different arguments. This could lead to different authentication rules than expected.

Reported to security team	2014-11-09
Issue public	2014-11-09
Update 2.4.12 released	2015-01-30
Affects	2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1

Fixed in Apache HTTP Server 2.4.10

moderate: mod_proxy denial of service (CVE-2014-0117)

A flaw was found in mod_proxy in httpd versions 2.4.6 to 2.4.9. A remote attacker could send a carefully crafted request to a server

configured as a reverse proxy, and cause the child process to crash. This could lead to a denial of service against a threaded MPM.

Acknowledgements: This issue was reported by Marek Kroemeke, AKAT-1 and 22733db72ab3ed94b5f8a1ffcde850251fe6f466 via HP ZDI

Reported to security team	2014-04-07
Issue public	2014-07-15
Update 2.4.10 released	2014-07-15
Affects	2.4.9, 2.4.7, 2.4.6

moderate: mod_deflate denial of service (CVE-2014-0118)

A resource consumption flaw was found in mod_deflate. If request body decompression was configured (using the "DEFLATE" input filter), a remote attacker could cause the server to consume significant memory and/or CPU resources. The use of request body decompression is not a common configuration.

Acknowledgements: This issue was reported by Giancarlo Pellegrino and Davide Balzarotti

Reported to security team	2014-02-19
Issue public	2014-07-14
Update 2.4.10 released	2014-07-15
Update 2.2.29 released	2014-09-03
Affects	2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.2.27, 2.2.26, 2.2.25, 2.2.24, 2.2.23, 2.2.22, 2.2.21, 2.2.20, 2.2.19, 2.2.18, 2.2.17, 2.2.16, 2.2.15, 2.2.14, 2.2.13, 2.2.12, 2.2.11, 2.2.10, 2.2.9, 2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0

moderate: mod_status buffer overflow (CVE-2014-0226)

A race condition was found in mod_status. An attacker able to access a public server status page on a server using a threaded MPM could send a carefully crafted request which could lead to a heap buffer overflow. Note that it is not a default or recommended configuration to have a public accessible server status page.

Acknowledgements: This issue was reported by Marek Kroemeke, AKAT-1 and 22733db72ab3ed94b5f8a1ffcde850251fe6f466 via HP ZDI

Reported to security team	2014-05-30
Issue public	2014-07-14
Update 2.4.10 released	2014-07-15
Update 2.2.29 released	2014-09-03
Affects	2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.2.27, 2.2.26, 2.2.25, 2.2.24, 2.2.23, 2.2.22, 2.2.21, 2.2.20, 2.2.19, 2.2.18, 2.2.17, 2.2.16, 2.2.15, 2.2.14, 2.2.13, 2.2.12, 2.2.11, 2.2.10, 2.2.9, 2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0

important: mod_cgid denial of service (CVE-2014-0231)

A flaw was found in mod_cgid. If a server using mod_cgid hosted CGI scripts which did not consume standard input, a remote attacker could cause child processes to hang indefinitely, leading to denial of service.

Acknowledgements: This issue was reported by Rainer Jung of the ASF

Reported to security team	2014-06-16
Issue public	2014-07-14
Update 2.4.10 released	2014-07-15
Update 2.2.29 released	2014-09-03
Affects	2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.2.27, 2.2.26, 2.2.25, 2.2.24, 2.2.23, 2.2.22, 2.2.21, 2.2.20, 2.2.19, 2.2.18, 2.2.17, 2.2.16, 2.2.15, 2.2.14, 2.2.13, 2.2.12, 2.2.11, 2.2.10, 2.2.9, 2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0

important: WinNT MPM denial of service (CVE-2014-3523)

A flaw was found in the WinNT MPM in httpd versions 2.4.1 to 2.4.9, when using the default AcceptFilter for that platform. A remote attacker could send carefully crafted requests that would leak memory and eventually lead to a denial of service against the server.

Acknowledgements: This issue was reported by Jeff Trawick of the ASF

Reported to security team	2014-07-01
Issue public	2014-07-15
Update 2.4.10 released	2014-07-15
Affects	2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1

Fixed in Apache HTTP Server 2.4.9

moderate: mod_dav crash (CVE-2013-6438)

XML parsing code in mod_dav incorrectly calculates the end of the string when removing leading spaces and places a NUL character outside the buffer, causing random crashes. This XML parsing code is only used with DAV provider modules that support DeltaV, of which the only publicly released provider is mod_dav_svn.

Acknowledgements: This issue was reported by Ning Zhang & Amin Tora of Neustar

Reported to security team	2013-12-10
Issue public	2014-03-17
Update 2.4.9 released	2014-03-17
Update 2.2.27 released	2014-03-26
Affects	2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.2.26, 2.2.25, 2.2.24, 2.2.23, 2.2.22, 2.2.21, 2.2.20, 2.2.19, 2.2.18, 2.2.17, 2.2.16, 2.2.15, 2.2.14, 2.2.13, 2.2.12,

	2.2.11, 2.2.10, 2.2.9, 2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0

low: mod_log_config crash (CVE-2014-0098)

A flaw was found in mod_log_config. A remote attacker could send a specific truncated cookie causing a crash. This crash would only be a denial of service if using a threaded MPM.

Acknowledgements: This issue was reported by Rainer M Canavan

Reported to security team	2014-02-25
Issue public	2014-03-17
Update 2.4.9 released	2014-03-17
Update 2.2.27 released	2014-03-26
Affects	2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.2.26, 2.2.25, 2.2.24, 2.2.23, 2.2.22, 2.2.21, 2.2.20, 2.2.19, 2.2.18, 2.2.17, 2.2.16, 2.2.15, 2.2.14, 2.2.13, 2.2.12, 2.2.11, 2.2.10, 2.2.9, 2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0

Fixed in Apache HTTP Server 2.4.7

low: mod_cache crash (CVE-2013-4352)

A NULL pointer dereference was found in mod_cache. A malicious HTTP server could cause a crash in a caching forward proxy configuration. (Note that this vulnerability was fixed in the 2.4.7 release, but the security impact was not disclosed at the time of the release.)

Reported to security team	2013-09-14
Issue public	2014-07-14
Update 2.4.7 released	2013-11-26
Affects	2.4.6

Fixed in Apache HTTP Server 2.4.6

moderate: mod_dav crash (CVE-2013-1896)

Sending a MERGE request against a URI handled by mod_dav_svn with the source href (sent as part of the request body as XML) pointing to a URI that is not configured for DAV will trigger a segfault.

Acknowledgements: This issue was reported by Ben Reser

Reported to security team	2013-03-07
Issue public	2013-05-23
Update 2.4.6 released	2013-07-22
Update 2.2.25 released	2013-07-22
Affects	2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.2.23, 2.2.22, 2.2.21, 2.2.20, 2.2.19, 2.2.18, 2.2.17, 2.2.16, 2.2.15, 2.2.14, 2.2.13, 2.2.12, 2.2.11, 2.2.10, 2.2.9, 2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0

moderate: mod_session_dbd session fixation flaw (CVE-2013-2249)

A flaw in mod_session_dbd caused it to proceed with save operations for a session without considering the dirty flag and the requirement for a new session ID.

Acknowledgements: This issue was reported by Takashi Sato

Reported to security team	2013-05-29
Issue public	2013-07-22
Update 2.4.6 released	2013-07-22
Affects	2.4.4, 2.4.3, 2.4.2, 2.4.1

Fixed in Apache HTTP Server 2.4.4

low: XSS due to unescaped hostnames (CVE-2012-3499)

Various XSS flaws due to unescaped hostnames and URIs HTML output in mod_info, mod_status, mod_imagemap, mod_ldap, and mod_proxy_ftp.

Acknowledgements: This issue was reported by Niels Heinen of Google

Reported to security team	2012-07-11
Issue public	2013-02-18
Update 2.4.4 released	2013-02-25
Update 2.2.24 released	2013-02-25
Affects	2.4.3, 2.4.2, 2.4.1, 2.2.23, 2.2.22, 2.2.21, 2.2.20, 2.2.19, 2.2.18, 2.2.17, 2.2.16, 2.2.15, 2.2.14, 2.2.13, 2.2.12, 2.2.11, 2.2.10, 2.2.9, 2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0

moderate: XSS in mod_proxy_balancer (CVE-2012-4558)

A XSS flaw affected the mod_proxy_balancer manager interface.

Acknowledgements: This issue was reported by Niels Heinen of Google

Reported to security team	2012-10-07
Issue public	2013-02-18
Update 2.4.4 released	2013-02-25
Update 2.2.24 released	2013-02-25
Affects	2.4.3, 2.4.2, 2.4.1, 2.2.23, 2.2.22, 2.2.21, 2.2.20, 2.2.19, 2.2.18, 2.2.17, 2.2.16, 2.2.15, 2.2.14, 2.2.13, 2.2.12, 2.2.11, 2.2.10, 2.2.9, 2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0

Fixed in Apache HTTP Server 2.4.3

low: XSS in mod_negotiation when untrusted uploads are supported (CVE-2012-2687)

Possible XSS for sites which use mod_negotiation and allow untrusted uploads to locations which have MultiViews enabled. Note: This issue is also known as CVE-2008-0455.

Reported to security team	2012-05-31
Issue public	2012-06-13
Update 2.2.23 released	2012-09-13
Update 2.4.3 released	2012-08-21
Affects	2.4.2, 2.4.1, 2.2.22, 2.2.21, 2.2.20, 2.2.19, 2.2.18, 2.2.17, 2.2.16, 2.2.15, 2.2.14, 2.2.13, 2.2.12, 2.2.11, 2.2.10, 2.2.9, 2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0

important: Response mixup when using mod_proxy_ajp or mod_proxy_http (CVE-2012-3502)

The modules mod_proxy_ajp and mod_proxy_http did not always close the connection to the back end server when necessary as part of error handling. This could lead to an information disclosure due to a response mixup between users.

Reported to security team	2012-08-16
Issue public	2012-08-16
Update 2.4.3 released	2012-08-21
Affects	2.4.2, 2.4.1

Fixed in Apache HTTP Server 2.4.2

low: insecure LD_LIBRARY_PATH handling (CVE-2012-0883)

Insecure handling of LD_LIBRARY_PATH was found that could lead to the current working directory to be searched for DSOs. This could allow a local user to execute code as root if an administrator runs apachectl from an untrusted directory.

Reported to security team	2012-02-14
Issue public	2012-03-02
Update 2.4.2 released	2012-04-17
Update 2.2.23 released	2012-09-13
Affects	2.4.1, 2.2.22, 2.2.21, 2.2.20, 2.2.19, 2.2.18, 2.2.17, 2.2.16, 2.2.15, 2.2.14, 2.2.13, 2.2.12, 2.2.11, 2.2.10, 2.2.9, 2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0