



NCSC-2026-0134

Kwetsbaarheden verholpen in Apache HTTP Server

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 06-05-2026

TLP:WHITE

Toegestane verspreiding van TLP:WHITE

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Apache Software Foundation heeft meerdere kwetsbaarheden verholpen in Apache HTTP Server.

Duiding

De kwetsbaarheden betreffen verschillende modules en functionaliteiten binnen Apache HTTP Server. De meest ernstige kwetsbaarheid betreft een double free in de HTTP/2-implementatie, die het voor een aanvaller mogelijk maakt om willekeurige code uit te voeren voorafgaand aan authenticatie.

Lokale .htaccess auteurs kunnen via een privilege-escalatie toegang krijgen tot bestanden met httpd-gebruikersrechten. Het mod_proxy_ajp module bevat een heap-based buffer overflow en een out-of-bounds read, waardoor geheugenbeschadiging kan optreden. In de mod_md module is een resource allocatieprobleem aanwezig dat de serverprestaties kan beïnvloeden. De mod_dav_lock module bevat een NULL pointer dereference die kan leiden tot servercrashes en daarmee denial of service. De mod_auth_digest module kent een timing attack die Digest authenticatie kan omzeilen. De mod_authn_socache module heeft een NULL pointer dereference die crashes veroorzaakt bij caching forward proxy configuraties. Verder is er een HTTP response splitting kwetsbaarheid die manipulatie van HTTP headers mogelijk maakt. Daarnaast is er een improper null termination en out-of-bounds read in de core server functionaliteit, en een buffer over-read die kan leiden tot informatielekken of instabiliteit.

Oplossingen

Apache Software Foundation heeft versie 2.4.67 uitgebracht waarin alle genoemde kwetsbaarheden zijn verholpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ https://httpd.apache.org/security/vulnerabilities_24.html

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-23918	6.9 MEDIUM
➤ CVE-2026-24072	4.8 MEDIUM
➤ CVE-2026-28780	6.9 MEDIUM

> CVE-2026-29168	7.3 HIGH
> CVE-2026-29169	6.9 MEDIUM
> CVE-2026-33006	6.3 MEDIUM
> CVE-2026-33007	6.9 MEDIUM
> CVE-2026-33523	6.9 MEDIUM
> CVE-2026-33857	6.9 MEDIUM
> CVE-2026-34032	6.9 MEDIUM
> CVE-2026-34059	6.9 MEDIUM

CWE's

CWE	Beschrijving
> CVE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
> CVE-122	Heap-based Buffer Overflow
> CVE-125	Out-of-bounds Read
> CVE-126	Buffer Over-read
> CVE-170	Improper Null Termination
> CVE-208	Observable Timing Discrepancy
> CVE-269	Improper Privilege Management
> CVE-415	Double Free
> CVE-443	DEPRECATED: HTTP response splitting
> CVE-476	NULL Pointer Dereference
> CVE-770	Allocation of Resources Without Limits or Throttling
> CVE-1341	Multiple Releases of Same Resource or Handle

Getroffen producten

Apache Software Foundation

Apache HTTP
Server

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.