Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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

Getroffen producten

Apache Software Foundation
Apache HTTP Server

Disclaimer