Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0484

PRIORITEIT: NORMAAL

Kwetsbaarheid verholpen in Apache HTTP Server

Publicatiedatum: 12-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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 de-len. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Apache heeft een kwetsbaarheid verholpen in Apache HTTP Server, specifiek in de mod_http2 module (versies 2.4.55 tot 2.4.70) en mod_h2 module (versies 2.0.8 tot 2.0.42).

Duiding

De kwetsbaarheid betreft een concurrency probleem in de assign_headers functie van de mod_http2 en mod_h2 modules. De kwetsbaarheid maakt het mogelijk voor niet-geauthenticeerde externe aanvallers om op afstand willekeurige commando's uit te voeren, wat kan leiden tot remote code execution op servers waar HTTP/2 is ingeschakeld. Servers die alleen HTTP/1.1 ondersteunen zijn niet kwetsbaar.

Oplossingen

Apache heeft updates uitgebracht om de kwetsbaarheid te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

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

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-119618	9.8 CRITICAL

CWE's

CWE	Beschrijving
CWE-122	Heap-based Buffer Overflow
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization

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.