ALVD-2026-302

ID alternative: CVE-2026-23918

8.8 | I LARTË

PËRSHKRIM

Cenueshmëria i mundëson aktorit dashakeq të çaktivizojë serverin Apache dhe, në kushte të caktuara konfigurimi, të ekzekutojë kod (Remote Code Execution), duke shfrytëzuar një error në trajtimin e memories (memory-handling) brenda modulit mod_http2. Nëpërmjet kërkesave HTTP/2 të përgatitura posaçërisht dhe pa qenë nevoja për autentikim apo ndërveprim nga përdoruesi, sulmuesi e çon procesin e serverit në ndalim, duke ndërprerë menjëherë shërbimin. Në disa konfigurime specifike, i njëjti error në menaxhimin e memories mund të shkojë përtej thjesht ndalimit — çka e bën këtë cenueshmëri veçanërisht kritike për instalimet e ekspozuara drejtpërdrejt ndaj internetit.

MASAT E REKOMANDUARA

Përditësimi i Apache HTTP Server në versionin 2.4.67 mbetet zgjidhja e plotë dhe e drejtpërdrejtë për këtë problem. Deri në kryerjen e përditësimit, rekomandohet çaktivizimi i përkohshëm i protokollit HTTP/2 (mod_http2) në serverët e prekur, kufizimi i numrit të rrjedhave (streams) të njëkohshme për lidhje, si dhe monitorimi i vazhdueshëm i konsumit të memories dhe i stabilitetit të procesit httpd për shenja anomalie.

KRITIKALITETI
CVSS Base Score: 8.8 (I lartë)
Versioni CVSS: 3.1

PUBLISHED
04.05.2026

VENDOR
Apache Software Foundation

PRODUCT
Apache HTTP Server

VERSION
Versioni 2.4.66

PRODUKTI I PREKUR

PRODHUESI	PRODUKTI	VERSIONI	ZGJIDHUR	PUBLIKUAR
Apache Software Foundation	Apache HTTP Server	2.4.66	2.4.67	04.05.2026

REFERENCA

- https://httpd.apache.org/security/vulnerabilities_24.html
- https://www.cve.org/CVERecord?id=CVE-2026-23918
- https://euvd.enisa.europa.eu/vulnerability/CVE-2026-23918