DJ-CERT | Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 13-05-2026

BULLETIN ALERTES

Object	Vulnérabilité Critique dans Apache HTTP Server (mod_http2)
Réference	1469
Date de Publication	2026-05-13
Sévérité	Critique

IMPACT :

Exécution de code arbitraire à distance (RCE)

Déni de service

Corruption mémoire de type double free dans le tas (heap)

SYSTÉME AFFECTÉ :

Apache HTTP Server version 2.4.66 — module mod_http2 activé (activation par défaut)

DÉSCRIPTION :

CVE-2026-23918 est une vulnérabilité de type double free dans le composant mod_http2 d'Apache HTTP Server 2.4.66, spécifiquement dans le chemin de nettoyage des streams HTTP/2 (fichier h2_mplx.c).

Mécanisme d'exploitation : un client envoie une frame HTTP/2 HEADERS immédiatement suivie d'une frame RST_STREAM avec un code d'erreur non nul sur le même stream, avant que le multiplexeur ait eu le temps d'enregistrer le stream. Cette séquence de timing provoque l'exécution de deux callbacks qui poussent le même pointeur de stream dans le tableau de nettoyage (spurge array) deux fois. Lors du passage en nettoyage (c1_purge_streams), la fonction h2_stream_destroy est appelée deux fois sur le même pointeur — opérant ainsi sur de la mémoire déjà libérée.

Conséquences : dans le cas minimal, le crash du processus worker Apache provoque un déni de service. Dans un scénario avancé, la corruption du tas permet potentiellement une exécution de code à distance (RCE). Un PoC fonctionnel démontrant le DoS fiable par corruption du free list de l'allocateur est déjà disponible publiquement sur GitHub. La progression vers le RCE nécessite un grooming mémoire supplémentaire.

Caractéristiques critiques : l'attaque est non authentifiée, ne requiert aucune interaction utilisateur, et exploite une séquence de frames HTTP/2 parfaitement valide selon le RFC — indétectable au niveau réseau sans inspection du trafic TLS déchiffré.

NB : Un code d'exploitation (PoC) est disponible en sources ouvertes sur GitHub.

SOLUTION :

Mettre à jour immédiatement vers Apache HTTP Server 2.4.67.

DOCUMENTATION :

• Advisory officiel Apache HTTP Server
— https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-23918

• NVD — CVE-2026-23918 — https://nvd.nist.gov/vuln/detail/CVE-2026-23918

• Debian Security Tracker
— https://security-tracker.debian.org/tracker/CVE-2026-23918

• SUSE Security Advisory
— https://www.suse.com/security/cve/CVE-2026-23918.html

• PoC public GitHub — https://github.com/12lie20/CVE-2026-23918-test

• The Hacker News — Analyse technique
— https://thehackernews.com/2026/05/critical-apache-http2-flaw-cve-2026.html