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

Autorité Nationale de Cybersécurité

Djibouti le, 12-11-2026

BULLETIN ALERTES

Object	Vulnérabilité critique dans Apache HTTP Server (mod_http2)
Réference	1515
Date de Publication	2026-11-12
Sévérité	Critique

IMPACT :

- Exécution de code à distance
- Corruption mémoire
- Atteinte potentielle à la confidentialité, à l'intégrité et à la disponibilité des données

SYSTÉME AFFECTÉ :

- Apache HTTP Server versions 2.4.55 à 2.4.70
- mod_h2 (version autonome publiée sur GitHub) versions 2.0.8 à 2.0.42

DÉSCRIPTION :

Une vulnérabilité critique a été corrigée dans le module mod_http2 d'Apache HTTP Server. Elle vient d'un défaut de synchronisation dans la fonction assign_headers(), qui traite en parallèle les requêtes HTTP/2 multiplexées sur une même connexion. Un attaquant distant non authentifié peut l'exploiter pour corrompre la mémoire du processus serveur, puis exécuter du code arbitraire à distance. Seuls les serveurs où HTTP/2 (h2 ou h2c) est activé par la directive Protocols sont exposés.

SOLUTION :

Mettre à jour Apache HTTP Server vers la version corrigée suivante, conformément au Bulletin de sécurité Apache :

- Apache HTTP Server 2.4.71 (ou une version ultérieure)

DOCUMENTATION :

Bulletin de sécurité Apache HTTP Server :

- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-119618

CVE-2026-119618 :

- https://www.cve.org/CVERecord?id=CVE-2026-119618
- https://access.redhat.com/security/cve/cve-2026-119618