ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilité critique affectant le protocole HTTP/2
Numéro de Référence	44171010/23
Date de Publication	11 Octobre 2023
Risque	Critique
Impact	Critique

Systèmes affectés

- le protocole HTTP/2

Identificateurs externes

- CVE-2023-44487

Bilan de la vulnérabilité

Des chercheurs en sécurité informatique annoncent l'existence d'une vulnérabilité critique identifiée par «CVE-2023-44487 » affectant le protocole HTTP/2. Cette vulnérabilité est activement exploitée depuis Aout 2023 et peut permettre à des personnes malveillantes de causer un nouveau type d'attaque de déni de service distribué nommé « Rapid Reset ». Dans certaines campagnes d'attaques le nombre de requêtes du déni de service a atteint le nombre record de 398 millions de requêtes par seconde.

Solution

Vu que le protocole HTTP/2 est implémenté dans de multiples solutions, cette vulnérabilité concerne plusieurs éditeurs (Cloudflare, Google, AWS, NGNIX, Microsoft…). Nous vous invitons de vérifier si vous êtes concernés par cette vulnérabilité et appliquer les recommandations de l'éditeur de votre produit.

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Risque

- Déni de service distribué

Annexe

- Cloudflare: HTTP/2 Rapid Reset: deconstructing the record-breaking attack
- Google: How it works: The novel HTTP/2 'Rapid Reset' DDoS attack
- AWS: CVE-2023-44487 - HTTP/2 Rapid Reset Attack
- NGINX: HTTP/2 Rapid Reset Attack Impacting NGINX Products
- Microsoft :https://msrc.microsoft.com/blog/2023/10/microsoft-response-to-distributed-denial-of-service-ddos-attacks-against-http/2/