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	Vulnérabilités critiques dans Nagios Log Server
Numéro de Référence	57360910/25
Date de Publication	09 Octobre 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- Nagios Log Server versions antérieures à 2024R1.3.2.

Identificateurs externes

- CVE-2025-44823, CVE-2025-44824

Bilan de la vulnérabilité

Deux vulnérabilités critiques ont été corrigées dans Nagios Log Server. La première faille (CVE-2025-44823, CVSS 9.9) permet de récupérer en clair les clés API de tous les utilisateurs, y compris celles des administrateurs, entraînant un risque de prise de contrôle totale du serveur. La seconde (CVE-2025-44824, CVSS 8.5) permet d'interrompre le service Elasticsearch interne, provoquant une perte complète des journaux et des capacités d'alerte.

Des codes d'exploitation publics sont déjà disponibles, rendant ces vulnérabilités particulièrement dangereuses. Il est fortement recommandé de :

- mettre à jour immédiatement vers la version 2024R1.3.2 ou ultérieure,
- révoquer les tokens API existants,
- restreindre l'accès à l'API aux adresses IP de confiance pour limiter les risques d'exploitation.

Solution

Veuillez se référer au bulletin de sécurité Nagios, afin d'installer les dernières mises à jour.

Risque

- Elévation de privilèges
- Atteinte à la confidentialité des données
- Déni de service

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

- Prise de contrôle du système

Références

Bulletin de sécurité Nagios:

- https://www.nagios.com/changelog/#log-server