ROYAUME DU MAROC

ADMINISTRATION
DE LA DEFENSE NATIONALE

Direction Générale de la Sécurité des Systèmes d'Information

Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية

إدارة الدفاع الوطني

المديرية العامة لأمن نظم المعلومات

مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre	Vulnérabilité critique activement exploitée affectant GNU InetUtils telnetd
Numéro de Référence	60312601/26
Date de Publication	26 janvier 2026
Risque	Critique
Impact	Critique

Systèmes affectés

- GNU InetUtils de la version 1.9.3 jusqu'à la version 2.7

Identificateurs externes

- CVE-2026-24061

Bilan de la vulnérabilité

Une vulnérabilité critique affectant GNU InetUtils est activement exploitée. Cette vulnérabilité qui a fait l'objet du bulletin de sécurité de la DGSSI «60272601/26 », concerne plus particulièrement le service telnetd et peut permettre à un attaquant distant de contourner l'authentification pour se connecter avec des droits root.

Solution

Cette vulnérabilité affecte plusieurs distributions Linux/Unix quand GNU Inetutils telnetd est activé. GNU n'a toujours pas publié de mise à jour. Cependant le patch de telnetd est disponible et il peut être implémenté en modifiant et compilant le code dans telnetd/utility.c. Dans le cas où cette solution n'est pas possible, il est recommandé de restreindre l'accès au serveur telnetd ou de le désactiver temporairement.

Risque

- Contournement de l’authentification

Références

Bulletin de sécurité d NVD :

- https://nvd.nist.gov/vuln/detail/CVE-2026-24061

Bulletin de sécurité de GNU :

- https://www.openwall.com/lists/oss-security/2026/01/20/2