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

Autorité Nationale de Cybersécurité

Djibouti le, 19-03-2026

BULLETIN ALERTES

Object	Vulnérabilité dans telnetd
Réference	1444
Date de Publication	2026-03-19
Sévérité	Critique

IMPACT :

- Exécution de code arbitraire à distance
- Compromission complète du système
- Atteinte à la confidentialité, intégrité et disponibilité des données

SYSTÉME AFFECTÉ :

- GNU InetUtils telnetd versions antérieures ou égales à **2.7**

DÉSCRIPTION :

Une vulnérabilité critique a été identifiée dans le service telnetd de GNU InetUtils. Cette faille, due à un dépassement de mémoire (buffer overflow), peut être exploitée par un attaquant distant non authentifié en envoyant une requête spécialement conçue lors de la phase initiale de connexion. L'exploitation ne nécessite ni authentification ni interaction utilisateur et peut permettre l'exécution de code arbitraire avec les privilèges **root**, conduisant à une compromission complète du système.

CONTOURNEMENT PROVISOIRE :

En l’absence de correctif immédiat :

- Désactiver le service telnet s’il n’est pas nécessaire
- Bloquer le port 23 au niveau réseau et pare-feu
- Restreindre l’accès au service telnet
- Exécuter telnetd avec des privilèges réduits

Un correctif est attendu prochainement (annoncé début **avril 2026**).

DOCUMENTATION :

CVE-2026-32746 :

- https://www.cve.org/CVERecord?id=CVE-2026-32746