Autorité Nationale de Cybersécurité

Djibouti le, 19-05-2026

BULLETIN ALERTES

Object	Vulnérabilité critique dans Fortinet FortiAuthenticator
Réference	1476
Date de Publication	2026-05-19
Sévérité	Critique

IMPACT :

- Exécution de code à distance (RCE) sans authentification
- Compromission complète de l'appliance FortiAuthenticator
- Accès aux bases de données d'utilisateurs et tokens
- Risque de vol de credentials et de sessions administrateurs

SYSTÉME AFFECTÉ :

- FortiAuthenticator 8.0.0 à 8.0.2
- FortiAuthenticator 6.6.0 à 6.6.8
- FortiAuthenticator 6.5.0 à 6.5.6

DÉSCRIPTION :

CVE-2026-44277 est une vulnérabilité critique de **contrôle d'accès impropre** (CWE-284) dans **Fortinet FortiAuthenticator**.

Cette faille permet à un attaquant **non authentifié** d'envoyer des requêtes spécialement conçues vers les endpoints API de l'application. En raison d'une vérification d'autorisation insuffisante, l'attaquant peut exécuter des commandes ou du code non autorisé sur le système.

NB : cette vulnérabilité est activement exploitée.

SOLUTION :

Mettez à jour immédiatement vers une version corrigée, surtout si l’appliance est exposée sur Internet.

DOCUMENTATION :

- **ID Fortinet** : FG-IR-26-128
- **Source officielle** : FortiGuard PSIRT Advisory
- **NVD** : CVE-2026-44277