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

Autorité Nationale de Cybersécurité

Djibouti le, 03-02-2026

BULLETIN ALERTES

Object	Vulnérabilité dans FortiOS SSL VPN
Réference	1414
Date de Publication	2025-12-26
Sévérité	Critique

IMPACT :

- Contournement de la politique de sécurité
- Accès aux informations confidentielles

SYSTÉME AFFECTÉ :

- FortiOS 6.4.0 et versions inférieures
- FortiOS versions 6.2.0 à 6.2.3
- FortiOS 6.0.9 et versions inférieures

DÉSCRIPTION :

Fortinet a identifié la vulnérabilité CVE-2020-12812, affectant certains pare-feu FortiGate mal configurés. Cette faille est causée par une différence de gestion de la casse des noms d'utilisateur : FortiGate considère les noms d'utilisateur comme sensibles à la casse, contrairement aux services LDAP/Active Directory. Cette incohérence peut empêcher la reconnaissance d'un compte local protégé par 2FA et entraîner un basculement vers une authentification LDAP classique, permettant ainsi le contournement du mécanisme 2FA et donnant un accès non autorisé à des ressources sensibles telles que les interfaces d'administration et les VPN.

SOLUTION :

- Activer set username-sensitivity disable sur les comptes locaux.
- Mettre à jour FortiOS. (Se référer à la documentation)

DOCUMENTATION :

- Bulletin de sécurité Fortinet du 13 juillet 2020 :

https://fortiguard.com/psirt/FG-IR-19-283

- Security Advisory Fortinet du 24 Décembre 2025 :

https://www.fortinet.com/blog/psirt-blogs/product-security-advisory-and-analysis-observed-abuse-of-fg-ir-19-283