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	Exploitation active de la vulnérabilité de contournement 2FA de FortiOS SSL VPN
Numéro de Référence	59622612/25
Date de Publication	26 Décembre 2025
Risque	Critique
Impact	Critique

Systèmes affectés

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

Identificateurs externes

- CVE-2020-12812;

Bilan de la vulnérabilité

Fortinet a récemment observé une exploitation active de la vulnérabilité « CVE-2020-12812 », identifiée en juillet 2020. Cette faille concerne certains pare-feu FortiGate mal configurés et permet à des utilisateurs authentifiés via LDAP avec authentification à deux facteurs (2FA) de contourner le mécanisme 2FA.

La cause principale de cette vulnérabilité réside dans une différence de gestion de la casse des noms d'utilisateur. Par défaut, FortiGate considère les noms d'utilisateur comme sensibles à la casse, tandis que les services LDAP ou Active Directory ne font pas cette distinction. Cette incohérence permet à FortiGate d'échouer à reconnaître un utilisateur local protégé par 2FA et de basculer vers une authentification LDAP classique.

L'exploitation de la faille n'est possible que sous certaines conditions. Des utilisateurs locaux configurés sur le FortiGate avec 2FA doivent exister et être liés à un annuaire LDAP. Ces utilisateurs doivent également être membres de groupes LDAP, et au moins un de ces groupes doit être utilisé dans une règle d'authentification sur le FortiGate.

Dans un scénario d'attaque, si un utilisateur se connecte avec une variation de casse du nom d'utilisateur, FortiGate ne reconnaît pas le compte local. Le système tente alors une autre méthode d'authentification disponible et bascule vers l'authentification LDAP directe. Si les identifiants sont valides dans l'annuaire, l'accès est accordé sans exiger le 2FA.

L'impact de cette vulnérabilité est critique. Elle permet un contournement du 2FA, entraînant un accès non sécurisé à des ressources sensibles telles que des interfaces d'administration ou des accès VPN. Si une exploitation est avérée ou suspectée, l'environnement doit être considéré comme compromis, et une réinitialisation complète des identifiants, tant au niveau du FortiGate que de l'annuaire LDAP/Active Directory, est fortement recommandée.

Solution

Correctif intégré dans :

- FortiOS 6.0.10, 6.2.4, 6.4.1 et versions ultérieures ;

Paramètre clé à activer sur les comptes locaux :

- set username-sensitivity disable.

Risque

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

Référence

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