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	Zero-day dans les produits Fortinet
Numéro de Référence	60382801/26
Date de Publication	28 Janvier 2026
Risque	Critique
Impact	Critique

Systèmes affectés

- FortiAnalyzer version 7.6.x de 7.6.0 à 7.6.5 ;
- FortiAnalyzer version 7.4.x de 7.4.0 à 7.4.9 ;
- FortiAnalyzer version 7.2.x de 7.2.0 à 7.2.11 ;
- FortiAnalyzer version 7.0.x de 7.0.0 à 7.0.15 ;
- FortiManager version 7.6.x de 7.6.0 à 7.6.5 ;
- FortiManager version 7.4.x de 7.4.0 à 7.4.9 ;
- FortiManager version 7.2.x de 7.2.0 à 7.2.11 ;
- FortiManager version 7.0.x de 7.0.0 à 7.0.15 ;
- FortiOS version 7.6.x de 7.6.0 à 7.6.5 ;
- FortiOS version 7.4.x de 7.4.0 à 7.4.10 ;
- FortiOS version 7.2.x de 7.2.0 à 7.2.12 ;
- FortiOS version 7.0.x de 7.0.0 à 7.0.18 ;
- FortiProxy version 7.6.x de 7.6.0 à 7.6.4 ;
- FortiProxy version 7.4.x de 7.4.0 à 7.4.12 ;
- FortiProxy version 7.2.x : toutes les versions ;
- FortiProxy version 7.0.x : toutes les versions ;

N.B : Les produits suivants sont actuellement en cours d'investigation par Fortinet :

- FortiWeb;
- FortiSwitch Manager ;

Identificateurs externes

- CVE-2026-24858 ;

Bilan de la vulnérabilité

Fortinet a publié un avis de sécurité afin d'alerter sur une vulnérabilité zero-day activement exploitée, affectant plusieurs produits de son écosystème, notamment FortiGate (FortiOS), FortiManager, FortiAnalyzer et FortiProxy, lorsque la fonctionnalité FortiCloud SSO est activée. Cette vulnérabilité, référencée par « CVE-2026-24858 », est liée à une mauvaise gestion du processus d'authentification SSO entre FortiCloud et les équipements Fortinet enregistrés.

L'exploitation de cette vulnérabilité permet à un attaquant d'obtenir un accès administrateur complet à distance. Une fois connecté, l'attaquant peut modifier la configuration du pare-feu, créer ou modifier des comptes administrateurs, exfiltrer des fichiers de configuration, installer des règles persistantes ou utiliser l'équipement comme point d'appui pour des mouvements latéraux au sein du réseau interne.

Solution

Veuillez se référer au bulletin de sécurité Fortinet du 27 Janvier 2026 pour plus d'information.

Risque

- Exfiltration des données confidentielles ;
- Contournement de la politique de sécurité ;
- Elévation de privilèges ;
- Prise de contrôle du système affecté ;

Indicateurs de compromission (IOCs):

Ces IoCs sont basés sur des analyses d'incidents observés et partagés par Fortinet et des chercheurs tiers pour aider à la détection et à la réponse aux incidents.

SSO Login User Accounts :

- cloud-noc@mail.io
- cloud-init@mail.io

IP Addresses :

- 104.28.244.115
- 104.28.212.114
- 104.28.212.115
- 104.28.195.105
- 104.28.195.106
- 104.28.227.106

- 104.28.227.105
- 104.28.244.114
- 37.1.209.19
- 217.119.139.50

Compte local malveillant :

Après une authentification réussie via SSO, l'attaquant crée un compte administrateur local afin de maintenir un accès persistant.

Les noms de comptes observés incluent (liste non exhaustive) :

- audit
- backup
- backupadmin
- deploy
- itadmin
- remoteadmin
- secadmin
- security
- support
- svcadmin
- system

Annexe

Bulletins de sécurité Fortinet du 27 Janvier 2026:

- https://fortiguard.fortinet.com/psirt/FG-IR-26-060