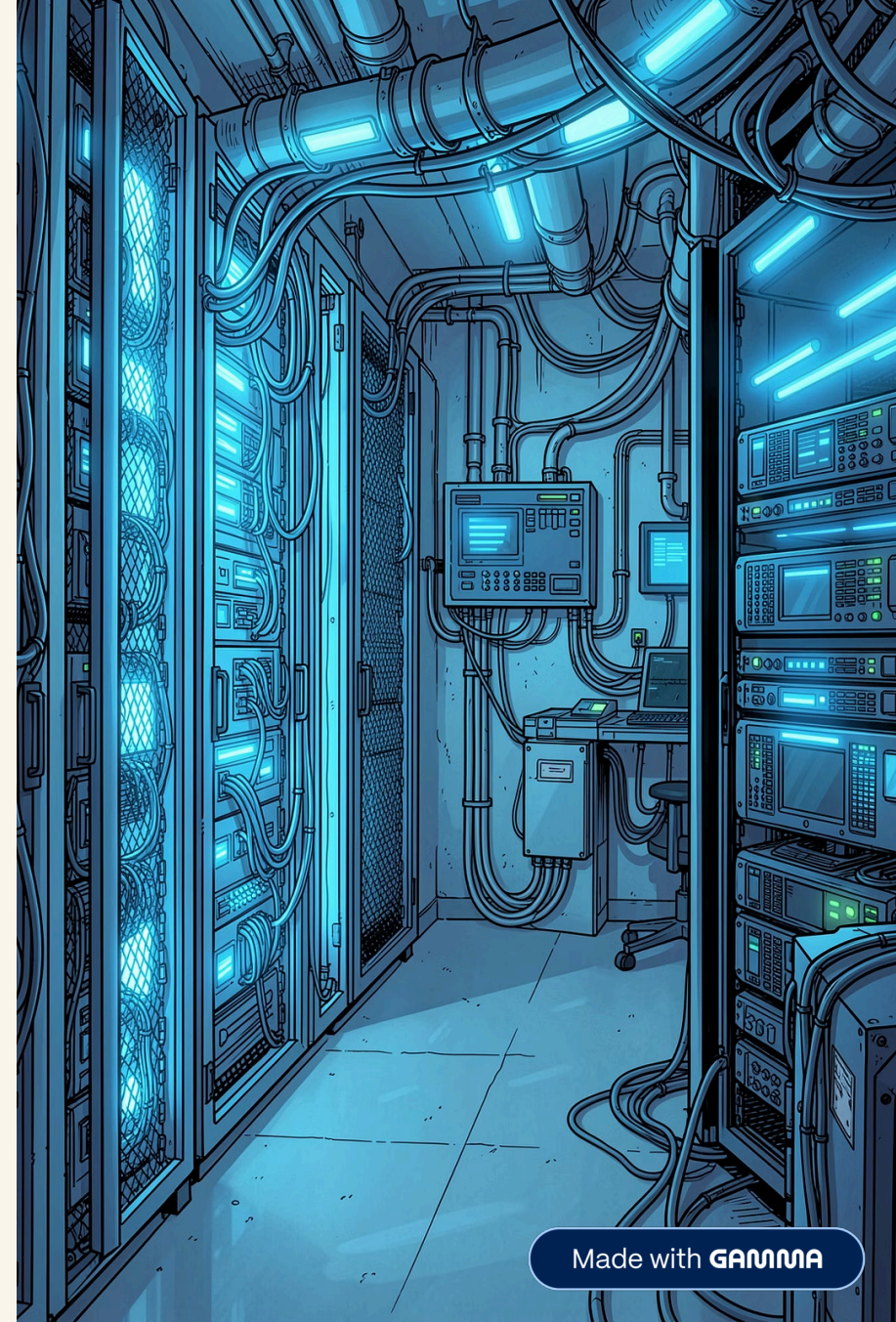


VEILLE TECHNOLOGIQUE 5 — FÉVRIER 2026


Vulnérabilité critique sur les pare-feux Fortinet

Découverte d'une faille de sécurité majeure touchant les équipements de périmètre Fortinet. Cette veille analyse les risques liés à l'exposition des interfaces d'administration sur Internet et l'importance d'une maintenance logicielle rigoureuse.




CONTEXTE

Une faille d'accès à distance sans authentification

 17 July

Quand

Février 2026

 Matériel

Pare-feux Fortigate (Fortinet)

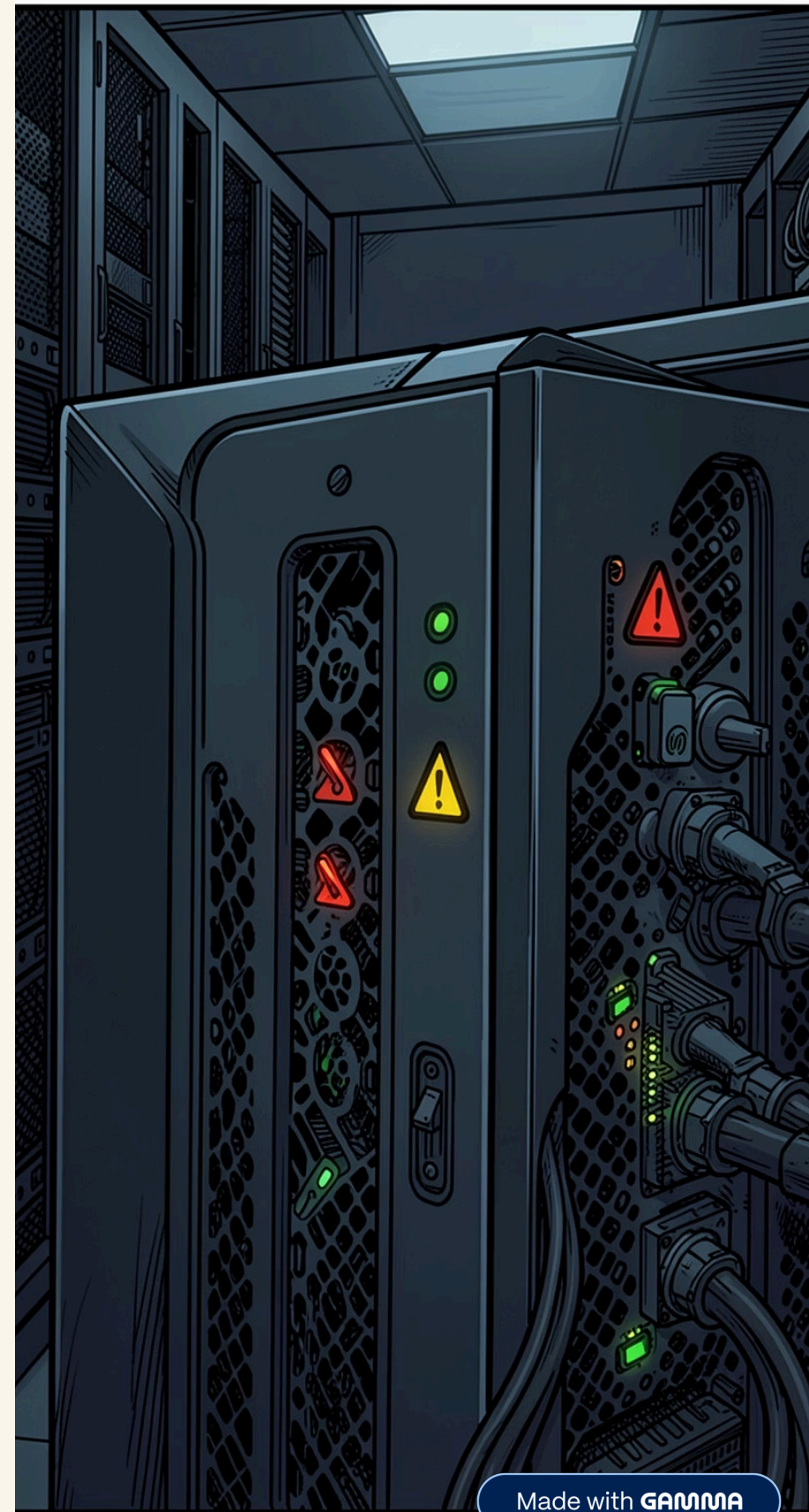
 Référence

CVE-2026-23113

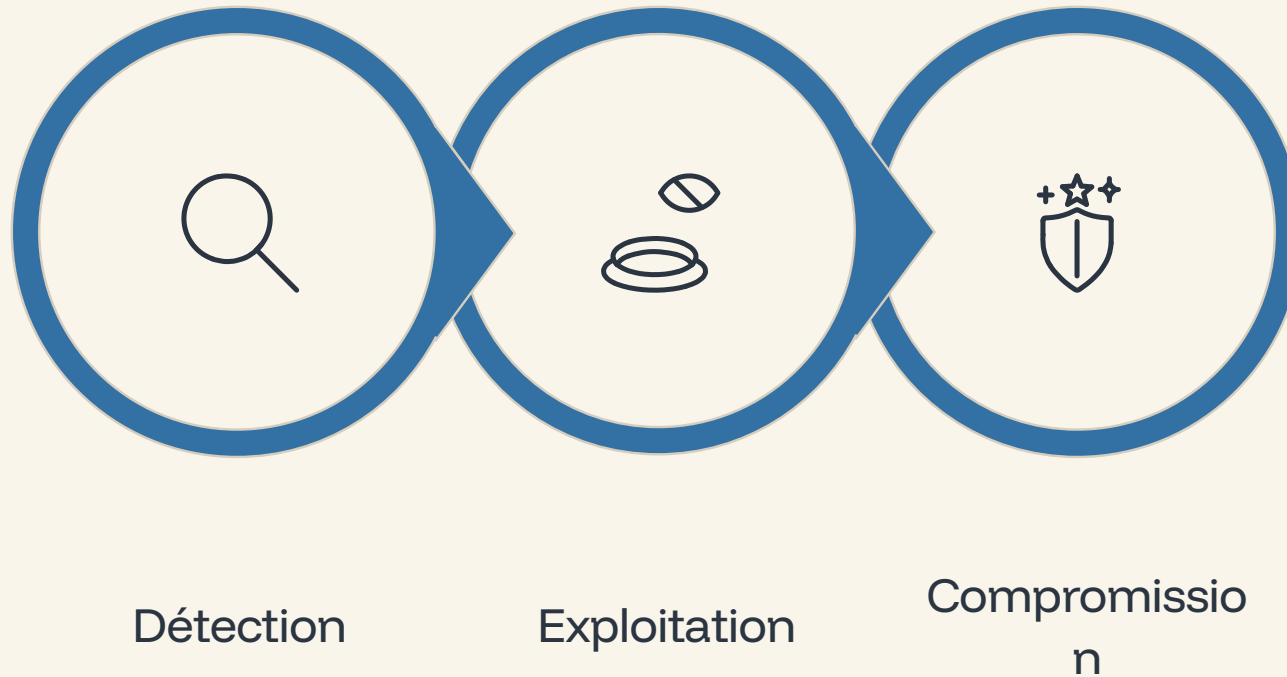
 Menace

Exécution de code à distance sans authentification

Un attaquant externe peut envoyer des commandes malveillantes directement au pare-feu — **sans identifiant, sans mot de passe, sans contournement du MFA.**



Comment l'attaque se déroule-t-elle ?



La simplicité de cette attaque la rend particulièrement dangereuse : aucune compétence avancée n'est requise pour l'exploiter dès lors que l'équipement est exposé sur Internet.



IMPACTS

Impacts potentiels sur l'infrastructure

Prise de contrôle

Modification de la configuration du pare-feu à distance pour ouvrir des accès permanents à l'attaquant.

Pivot réseau interne

Contournement du filtrage pour atteindre les serveurs, voler des données ou déployer un rançongiciel.

Coupure de service

Blocage complet du trafic Internet si l'équipement est rendu instable ou saboté par l'attaque.

SÉVÉRITÉ

Pourquoi cette faille est-elle critique ?

Cette combinaison de facteurs fait de CVE-2026-23113 une menace de **premier ordre** pour toute organisation disposant d'équipements Fortinet exposés.

 Tout pare-feu Fortigate accessible depuis Internet doit être considéré comme compromis jusqu'à preuve du contraire.



REMÉDIATION

Solutions techniques et remédiation

1

Mise à jour immédiate

Installer le correctif FortiOS fourni en urgence par Fortinet. Priorité absolue sur tous les équipements exposés.

2

Restriction des accès

Désactiver l'accès à l'interface de gestion depuis Internet. Administration uniquement depuis le réseau local ou via un accès ultra-sécurisé (VPN, bastion).

3

Analyse des logs

Vérifier l'historique des connexions pour détecter toute tentative d'exploitation antérieure à l'application du correctif.

Renforcer la posture de sécurité périmétrique

→ Segmenter les interfaces de gestion

Isoler l'administration des équipements dans un VLAN dédié, inaccessible depuis l'extérieur.

→ Activer la surveillance continue

Mettre en place des alertes automatiques sur les tentatives de connexion anormales vers les interfaces d'administration.

→ Planifier les mises à jour

Intégrer la veille CVE dans un processus formel de gestion des correctifs avec délais d'application définis.

Sources documentaires de la veille

1

Le Monde Informatique

12 février 2026 — « Fortinet publie des correctifs urgents pour une faille critique de commande à distance »

[lemondeinformatique.fr](https://www.lemondeinformatique.fr)

2

CERT-FR (ANSSI)

13 février 2026 — Bulletin d'alerte officiel : « Vulnérabilité critique dans FortiOS » — Réf : **CERTFR-2026-AVI-0214**

cert.ssi.gouv.fr

3

NVD — National Vulnerability Database

Février 2026 — Fiche technique : « CVE-2026-23113 Detail - Fortinet FortiOS Remote Code Execution »

nvd.nist.gov

