AVIS DE SECURITE

Objet	**Mise à jour de sécurité critique pour plusieurs produits Fortinet (FortiOS, FortiManager, FortiAnalyzer, FortiMail, FortiAuthenticator)**
Niveau de criticité	**CRITIQUE**
Référence	SNCSIRT-2026-ADS-267
TLP	WHITE

Résumé

Fortinet a publié le 21/10/2026 une mise à jour de sécurité qualifiée de prioritaire (« security hardening release ») pour FortiOS, FortiManager, FortiAnalyzer, FortiMail et FortiAuthenticator. Elle corrige des vulnérabilités de gravité critique et élevée identifiées dans le cadre du programme de tests de sécurité assistés par intelligence artificielle de l'éditeur. Les identifiants CVE, les scores CVSS et les détails techniques ne seront publiés que le 10/11/2026 ; l'éditeur, relayé par le Centre pour la Cybersécurité Belgique (CCB), recommande néanmoins d'appliquer les correctifs sans attendre, l'analyse différentielle des correctifs pouvant permettre à des attaquants de développer rapidement des exploits.

Aucune exploitation active n'est signalée à ce jour. Les mises à jour de FortiMail et FortiAuthenticator sont disponibles depuis le 21/10/2026, celles de FortiOS, FortiManager et FortiAnalyzer depuis le 22/10/2026 ; FortiSASE a été mis à jour automatiquement par l'éditeur.

Risque de sécurité

- Atteinte à la sécurité des équipements de sécurité périmétrique, de messagerie, d'authentification et d'administration centralisée (vulnérabilités critiques et élevées non encore détaillées)
- Exploitation rapide par rétro-ingénierie des correctifs (analyse différentielle assistée par IA)
- Chaînage de vulnérabilités de moindre gravité aboutissant à une compromission
- Atteinte à la confidentialité, à l'intégrité et à la disponibilité des systèmes

Systèmes affectés

- FortiOS 8.0.0 à 8.0.1, 7.6.0 à 7.6.7, 7.4.0 à 7.4.12, 7.2.0 à 7.2.13
- FortiManager 8.0.0 à 8.0.1, 7.6.0 à 7.6.7, 7.4.0 à 7.4.11, 7.2.0 à 7.2.12
- FortiAnalyzer 8.0.0 à 8.0.1, 7.6.0 à 7.6.7, 7.4.0 à 7.4.11, 7.2.0 à 7.2.12
- FortiMail 8.0.0 à 8.0.1, 7.6.0 à 7.6.6, 7.4.0 à 7.4.8, 7.2.0 à 7.2.9
- FortiAuthenticator 8.0.0 à 8.0.3, 6.6.0 à 6.6.10
- FortiManager Cloud et instances déployées en cloud public (mise à jour manuelle ou via le fournisseur cloud)

Recommandations

1. Mettre à jour sans délai, en priorisant les équipements exposés sur Internet, vers :
   - FortiOS 8.0.2, 7.6.8, 7.4.13 ou 7.2.14 ; FortiManager et FortiAnalyzer 8.0.2, 7.6.8, 7.4.12 ou 7.2.13 ;
   - FortiMail 8.0.2, 7.6.7 ou 7.4.9 (migrer vers la branche 7.4 ou ultérieure pour la branche 7.2) ;
   - FortiAuthenticator 8.0.4 ou 6.6.11 (ou versions ultérieures).
2. Sauvegarder les configurations avant la mise à jour et surveiller les journaux à la recherche d'accès administratifs inhabituels ou de modifications de configuration non approuvées ;
3. Dans l'attente, restreindre les interfaces d'administration HTTPS/SSH à des adresses de confiance, ne pas exposer FortiManager sur Internet et imposer l'authentification multifacteur à tous les comptes administrateurs.
4. Se référer à la publication de l'éditeur du 21/10/2026 et

   - https://www.fortinet.com/blog/ciso-collective/fortinet-releases-security-hardening-release-for-multiple-products
   - https://www.fortiguard.com/psirt
   - https://ccb.belgium.be/advisories/warning-fortinet-releases-critical-security-hardening-updates-multiple-products-patch

5. Les avis détaillés seront publiés sur le portail PSIRT le **10/11/2026**

Adresse : Avenue Leopold S. Senghor, BP: 4026, Dakar
https://www.stcc-ssi.sn/

E-mail : sncsirt@dcssi.sn

Date de publication : 23/10/2026