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

Autorité Nationale de Cybersécurité

Djibouti le, 12-11-2026

BULLETIN ALERTES

Object	Vulnérabilité critique dans Fortinet FortiMail
Réference	1513
Date de Publication	2026-11-12
Sévérité	Critique

IMPACT :

- Exécution de code à distance
- Atteinte potentielle à la confidentialité, à l'intégrité et à la disponibilité des données

SYSTÉME AFFECTÉ :

- FortiMail versions 8.0.0 à 8.0.1
- FortiMail versions 7.6.0 à 7.6.6
- FortiMail versions 7.4.0 à 7.4.8
- FortiMail 7.2, toutes versions

DÉSCRIPTION :

Une vulnérabilité critique de type traversée de répertoire (path traversal) a été corrigée dans Fortinet FortiMail. Elle se situe dans le composant API. Un attaquant distant non authentifié pourrait l'exploiter en envoyant des requêtes spécialement conçues, afin d'exécuter du code ou des commandes non autorisés sur l'équipement concerné.

SOLUTION :

Mettre à jour FortiMail vers les versions corrigées suivantes :

- FortiMail 8.0 : 8.0.2 (ou une version ultérieure)
- FortiMail 7.6 : 7.6.7 (ou une version ultérieure)
- FortiMail 7.4 : 7.4.9 (ou une version ultérieure)
- FortiMail 7.2 : migrer vers une version corrigée, aucun correctif n'étant publié pour cette branche

Selon l'éditeur, FortiMail Cloud a été corrigé le 5 octobre 2026 (micrologiciels 7.6.7 GA ou 8.0.2 GA). Les clients FortiMail Cloud n'ont donc aucune action à mener.

DOCUMENTATION :

Bulletin de sécurité Fortinet :

- https://fortiguard.fortinet.com/psirt/FG-IR-26-199

CVE-2026-126147 :

- https://www.cve.org/CVERecord?id=CVE-2026-126147