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

Autorité Nationale de Cybersécurité

Djibouti le, 11-11-2026

BULLETIN ALERTES

Object	Vulnérabilité critique dans Fortinet FortiClient
Réference	1512
Date de Publication	2026-11-11
Sévérité	Critique

IMPACT :

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

SYSTÉME AFFECTÉ :

- FortiClientMac versions 7.4.0 à 7.4.7
- FortiClientWindows versions 7.4.0 à 7.4.7
- FortiClientWindows versions 7.2.0 à 7.2.14
- FortiClientWindowsPAM versions 7.4.0 à 7.4.7
- FortiClientWindowsPAM versions 7.2.0 à 7.2.14

DÉSCRIPTION :

Une vulnérabilité critique a été corrigée dans FortiClient pour Mac, Windows et Windows PAM de Fortinet. Elle se trouve dans l'interface de programmation (API) locale de FortiClient, qui ne vérifie pas correctement l'origine des requêtes qu'elle reçoit. Un attaquant distant non authentifié peut ainsi faire exécuter du code ou des commandes non autorisés sur le poste de travail. L'exploitation nécessite une action de la victime.

SOLUTION :

Mettre à jour FortiClient vers les versions corrigées suivantes :

- FortiClientMac 7.4 : 7.4.8 (ou une version ultérieure)
- FortiClientWindows 7.4 : 7.4.8 (ou une version ultérieure)
- FortiClientWindows 7.2 : 7.2.15 (ou une version ultérieure)
- FortiClientWindowsPAM 7.4 : 7.4.8 (ou une version ultérieure)
- FortiClientWindowsPAM 7.2 : 7.2.15 (ou une version ultérieure)

DOCUMENTATION :

Bulletin de sécurité Fortinet

- https://fortiguard.fortinet.com/psirt/FG-IR-26-194

CVE-2026-121529 :

- https://www.cve.org/CVERecord?id=CVE-2026-121529