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

Autorité Nationale de Cybersécurité

Djibouti le, 12-03-2026

BULLETIN ALERTES

Object	Multiples vulnérabilités dans les produits Fortinet
Réference	1435
Date de Publication	2026-03-12
Sévérité	Elevé

IMPACT :

- Atteinte à la confidentialité des données
- Contournement de la politique de sécurité
- Déni de service
- Exécution de code arbitraire
- Injection de code indirecte à distance (XSS)
- Injection SQL (SQLi)
- Élévation de privilèges
- Vulnérabilités non spécifiées par l'éditeur

SYSTÉME AFFECTÉ :

- FortiAnalyzer Cloud versions antérieures à **7.6.5**
- FortiAnalyzer versions antérieures à **7.6.5**
- FortiAnalyzer-BigData versions **7.6.x antérieures à 7.6.1**
- FortiAnalyzer-BigData versions **antérieures à 7.4.5**
- FortiClientLinux versions **7.4.x antérieures à 7.4.5**
- FortiClientLinux versions **antérieures à 7.2.13**
- FortiDeceptor toutes versions **antérieures à 6.2.1**
- FortiMail versions **7.0.x antérieures à 7.0.9**
- FortiMail versions **7.2.x antérieures à 7.2.8**
- FortiMail versions **7.4.x antérieures à 7.4.5**
- FortiMail versions **7.6.x antérieures à 7.6.3**
- FortiManager Cloud versions **antérieures à 7.6.5**
- FortiManager versions **antérieures à 7.6.5**
- FortiRecorder toutes versions **antérieures à 7.2.4**
- FortiSandbox versions **antérieures à 4.4.8**
- FortiSIEM versions **7.3.x antérieures à 7.3.5**
- FortiSIEM versions **7.4.x antérieures à 7.4.1**
- FortiSOAR Agent Communication Bridge versions **antérieures à 1.1.1**
- FortiSwitchAXFixed versions **1.0.x antérieures à 1.0.2**
- FortiVoice versions **7.0.x antérieures à 7.0.7**
- FortiVoice versions **7.2.x antérieures à 7.2.1**
- FortiWeb versions **8.0.x antérieures à 8.0.4**
- FortiWeb versions **antérieures à 7.6.7**

DÉSCRIPTION :

Plusieurs vulnérabilités ont été identifiées dans certains produits Fortinet. Elles peuvent être exploitées par un attaquant pour exécuter du code arbitraire, élever ses privilèges, contourner des mécanismes de sécurité, accéder à des informations sensibles ou provoquer un déni de service. Certaines failles peuvent également permettre des attaques de type XSS ou injection SQL. Il est recommandé d'appliquer les mises à jour de sécurité publiées par l'éditeur afin de corriger ces vulnérabilités.

SOLUTION :

Mettre à jour les produits affectés vers les versions corrigées fournies par Fortinet. Se référer aux bulletins de sécurité de l'éditeur pour obtenir les correctifs.

DOCUMENTATION :

Bulletins Fortinet

- https://www.fortiguard.com/psirt/FG-IR-26-077
- https://www.fortiguard.com/psirt/FG-IR-26-078
- https://www.fortiguard.com/psirt/FG-IR-26-079
- https://www.fortiguard.com/psirt/FG-IR-26-080
- https://www.fortiguard.com/psirt/FG-IR-26-081
- https://www.fortiguard.com/psirt/FG-IR-26-082
- https://www.fortiguard.com/psirt/FG-IR-26-083
- https://www.fortiguard.com/psirt/FG-IR-26-084
- https://www.fortiguard.com/psirt/FG-IR-26-085
- https://www.fortiguard.com/psirt/FG-IR-26-086
- https://www.fortiguard.com/psirt/FG-IR-26-087
- https://www.fortiguard.com/psirt/FG-IR-26-088
- https://www.fortiguard.com/psirt/FG-IR-26-089
- https://www.fortiguard.com/psirt/FG-IR-26-090
- https://www.fortiguard.com/psirt/FG-IR-26-091
- https://www.fortiguard.com/psirt/FG-IR-26-092
- https://www.fortiguard.com/psirt/FG-IR-26-093
- https://www.fortiguard.com/psirt/FG-IR-26-094
- https://www.fortiguard.com/psirt/FG-IR-26-095
- https://www.fortiguard.com/psirt/FG-IR-26-096
- https://www.fortiguard.com/psirt/FG-IR-26-097
- https://www.fortiguard.com/psirt/FG-IR-26-098
- https://www.fortiguard.com/psirt/FG-IR-26-098

CVE-2025-48418 :

- https://www.cve.org/CVERecord?id=CVE-2025-48418

CVE-2025-48840 :

- https://www.cve.org/CVERecord?id=CVE-2025-48840

CVE-2025-49784 :

- https://www.cve.org/CVERecord?id=CVE-2025-49784

CVE-2025-53608 :

- https://www.cve.org/CVERecord?id=CVE-2025-53608

CVE-2025-54659 :

- https://www.cve.org/CVERecord?id=CVE-2025-54659

CVE-2025-54820 :

- https://www.cve.org/CVERecord?id=CVE-2025-54820

CVE-2025-55717 :

- https://www.cve.org/CVERecord?id=CVE-2025-55717

CVE-2025-66178 :

- https://www.cve.org/CVERecord?id=CVE-2025-66178

CVE-2025-68482 :

- https://www.cve.org/CVERecord?id=CVE-2025-68482

CVE-2025-68648 :

- https://www.cve.org/CVERecord?id=CVE-2025-68648

CVE-2026-22572 :

- https://www.cve.org/CVERecord?id=CVE-2026-22572

CVE-2026-22627 :

- https://www.cve.org/CVERecord?id=CVE-2026-22627

CVE-2026-22628 :

- https://www.cve.org/CVERecord?id=CVE-2026-22628

CVE-2026-22629 :

- https://www.cve.org/CVERecord?id=CVE-2026-22629

CVE-2026-24017 :

- https://www.cve.org/CVERecord?id=CVE-2026-24017

CVE-2026-24018 :

- https://www.cve.org/CVERecord?id=CVE-2026-24018

CVE-2026-24640 :

- https://www.cve.org/CVERecord?id=CVE-2026-24640

CVE-2026-24641 :

- https://www.cve.org/CVERecord?id=CVE-2026-24641

CVE-2026-25689 :

- https://www.cve.org/CVERecord?id=CVE-2026-25689

CVE-2026-25836 :

- https://www.cve.org/CVERecord?id=CVE-2026-25836

CVE-2026-25972 :

- https://www.cve.org/CVERecord?id=CVE-2026-25972

CVE-2026-30897 :

- https://www.cve.org/CVERecord?id=CVE-2026-30897