aDvens

Security for the greater good

Bulletin d’alerte
Vulnérabilité critique dans FortiSIEM

2024-02-06 | **TLP:CLEAR** | CERT aDvens - CTI
Advens - 16 Quai de la Mégisserie - 75001 Paris

aDvens

Sommaire

FortiSIEM - CVE-2024-23108/CVE-2024-23109

Le 5 février 2024, deux nouvelles vulnérabilités critiques dans Fortinet ont été publiées. Ces vulnérabilités identifiées en tant que CVE-2024-23108 et CVE-2024-23109, concernent l'API du produit FortiSIEM.

Un défaut de gestion des données envoyées via l'API de FortiSIEM permet à un attaquant non authentifié d'exécuter à distance du code arbitraire via des requêtes forgées.

Type de vulnérabilité

- **CWE-78** : Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Risque

- Exécution de code arbitraire

Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Changée
Complexité d'attaque	Faible	Impact sur la confidentialité	Élevé
Privilèges requis	Aucun	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

Produits impactés

- FortiSIEM versions comprises entre 7.1.0 et 7.1.1
- FortiSIEM versions comprises entre 7.0.0 et 7.0.2
- FortiSIEM versions comprises entre 6.7.0 et 6.7.8
- FortiSIEM versions comprises entre 6.6.0 et 6.6.3
- FortiSIEM versions comprises entre 6.5.0 et 6.5.2
- FortiSIEM versions comprises entre 6.4.0 et 6.4.2

Recommandations

- Mettre à jour FortiSIEM vers la version 6.7.9, 7.0.3, 7.1.3 ou ultérieure. Fortinet n'a pas confirmé que ces vulnérabilités sont corrigées par les dernières versions.

Preuve de concept

Actuellement, aucune preuve de concept n'est disponible en sources ouvertes.

Références

- https://www.cve.org/CVERecord?id=CVE-2024-23108
- https://www.cve.org/CVERecord?id=CVE-2024-23109
- https://www.fortiguard.com/psirt/FG-IR-23-130