aDvens

Security for the greater good

Bulletin d’alerte

Vulnérabilités critiques dans Fortinet

2024-02-09 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

Fortinet

Le 8 février 2024, Fortinet a publié 7 bulletins de vulnérabilités dans leurs produits. Les deux failles les plus critiques, CVE-2024-21762 et CVE-2024-23113, affectent FortiOS.

CVE-2024-21762

Cette faille provient d'un défaut de contrôle de la mémoire dans le *SSL-VPN* de FortiOS . Elle permet à un attaquant non authentifié d'exécuter du code arbitraire via des requêtes spécifiquement forgées.

Cette vulnérabilité est exploitée.

Type de vulnérabilité

- CWE-787 : Out-of-bounds Write

Risque

- Exécution de code arbitraire

Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Inchangée
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

FortiOS :

- Versions 6.0.x antérieures à 6.0.17 (incluse)
- Versions 6.2.x antérieures à 6.2.15 (incluse)
- Versions 6.4.x antérieures à 6.4.14 (incluse)
- Versions 7.0.x antérieures à 7.0.13 (incluse)
- Versions 7.2.x antérieures à 7.2.6 (incluse)
- Versions 7.4.x antérieures à 7.4.2 (incluse)

Recommandations

- Mettre à jour FortiOS vers la version 6.2.16, 6.4.15, 7.0.14, 7.2.7, 7.4.3, 7.6 ou ultérieure.
- Si les correctifs ne peuvent pas être déployé, Fortinet recommande de désactiver la fonctionalité *SSL-VPN*.
- Des informations complémentaires sont disponible dans le bulletin de Fortinet.

Preuve de concept

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

CVE-2024-23113

Cette faille est due à un défaut de contrôle de données transmises par l'utilisateur dans le *FortiGate to FortiManager Deamon* (*FGFMD*) de FortiOS. En envoyant des requêtes forgées, un attaquant non authentifié peut exécuter du code arbitraire.

Type de vulnérabilité

- CWE-134 : Use of Externally-Controlled Format String

Risque

- Exécution de code arbitraire

Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Inchangée
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

FortiOS :

- Versions 7.0.x antérieures à 7.0.13 (incluse)
- Versions 7.2.x antérieures à 7.2.6 (incluse)
- Versions 7.4.x antérieures à 7.4.2 (incluse)

Recommandations

- Mettre à jour FortiOS vers la version 7.0.14, 7.2.7, 7.4.3, 7.6 ou ultérieure.
- Des informations complémentaires sont disponible dans le bulletin de Fortinet.

Preuve de concept

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

Références

- https://www.cve.org/CVERecord?id=CVE-2024-21762
- https://www.cve.org/CVERecord?id=CVE-2024-23113
- https://www.fortiguard.com/psirt/FG-IR-24-015
- https://fortiguard.fortinet.com/psirt/FG-IR-24-029
- https://thehackernews.com/2024/02/fortinet-warns-of-critical-fortios-ssl.html