aDvens

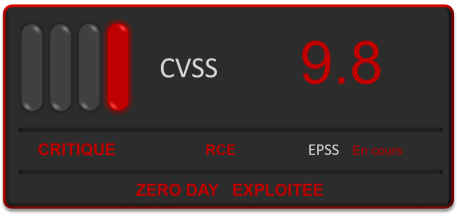
Security for the greater good

Newscast
Vulnérabilité critique FortiNet

2022-12-13 | **TLP:CLEAR** | CERT aDvens - CTI
Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

1. CVE-2022-42475 (Critique)



Découverte le 9 décembre 2022 par la société *Olympe Cyberdéfense* et officialisée par *FortiNet* le 12 décembre, cette vulnérabilité a été identifiée dans le service des communications sécurisées SSL-VPN.

Il s'agit d'une faille zero-day, de type débordement de tas (*Heap-based Buffer Overflow*), qui affecte les produits *FortiOS* et *FortiOS-6K7K*.

L'exploitation de cette vulnérabilité permet à un attaquant distant et non authentifié, via des requêtes spécifiquement forgées, d'exécuter du code arbitraire sur le système.

Cette vulnérabilité est exploitée.

1.1. Risque

- Exécution de code arbitraire à distance.

1.2. Type de vulnérabilité

- **CWE-122**: heap-based buffer overflow.

1.3. Criticité

Vecteur d'attaque : Réseau	Interaction de l'utilisateur : Non	Impact sur l'intégrité : Fort
Complexité d'attaque : Faible	Portée : Inchangée	Impact sur la disponibilité : Fort
Privilèges requis : Aucun	Impact sur la confidentialité : Fort	

1.4. Produits impactés

FortiOS

- De la version 7.2.0 à la version 7.2.2 (incluse).
- De la version 7.0.0 à la version 7.0.8 (incluse).
- De la version 6.4.0 à la version 6.4.10 (incluse).
- De la version 6.2.0 à la version 6.2.11 (incluse).

FortiOS-6K7K

- De la version 7.0.0 à la version 7.0.7 (incluse).
- De la version 6.4.0 à la version 6.4.9 (incluse).
- De la version 6.2.0 à la version 6.2.11 (incluse).
- De la version 6.0.0 à la version 6.0.14 (incluse).

1.5. Recommandations

Pour FortiOS, il est recommandé d'appliquer la mise à jour vers les versions suivantes ou ultérieures:

- Version 7.2.3.
- Version 7.0.9.
- Version 6.4.11.
- Version 6.2.12.

Pour FortiOS-6K7K, il est recommandé d'appliquer la mise à jour vers les versions suivantes ou ultérieures:

- Version 7.0.8.
- Version 6.4.10.
- Version 6.2.12.
- Version 6.0.15.

Des informations complémentaires sont disponibles sur le site de l'éditeur.

Si les correctifs ne peuvent être appliqués, Fortinet recommande de désactiver le module *SSL-VPN*.

1.6. Indices de compromission

La société FortiNet met à disposition des indicateurs de compromission discriminants d'une exploitation de la vulnérabilité et recommande aux utilisateurs de vérifier leurs journaux d'activité :

La présence de l'erreur suivantes :

- Logdesc="Application crashed" and msg="[…] application:sslvpnd,[…], Signal 11 received, Backtrace: […]"

Des communications vers les adresses IP ci-dessous, depuis FortiGate :

- 188.34.130.40 sur le port 444
- 103.131.189.143 sur les ports 30080,30081,30443 et 20443
- 192.36.119.61 sur les ports 8443 et 444
- 172.247.168.153 sur le port 8033

La présence des fichiers ci-dessous dans le système de fichiers :

- /data/lib/libips.bak
- /data/lib/libgif.so
- /data/lib/libiptcp.so
- /data/lib/libipudp.so
- /data/lib/libjepg.so
- /var/.sslvpnconfigbk
- /data/etc/wxd.conf
- /flash

1.7. Preuve de concept

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

2. Références

- https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:X/RC:C
- https://www.fortiguard.com/psirt/FG-IR-22-398
- https://www.cybersecurity-help.cz/vdb/SB2022121216
- https://exchange.xforce.ibmcloud.com/vulnerabilities/241856
- https://www.lemagit.fr/actualites/252528257/VPN-SSL-nouvelle-vulnerabilite-critique-inedite-chez-Fortinet
- https://olympecyberdefense.fr/vpn-ssl-fortigate/