aDvens

Security for the greater good

Newscast

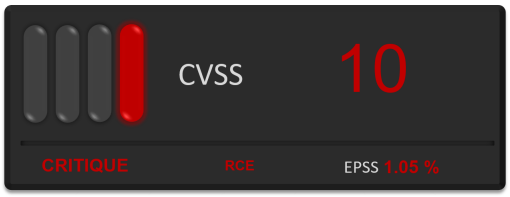
Vulnérabilité critique Synology

2023-01-05 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

1. CVE-2022-43931 (Critique)



Le 30 décembre 2022, la société taiwanaise Synology publie un bulletin de sécurité informant de la mise en ligne d'un correctif pour le composant VPN Plus Server (SRM 1.2 et SRM 1.3) de leurs routeurs.

VPN Plus Server permet de configurer des routeurs Synology comme serveur VPN.

Découverte par le chercheur Kevin Wang, la CVE-2022-43931 est une vulnérabilité de type «*out-of-bound write*» affectant la fonction *Remote Desktop*. Elle permet à un attaquant distant et non authentifié d'exécuter du code arbitraire.

Un routeur est un élément important d'un réseau informatique et reste une cible privilégiée par les attaquants. Au début de l'année 2020, le botnet Dark Nexus a exploité la vulnérabilité CVE-2019-7256 pour injecter du code dans différents routeurs (e.g. DGN1000 de Netgear) afin de mener des campagnes massives de DDoS.

1.1. Risque

- Exécution de code arbitraire à distance.

1.2. Type de vulnérabilité

- **CWE-787**: Out-of-bounds Write

1.3. Criticité

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

1.4. Produits impactés

- VPN Plus Server SRM 1.2, les versions antérieures à 1.4.3-0534.
- VPN Plus Server SRM 1.3, les versions antérieures à 1.4.4-0635.

1.5. Recommandations

- Mettre à jour VPN Plus Server SRM 1.2 vers la version 1.4.3-0534 ou ultérieures.
- Mettre à jour VPN Plus Server SRM 1.3 vers la version 1.4.4-0635 ou ultérieures.
- Des informations complémentaires sont disponibles sur le site du constructeur.

1.6. Preuve de concept

Aucune preuve de concept (POC) n'est disponible en sources ouvertes.

2. Références

- https://exchange.xforce.ibmcloud.com/vulnerabilities/243599
- https://www.synology.com/en-global/security/advisory/Synology_SA_22_26
- https://nvd.nist.gov/vuln/detail/CVE-2022-43931
- https://www.it-connect.fr/synology-a-corrige-une-faille-de-securite-critique-dans-vpn-plus-server/