aDvens

Security for the greater good

Bulletin d’alerte

Vulnérabilité critique dans CISCO IOS XE

2023-10-31 | **TLP:CLEAR** | CERT aDvens - CTI
Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

CVE-2023-20198 (EXPLOITÉE) 2
Type de vulnérabilité 2
Risque 2
Criticité (score de base CVSS v3.1) 2
Produit impacté 2
Recommandations 2
Correctif 2
Arbre de décision 3
Agence CISA 3
Indicateur de compromission 3
Vérifications des journaux d'activité 3
Vérifications de la présence d'implant 3
Preuve de concept 4
RÉFÉRENCES 5

CVE-2023-20198 (Exploitée)

Le 16 octobre 2023, *Cisco* alerte dans son bulletin de sécurité la découverte de la CVE-2023-20198 : une vulnérabilité critique et activement exploitée qui affecte l'interface utilisateur Web de Cisco *IOS XE*.

Mise à jour du 31 octobre 2023 : Cette faille provient d'un défaut de contrôle des requêtes envoyées par l'utilisateur et permet de contourner des vérifications effectués par Nginx.

Mise à jour du 31 octobre 2023 : En envoyant une requête spécifiquement forgée, un attaquant non authentifié peut accéder au service *wsma*, sans passer par *WSMASendCommand* (qui vérifie l'authentification), lui permettant d'exécuter des commandes, modifier la configuration et de créer un nouvel utilisateur disposant de privilèges de niveau 15.

Cette vulnérabilité est activement exploitée.
Mise à jour du 31 octobre 2023 : Le 25 octobre, Censys estime qu'environ **28 000 appareils** Cisco exposés sur internet ont été compromis.

Type de vulnérabilité

CWE-269 : Improper Privilege Management

Risque

- Élévation de privilèges

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

Produit impacté

- Cisco IOS XE : lorsque l'interface utilisateur Web est activée.

Recommandations

Correctif

- Mise à jour du 31 octobre 2023 : Mettre à jour Cisco IOS XE vers la version 16.12.10a, 17.3.8a, 17.6.5a, 17.6.6a, 17.9.4a ou ultérieure. La mise à jour 17.12.2 est également prévue pour le 15 novembre 2023. Des informations sur les correctifs sont disponibles dans le bulletin de Cisco dédié.
- Des informations complémentaires sont disponibles sur le site de l'éditeur.

Arbre de décision

Ci-dessous, un arbre de décision proposée par l'éditeur.

Utilisez-vous IOS XE ?

- Non, le système n'est pas vulnérable. Aucune autre action n'est nécessaire.
- Oui.

Si oui, les *serveurs IP HTTP* ou les *serveurs sécurisés IP HTTP* sont-ils configurés ?

- Non. La vulnérabilité n'est pas exploitable. Aucune autre action n'est nécessaire.
- Oui.

Si oui, utilisez-vous des services qui nécessitent une communication HTTP / HTTPS (par exemple, eWLC) ?

- Non. Désactivez la fonctionnalité *serveur HTTP/HTTPS*.
- Oui.

Si oui, limitez l'accès à ces services aux réseaux de confiance.

Il existe un risque d'interruption des services de production lors de la mise en œuvre des contrôles d'accès.

Après l'implémentation de ces modifications, la commande *copy running-configuration startup-configuration* doit être exécutée pour enregistrer la nouvelle configuration.

Agence CISA

L'agence CISA met à disposition la ressource suivante

- BOD 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities

Indicateur de compromission

Vérifications des journaux d'activité

Dans les journaux d'activité du système, vérifier la présence des messages où l'utilisateur pourrait être cisco_tac_admin, cisco_support ou un utilisateur inconnu de l'administrateur:

```
%SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as user on line
```

```
%SEC_LOGIN-5-WEBLOGIN_SUCCESS: Login Success [user: user] [Source: source_IP_address] at 03:42:13 UTC Wed
Oct 11 2023
```

%SYS-5-CONFIG_P est indiqué lorsqu'un utilisateur accède à l'interface utilisateur Web. L'indicateur à rechercher est celui des **noms d'utilisateur nouveaux** ou **inconnus** présents dans le message.

Dans les journaux d'activité du système, vérifier les messages dans lesquels le nom de fichier est inconnu et qui ne correspondent pas à une action d'installation de fichier attendue :

```
%WEBUI-6-INSTALL_OPERATION_INFO: User: username, Install Operation: ADD filename
```

Vérifications de la présence d'implant

La commande suivante permet d'indiquer la présence d'un implant. "*Systemip*" correspond à l'adresse IP du système à vérifier.

Cette commande doit être émise depuis un poste de travail ayant accès au système :

```
curl -k -X POST "https://systemip/webui/logoutconfirm.html?logon_hash=1"
```

Un implant **est présent si la réponse est une chaine hexadécimale**.

Si le système est configuré pour l'accès HTTP uniquement, utilisez HTTP dans la commande.

Pour détecter une exploitation, les identifiants de règles *Snort* sont disponibles

- 3:50118:2 - Alerte de l'injection initiale d'un implant
- 3:62527:1 - Alerte de l'interaction de l'implant
- 3:62528:1 - Alerte de l'interaction de l'implant
- 3:62529:1 - Alerte de l'interaction de l'implant

Preuve de concept

Mise à jour du 31 octobre 2023 : Une preuve de concept est disponible en sources ouvertes depuis le 30 octobre 2023.

Références

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z
- https://nvd.nist.gov/vuln/detail/CVE-2023-20198
- https://www.cybersecurity-help.cz/vdb/SB2023101701
- https://exchange.xforce.ibmcloud.com/vulnerabilities/268681
- https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-dublin-17121/221128-software-fix-availability-for-cisco-ios.html
- https://www.cisa.gov/guidance-addressing-cisco-ios-xe-web-ui-vulnerabilities
- https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/