aDvens

Security for the greater good

Bulletin d’alerte

Vulnérabilité critique dans CISCO IOS XE

2023-10-23 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

CVE-2023-20273 (Exploitée)

Le 20 octobre 2023, *Cisco* a mis à jour un bulletin de sécurité afin d'indiquer la découverte d'une nouvelle 0-day : la CVE-2023-20273. Cette vulnérabilité a été exploitée suite à la compromission via la CVE-2023-20198.

Cette faille permet à un attaquant authentifié d'exploiter un défaut dans l'interface utilisateur web afin d'injecter des commandes avec les privilèges *root* et d'exécuter du code arbitraire.

Cette vulnérabilité est activement exploitée. Talos Intelligence a observé l'exploitation de cette vulnérabilité, suite à une primo-infection par la CVE-2023-20198, afin d'installer des implants LUA.

Risque

- Élévation de privilèges
- 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	Élevé	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

Produit impacté

Les versions suivantes de Cisco IOS XE lorsque l'interface utilisateur Web est activée :

- versions 16.12 (seul Catalyst 3650 et 3850)
- versions 17.3
- versions 17.6
- versions 17.9

Recommandations

Le CERT aDvens recommande de tester les mesures de contournement proposées dans un environnement dédié avant leur déploiement en production afin de prévenir tout effet de bord.

Correctif

- Mettre à jour Cisco IOS XE versions 17.9 vers la version 17.9.4.
- D'autres mises à jour seront publiées prochainement. Il est possible de rester informé en surveillant 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

Preuve de concept

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

Indicateurs 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 - Alerte de l'injection initiale d'un implant (CVE-2023-20273)
- 3:62527 - Alerte de l'interaction de l'implant
- 3:62528 - Alerte de l'interaction de l'implant
- 3:62529 - Alerte de l'interaction de l'implant
- 3:62541 - Alerte de tentatives d'intrusion via la CVE-2023-20198.
- 3:62542 - Alerte de tentatives d'intrusion via la CVE-2023-20198.

TLP	TYPE	VALEUR
TLP:CLEAR	IP	5.149.249.74
TLP:CLEAR	IP	154.53.56.231
TLP:CLEAR	IP	154.53.63.93
TLP:CLEAR	identifiant	cisco_tac_admin
TLP:CLEAR	identifiant	cisco_support
TLP:CLEAR	identifiant	cisco_sys_manager

Références

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z
- 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://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/