DJ-CERT | Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 18-10-2023

BULLETIN ALERTES

Object	Vulnérabilité dans Cisco IOS XE
Réference	1050
Date de Publication	2023-10-17
Sévérité	Critique

IMPACT :

- Contournement de la politique de sécurité
- Exécution de code arbitraire à distance
- Accès aux informations confidentielles

SYSTÉME AFFECTÉ :

- Cisco IOS XE avec la fonction « web UI » activée

DÉSCRIPTION :

Cisco a publié un avis de sécurité le 16 octobre 2023 pour une vulnérabilité critique dans son interface Web de gestion IOS XE. Cette vulnérabilité permet à un attaquant non authentifié de créer un compte administrateur sur un équipement vulnérable. Cela donne à l'attaquant un accès complet à l'équipement, ce qui peut entraîner une compromission complète du réseau.

Cisco n'a pas encore publié de correctif pour cette vulnérabilité. Cependant, l'entreprise a indiqué qu'elle est activement exploitée par des attaquants. L'avis de sécurité de Cisco fournit des indicateurs de compromission qui peuvent être utilisés pour détecter les attaques.

CONTOURNEMENT PROVISOIRE :

Cisco recommande de désactiver le serveur HTTP sur tous les systèmes connectés à Internet. Pour cela, utilisez la commande « no ip http server » ou « no ip http secure-server » en mode de configuration globale. Si vous utilisez les deux serveurs, vous devez utiliser les deux commandes pour les désactiver.

DOCUMENTATION :

Bulletin de sécurité Cisco du 16 Octobre 2023:

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

CVE CVE-2023-20198 :

https://www.cve.org/CVERecord?id=CVE-2023-20198