FAQ technique du centre d'assistance technique Cisco pour le logiciel Cisco IOS XE Vulnérabilité de remontée des privilèges de l'interface utilisateur Web - CVE-2023-20198

Table des matières

Introduction

Aperçu

1. Mon produit est-il affecté ?

2. Comment puis-je déterminer si mon produit exécute Cisco IOS XE ?

3. J'utilise des exemples d'utilisation de redirection Identity Services Engine (ISE) et je ne peux pas désactiver les serveurs http/https. Que puis-je faire ?

4. J'utilise le contrôleur de réseau local sans fil (WLC) C9800 et je ne peux pas désactiver les serveurs http/http. Que puis-je faire ?

5. Dans l'avis de sécurité, il est mentionné qu'il existe des règles de détection et de blocage de cette vulnérabilité. Comment puis-je confirmer que ces règles sont installées et qu'elles fonctionnent sur mon FTD ?

6. J'ai un CUBE (Cisco Unified Border Element) qui exécute Cisco IOS XE. Puis-je désactiver le serveur http/https ?

7. J'ai un Cisco Unified Communications Manager Express (CME) exécutant Cisco IOS XE. Puis-je désactiver le serveur http/https ?

8. Si je désactive le serveur http/https, cela aura-t-il un impact sur ma capacité à gérer mes périphériques avec Cisco DNA Center ?

9. La désactivation du serveur HTTP/HTTPS sur le périphérique aura-t-elle un impact sur Smart Licensing ?

10. Un acteur de la menace peut-il exploiter la vulnérabilité et créer un utilisateur local même si AAA est en place ?

11. Quelle doit être la réponse « curl » si j'utilise mon routeur comme serveur AC et que la liste de contrôle d'accès HTTP/S est déjà configurée pour bloquer l'adresse IP de l'ordinateur ?

12. Où puis-je trouver des informations sur la disponibilité des correctifs logiciels ou des unités de maintenance logicielle (SMU) ?

Introduction

Ce document représente la FAQ technique du Centre d'assistance technique de Cisco pour la vulnérabilité de remontée des privilèges de l'interface utilisateur Web du logiciel Cisco IOS XE. Des détails supplémentaires sont disponibles dans l'avis de sécurité pour la vulnérabilité et le blog Cisco Talos.

Aperçu

Ce document décrit les implications de la désactivation des commandes ip http server ou ip http

secure-server et quelles autres fonctionnalités sont affectées par cette désactivation. En outre, il fournit des exemples sur la façon de configurer les listes d'accès décrites dans l'avis pour limiter l'accès au webui dans le cas où vous ne pouvez pas désactiver complètement les fonctionnalités.

1. Mon produit est-il affecté ?

Seuls les produits exécutant le logiciel Cisco IOS XE avec les versions 16.x et ultérieures sont concernés. Les produits Nexus, l'ACI, les périphériques IOS traditionnels, IOS XR, les pare-feu (ASA/FTD) et ISE ne sont pas affectés. Dans le cas d'Identity Services Engine, la désactivation du serveur http/https peut avoir d'autres implications. Reportez-vous à la section ISE.

2. Comment puis-je déterminer si mon produit exécute Cisco IOS XE ?

Exécutez la commande show version à partir de l'interface de ligne de commande (CLI) et vous verrez le type de logiciel suivant :

switch#show version

Logiciel Cisco IOS XE, version 17.09.03

Logiciel Cisco IOS [Cupertino], Logiciel C9800-CL (C9800-CL-K9_IOSXE), Version 17.9.3, LOGICIEL DE VERSION (fc6)

Assistance technique : http://www.cisco.com/techsupport

Copyright (c) 1986-2023 par Cisco Systems, Inc.

Compilé mar. 14-mars-23 18:12 par mcpre

Logiciel Cisco IOS-XE, Copyright (c) 2005-2023 par cisco Systems, Inc.

Tous droits réservés. Certains composants du logiciel Cisco IOS-XE sont concédés sous licence GNU General Public License ("GPL") Version 2.0. Le code logiciel concédé sous licence GPL Version 2.0 est un logiciel gratuit qui n'est ABSOLUMENT PAS COUVERT PAR LA GARANTIE. Vous pouvez redistribuer et/ou modifier ce code GPL selon les termes de la GPL Version 2.0. Pour plus d'informations, consultez la documentation ou le fichier "License Notice" accompagnant le logiciel IOS-XE, ou l'URL applicable fournie sur le prospectus accompagnant le logiciel IOS-XE.

Seules les versions logicielles 16.x et ultérieures sont affectées par cette vulnérabilité. Les exemples de versions logicielles concernées sont les suivants :

16.3.5

16.12.4

17.3.5

17.6.1

17.9.4

Exemples de versions d'IOS XE NON affectées :

3.17.4S

3.11.7E

15,6-1,S4

15,2-7,E7

3. J'utilise des exemples d'utilisation de redirection Identity Services Engine (ISE) et je ne peux pas désactiver les serveurs http/https. Que puis-je faire ?

La désactivation de ip http server et ip http secure-server empêchera les cas d'utilisation tels que ceux-ci de fonctionner :

- Profilage basé sur un capteur de périphérique
- Redirection de posture et détection
- Redirection d'invité
- Intégration du BYOD
- Intégration MDM

Sur les périphériques IOS-XE qui ne nécessitent pas d'accès au webui, il est recommandé d'utiliser les commandes suivantes pour empêcher l'accès au webui tout en autorisant les cas d'utilisation de redirection ISE :

- ip http active-session-modules none
- ip http secure-active-session-modules none

Si l'accès au webui est nécessaire, comme avec les contrôleurs Catalyst 9800, l'accès au webui peut être restreint à l'aide de listes de contrôle d'accès http access-class : https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-17/221107-filter-traffic-destin...

Les listes de contrôle d’accès http access-class permettent toujours aux cas d’utilisation de redirection ISE de fonctionner.

4. J'utilise un contrôleur de réseau local sans fil (WLC) C9800 et je ne peux pas désactiver les serveurs http/http. Que puis-je faire ?

A4. La désactivation de ip http server et ip http secure-server interrompra les cas d'utilisation suivants :

- Accès à l'interface utilisateur Web du WLC. Cela est vrai que l'interface de gestion sans fil (WMI), le port de service ou toute autre interface SVI soit utilisé pour accéder à l'interface utilisateur graphique WebAdmin.
- L'assistant de configuration du jour 0 échouera.
- Authentification Web - Accès invité si la page interne du WLC, la page d'authentification Web personnalisée, l'authentification Web locale, l'authentification Web centrale cesseront d'être redirigées
- Sur un C9800-CL, la génération de certificat auto-signé échouera
- Accès RESTCONF
- S3 et Cloudwatch
- Hébergement d'applications IOX sur les points d'accès sans fil

Pour continuer à utiliser ces services, vous devez effectuer les étapes suivantes :

(1) Maintenir HTTP/HTTPS activé

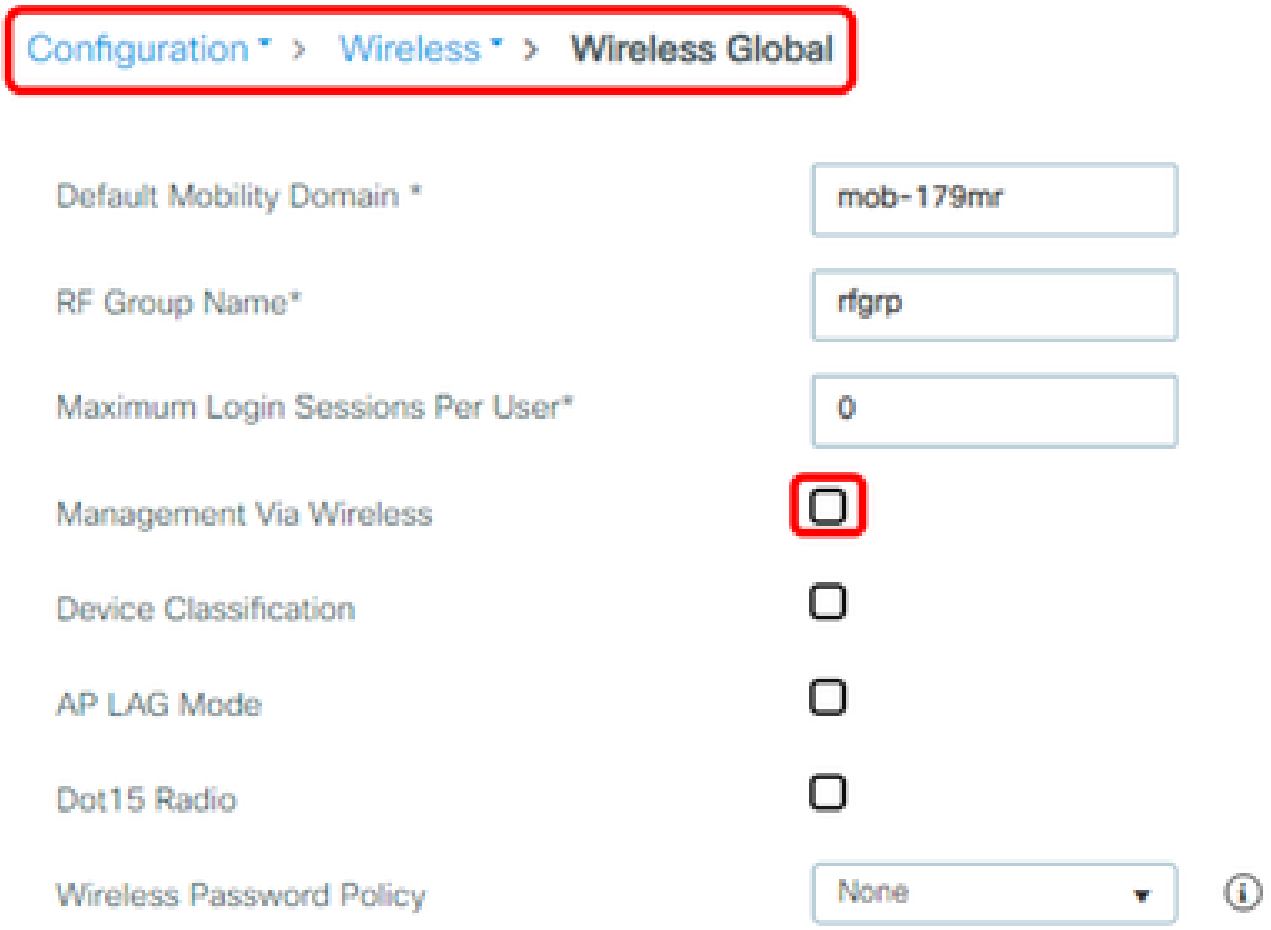
(2) Utilisez une liste de contrôle d'accès pour limiter l'accès au serveur Web C9800 WLC, uniquement aux sous-réseaux/adresses approuvés.
Vous trouverez des détails sur la configuration de la liste de contrôle d'accès : https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-17/221107-filter-traffic-destined-to-cisco-ios-xe.html.

Remarque :

1. Les WLC AireOS ne sont pas vulnérables
2. Tous les facteurs de forme de C9800 (C9800-80, C9800-40, C9800-L, C9800-CL), y compris le sans fil intégré sur AP (EWC-AP) et le sans fil intégré sur commutateur (EWC-SW), sont vulnérables
3. La liste de contrôle d'accès HTTP bloquera uniquement l'accès au serveur HTTP sur le WLC C9800. Il n'aura pas d'impact sur l'accès invité WebAuth que ce soit en utilisant la page interne du WLC, la page d'authentification Web personnalisée, l'authentification Web locale ou l'authentification Web centrale
4. La liste de contrôle d'accès HTTP n'a pas non plus d'impact sur le trafic de données ou de contrôle CAPWAP.
5. Assurez-vous que les réseaux non approuvés tels que les invités ne sont pas autorisés dans la liste de contrôle d'accès HTTP.

Si vous souhaitez bloquer complètement l'accès de vos clients sans fil à l'interface utilisateur graphique WebAdmin, assurez-vous que l'option Gestion via le réseau sans fil est désactivée.

IUG:



CLI :

```
C9800(config)#no wireless mgmt-via-wireless
C9800(config)#exit
```

5. Dans l'avis de sécurité, il mentionne qu'il y a des règles de sniffage pour détecter et bloquer cette vulnérabilité. Comment puis-je confirmer que ces règles sont installées et qu'elles fonctionnent sur mon FTD ?

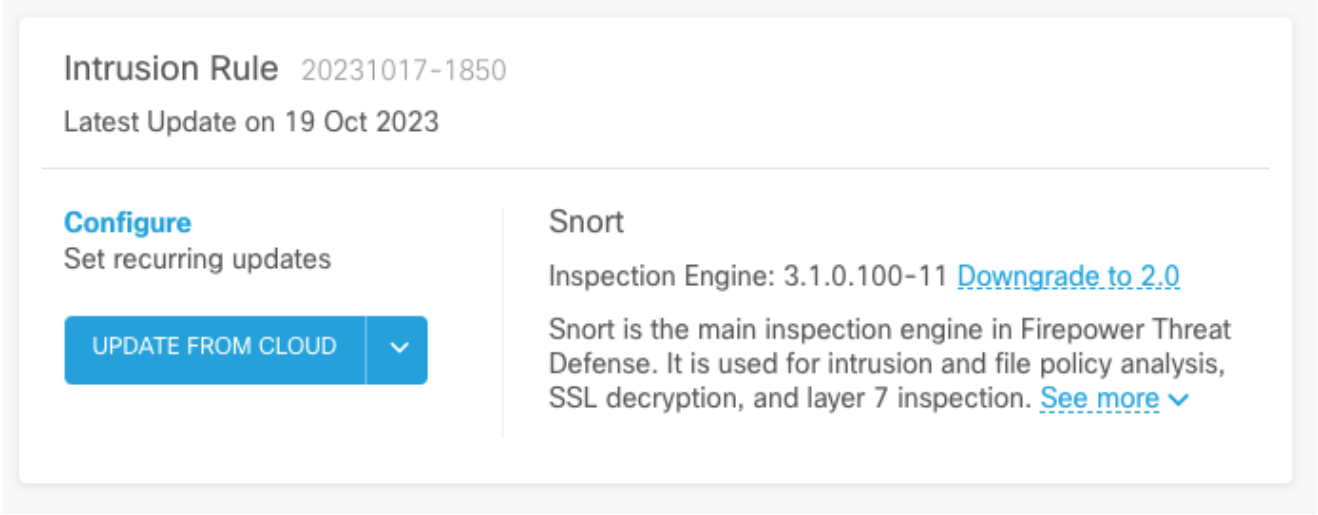
Pour vous assurer que les règles Snort sont installées sur votre périphérique, vérifiez que vous disposez du LSP 20231014-1509 ou du SRU-2023-10-14-001. Vérifiez si ce dernier est installé différemment sur les périphériques gérés par FDM et FMC :

a. Assurez-vous que les règles sont installées :

FDM

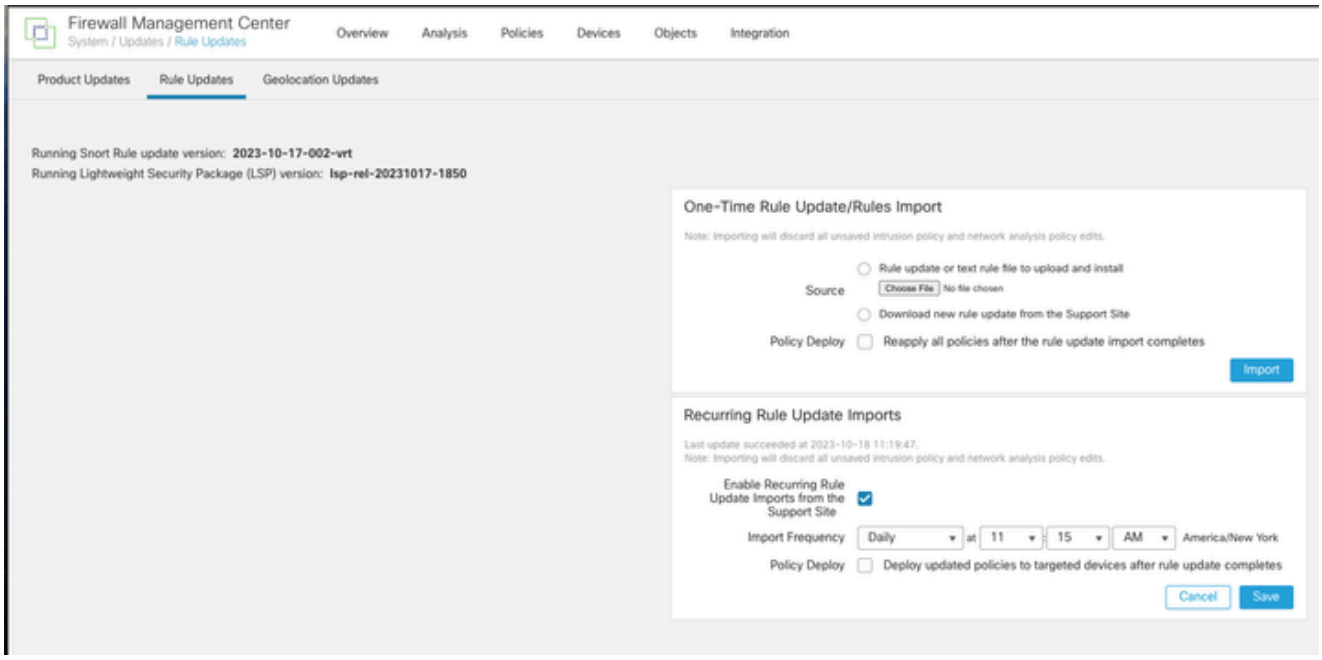
1. Accédez à Device > Updates (View Configuration)

2. Vérifiez la règle d'intrusion et assurez-vous qu'elle est 20231014-1509 ou plus récente



FMC

1. Accédez à Système > Mises à jour > Mises à jour des règles
2. Vérifiez la mise à jour des règles Running Snort et Running Lightweight Security Package (LSP) et assurez-vous qu'ils exécutent le LSP 20231014-1509 ou SRU-2023-10-14-001 ou version ultérieure.



b. Assurez-vous que les règles sont activées dans votre stratégie d'intrusion

Si vos stratégies d'intrusion sont basées sur les stratégies intégrées de Talos (connectivité sur la sécurité, sécurité sur la connectivité, sécurité équilibrée et connectivité), ces règles seront activées et définies pour être supprimées par défaut.

Si vous ne basez pas votre politique sur l'une des politiques intégrées de Talos. Vous devez activer manuellement la définition des actions de règle pour ces règles dans votre stratégie d'intrusion. Pour ce faire, consultez la documentation ci-dessous :

Snort 3 : https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/snort/720/snort3-configuration-guide-v72/tuning-intrusion-policies.html#ID-2237-00000683_snort3

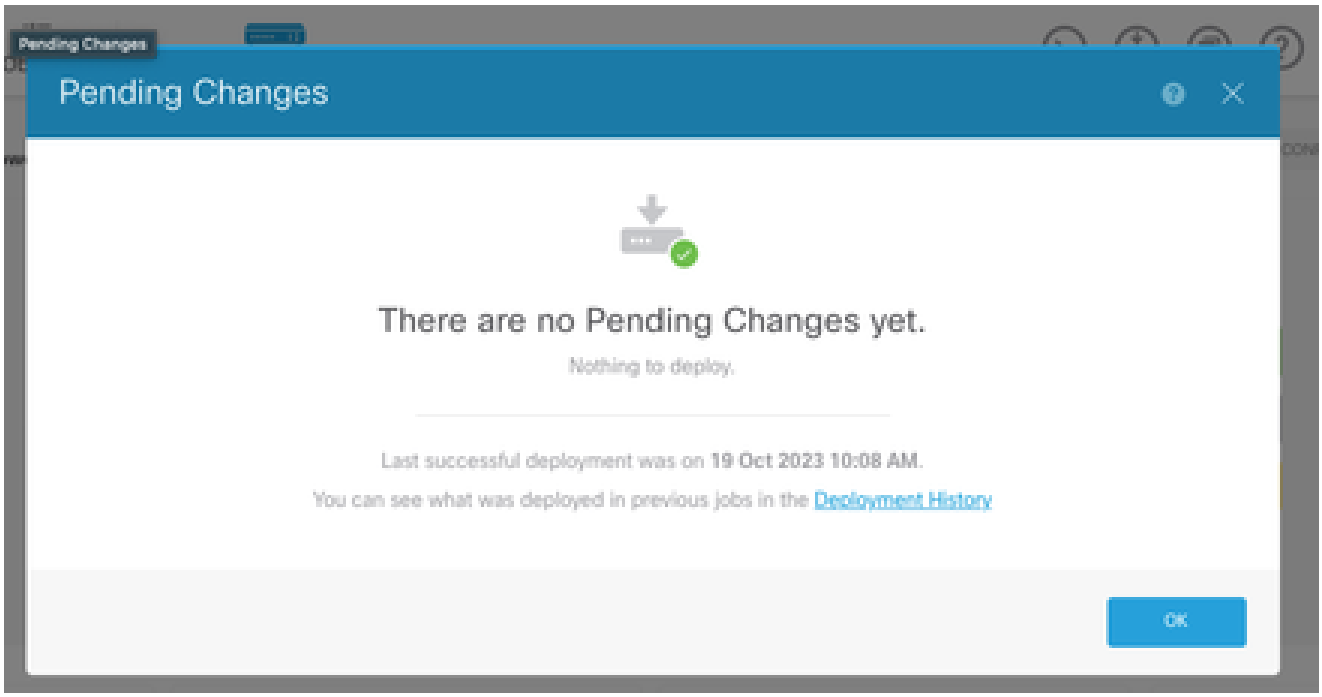
Snort 2 : https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/720/management-center-device-config-72/intrusion-tuning-rules.html#ID-2237-00000683

c. Assurez-vous que vos stratégies IPS ont été déployées sur vos périphériques FTD :

FDM

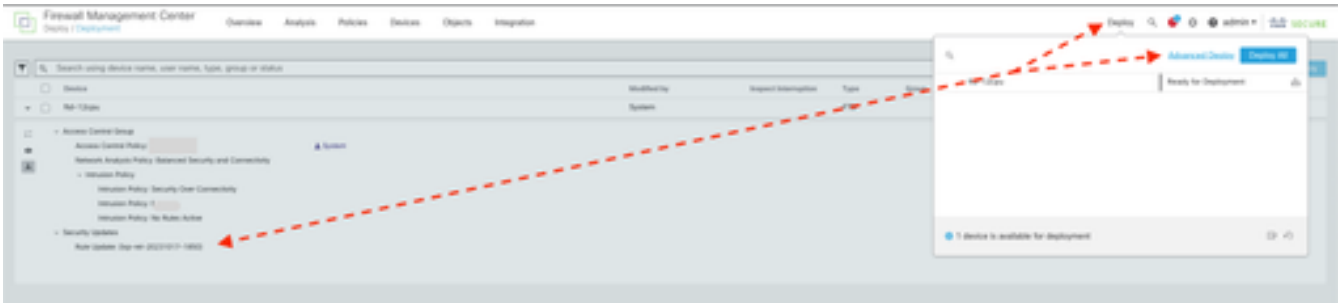


1. Cliquez sur l'icône de déploiement
2. Assurez-vous qu'aucune modification n'est en attente concernant le SRU/LSP



FMC

1. Cliquez sur Déployer > Déploiement avancé
2. S'assurer qu'aucun déploiement en attente n'est associé à SRU/LSP



6. J'ai un CUBE (Cisco Unified Border Element) qui exécute Cisco IOS XE. Puis-je désactiver le serveur http/https ?

La majorité des déploiements CUBE n'utilisent pas le service HTTP/HTTPS fourni avec IOS XE et sa désactivation n'aura aucun impact sur les fonctionnalités. Si vous utilisez la fonctionnalité XMF de liaison de support, vous devrez configurer une liste d'accès et restreindre l'accès au service HTTP pour inclure uniquement les hôtes approuvés (clients CUCM/tiers). Vous pouvez voir un exemple de configuration ici.

7. J'ai un Cisco Unified Communications Manager Express (CME) exécutant Cisco IOS XE. Puis-je désactiver le serveur http/https ?

La solution CME utilise les services HTTP pour l'annuaire des utilisateurs et des services supplémentaires pour les téléphones IP enregistrés. La désactivation du service entraînera l'échec de cette fonctionnalité. Vous devrez configurer une liste de contrôle d'accès et restreindre l'accès au service HTTP pour inclure uniquement le sous-réseau du réseau téléphonique IP. Vous pouvez voir un exemple de configuration ici.

8. Si je désactive le serveur http/https, cela aura-t-il un impact sur ma capacité à gérer mes périphériques avec Cisco DNA Center ?

La désactivation du serveur HTTP/HTTPS n'affectera pas les fonctionnalités de gestion des périphériques ni l'accessibilité des périphériques gérés avec Cisco DNA Center, y compris ceux des environnements SDA (Software-Defined Access). La désactivation du serveur HTTP/HTTPS aura un impact sur la fonctionnalité d'hébergement d'applications et sur toutes les applications tierces utilisées dans l'environnement d'hébergement d'applications de Cisco DNA Center. Ces applications tierces peuvent s'appuyer sur le serveur HTTP/HTTPS pour la communication et les fonctionnalités.

9. La désactivation du serveur HTTP/HTTPS sur le périphérique aura-t-elle un impact sur Smart Licensing ?

En général, Smart Licensing utilise la fonctionnalité Client HTTPS et la désactivation de la fonctionnalité de serveur HTTP(S) n'a donc pas d'impact sur les opérations Smart Licensing. Le seul scénario où la communication de licences Smart serait compromise est lorsque l'application externe CSLU ou SSM On-Prem est utilisée et configurée avec RESTCONF pour récupérer les rapports RUM à partir des périphériques.

10. Un acteur de la menace peut-il exploiter la vulnérabilité et créer un utilisateur local même si AAA est en place ?

Oui, nous pensons qu'un cybercriminel peut exploiter cette vulnérabilité pour créer un utilisateur local, quelle que soit la méthode d'authentification que vous utilisez. Veuillez noter que les informations d'identification seront locales au périphérique exploité et non dans le système AAA.

11. Quelle doit être la réponse « curl » si j'utilise mon routeur comme serveur AC et que la liste de contrôle d'accès HTTP/S est déjà configurée pour bloquer l'IP de l'ordinateur ?

la réponse 'curl' est 403 interdit comme ci-dessous :

bureau (base) ~ % curl http://<ip du périphérique>

<html>

<head><title>403 Interdit</title></head>

<body bgcolor="white">

<h1>403 Interdit</h1>

<hr> nginx

</body>

</html>

12. Où puis-je trouver des informations sur la disponibilité des correctifs logiciels ou des unités de maintenance logicielle (SMU) ?

Pour plus d'informations, consultez la page Software Fix Availability for Cisco IOS XE Software

Web UI Privilege Escalation Vulnerability.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.