Cisco TAC technische veelgestelde vragen voor Cisco IOS XE Software Web UI-kwetsbaarheid voor prioriteitsescalatie - CVE-2023-20198

Inhoud

Inleiding

Dit document geeft de technische veelgestelde vragen van Cisco Technical Assistance Center weer voor de kwetsbaarheid voor escalatie van Cisco IOS XE-software-webinterface. Er zijn aanvullende details beschikbaar in het veiligheidsadvies voor de kwetsbaarheid en in het blog Cisco Talos.

Overzicht

Dit document schetst de implicaties van het uitschakelen van de ip http server of ip http security-server opdrachten en welke andere functies worden beïnvloed door dit te doen. Bovendien, het verstrekt voorbeelden op hoe te om de toegang-lijsten te vormen die in het advies worden geschetst om toegang tot webui te beperken in het geval dat u niet kunt de eigenschappen

volledig onbruikbaar maken.

1. Is mijn product aangetast?

Alleen producten waarop Cisco IOS XE-software met versies 16.x en hoger wordt uitgevoerd, worden beïnvloed. Nexus-producten, ACI, traditionele IOS-apparaten, IOS XR, firewalls (ASA/FTD) en ISE worden niet beïnvloed. In het geval van Identity Services Engine kan het ook andere gevolgen hebben als de http/https-server wordt uitgeschakeld. Zie het gedeelte ISE.

2. Hoe kan ik bepalen of op mijn product Cisco IOS XE wordt uitgevoerd?

Voer de opdracht tonen versie van de opdrachtregel interface (CLI) en u zult het type software als dit zien:

switch #show versie

Cisco IOS XE-software, versie 17.09.03

Cisco IOS-software [Cupertino], C9800-CL-software (C9800-CL-K9_IOSXE), versie 17.9.3, RELEASESOFtware (fc6)

Technische ondersteuning: http://www.cisco.com/techsupport

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

Samengesteld Tue 14-Mar-23 18:12 door mcpre

Cisco IOS-XE-software, Copyright (c) 2005-2023 van Cisco Systems, Inc.

Alle rechten voorbehouden. Bepaalde componenten van Cisco IOS-XE-software zijn gelicentieerd onder de GNU General Public License ("GPL"), versie 2.0. De softwarecode gelicentieerd onder GPL Versie 2.0 is gratis software die geleverd wordt met ABSOLUUT GEEN GARANTIE. U kunt een dergelijke GPL-code opnieuw distribueren en/of wijzigen onder de voorwaarden van GPL versie 2.0. Zie voor meer informatie de documentatie of het "Licentiebericht"-bestand dat bij de IOS-XE-software is meegeleverd, of de toepasselijke URL op de flyer die bij de IOS-XE-software is meegeleverd.

Alleen softwareversies 16.x en hoger worden beïnvloed door deze kwetsbaarheid. Bijvoorbeeld softwareversies die worden beïnvloed zijn:

16.3.5

16.12.4

17.3.5

17.6.1

17.9.4

Voorbeelden van IOS XE-versies die NIET worden beïnvloed:

3.17.4S.

3.11.7E

15.6-1.S4

15.2-7.E7

3. Ik gebruik Identity Services Engine (ISE) om gebruikscases om te leiden en kan de http/https-servers niet uitschakelen. Wat kan ik doen?

Het uitschakelen van ip http server en ip http secure-server zal voorkomen dat gebruik cases zoals de volgende werken:

- Op apparaatsensor gebaseerde profilering
- Houding omleiden en detecteren
- Gastenomleiding
- BYOD Onboarding
- MDM-onboarding

Op IOS-XE-apparaten waarvoor geen toegang tot de webui nodig is, wordt aanbevolen de volgende opdrachten te gebruiken om toegang tot de webui te voorkomen terwijl de ISE-omleidingscases nog steeds zijn toegestaan:

- ip http active-sessie-modules geen
- ip http Secure-Active-Session-modules geen

Als toegang tot de webui nodig is, zoals met de Catalyst 9800 controllers, kan toegang tot de webui worden beperkt met behulp van http access-class ACL's: https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-17/221107-filter-traffic-destin...

http access-class ACL's maken het nog steeds mogelijk om de ISE-omleidingscases te laten functioneren.

4. Ik gebruik de C9800 draadloze LAN-controller (WLC) en kan de http/http servers niet uitschakelen. Wat kan ik doen?

A4. Het uitschakelen van ip http server en ip http secure-server zal de volgende gebruikscases breken:

- Toegang tot de WLC WebUI. Dit geldt wanneer draadloze beheerinterface (WMI) of servicepoort of een andere SVI wordt gebruikt voor toegang tot de WebAdmin GUI.
- De wizard Day 0 Setup zal mislukken.
- Web-Verificatie - Guest Access of WLC Interne pagina, Aangepaste Web-Auth pagina, Lokale Web Verificatie, Centrale Web Verificatie zal ophouden met opnieuw te sturen
- Op een C9800-CL zal de zelfondertekende certificaatgeneratie mislukken
- RESTCONF-toegang
- S3 en Cloudwatch
- IOS app-hosting op draadloze access points

Om deze services te kunnen blijven gebruiken, moet u de volgende stappen uitvoeren:

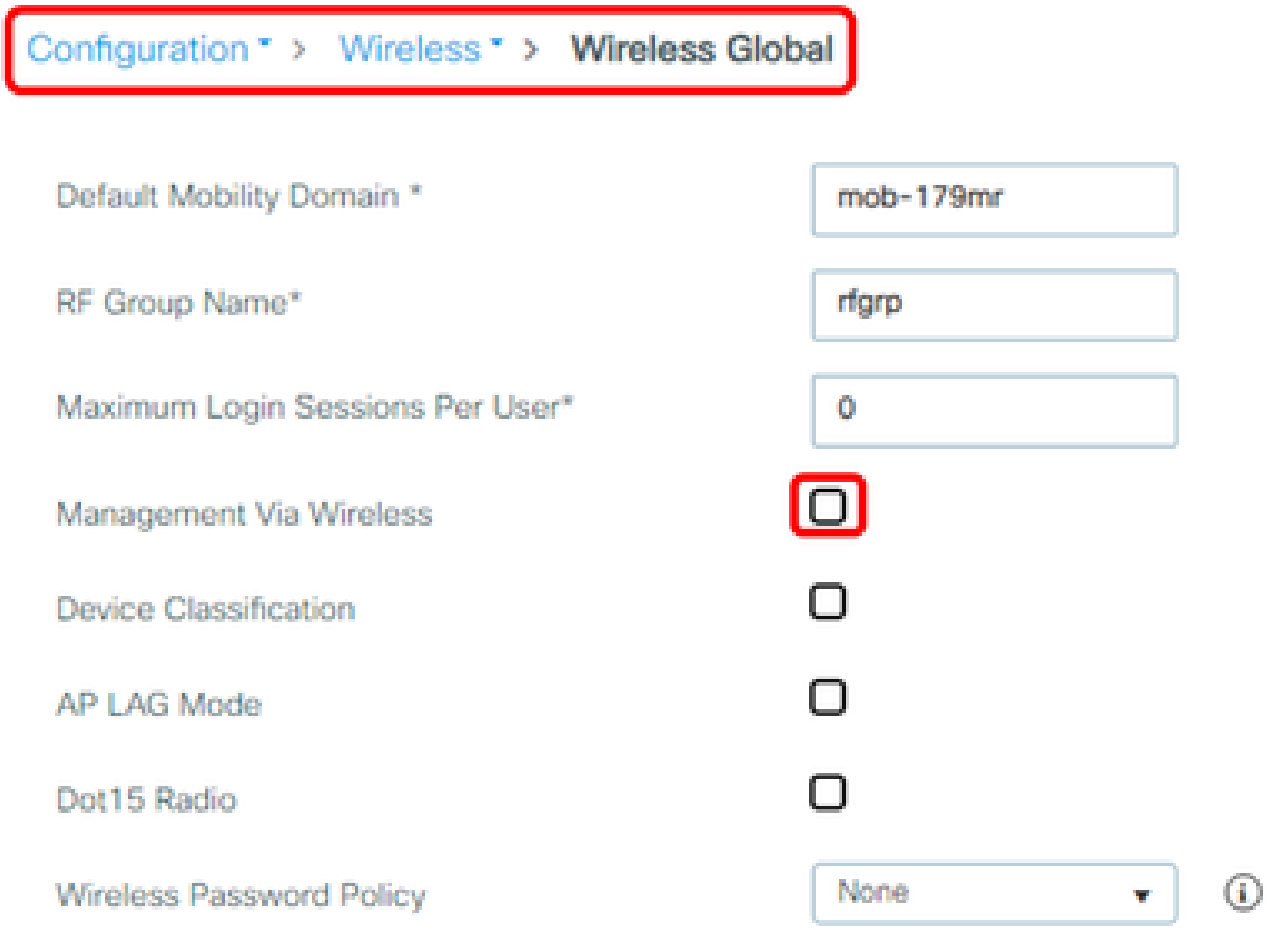
(1) HTTP/HTTPS ingeschakeld houden

(2) Gebruik een ACL om toegang tot C9800 WLC-webserver te beperken, alleen tot vertrouwde subnetten / adressen.
Nadere informatie over het configureren van de toegangslijst is te vinden: 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.

Opmerking:
1. AireOS WLC's zijn niet kwetsbaar
2. Alle vormfactoren van C9800 (C9800-80, C9800-40, C9800-L, C9800-CL), inclusief ingesloten draadloze verbindingen op het AP (EWC-AP) en ingesloten draadloze verbindingen op de Switch (EWC-SW) zijn kwetsbaar
3. HTTP ACL zal alleen toegang tot HTTP-server op de C9800 WLC blokkeren. Het zal niet van invloed zijn op WebAuth Guest Access of het gebruik van de WLC Interne pagina, Aangepaste Web-Auth pagina, Lokale Web Verificatie, of Centrale Web Verificatie
4. HTTP ACL heeft ook geen invloed op CAPWAP Control of Data traffic.
5. Zorg ervoor dat onbetrouwbare netwerken zoals gasten niet zijn toegestaan in de HTTP ACL.

Als u de toegang van uw draadloze clients tot de WebAdmin GUI volledig wilt blokkeren, dient u er optioneel voor te zorgen dat "Beheer via draadloos" is uitgeschakeld.

GUI:



CLI:

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

5. In het veiligheidsadvies wordt vermeld dat er korte regels zijn om deze kwetsbaarheid op te sporen en te blokkeren. Hoe kan ik bevestigen dat deze regels zijn geïnstalleerd en werken aan mijn FTD?

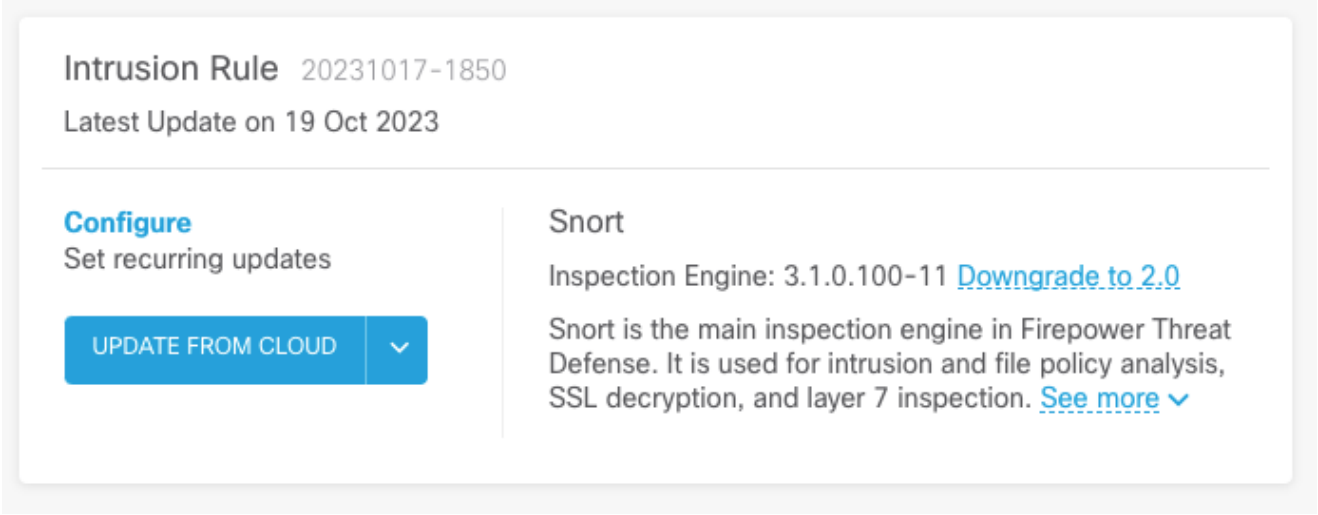
Om er zeker van te zijn dat de Snortregels op uw apparaat zijn geïnstalleerd, controleert u of u LSP 20231014-1509 of SRU-2023-10-14-001 hebt. Controleren of deze is geïnstalleerd, is anders op door FDM en FMC beheerde apparaten:

a. Zorg ervoor dat de regels worden geïnstalleerd:

FDM

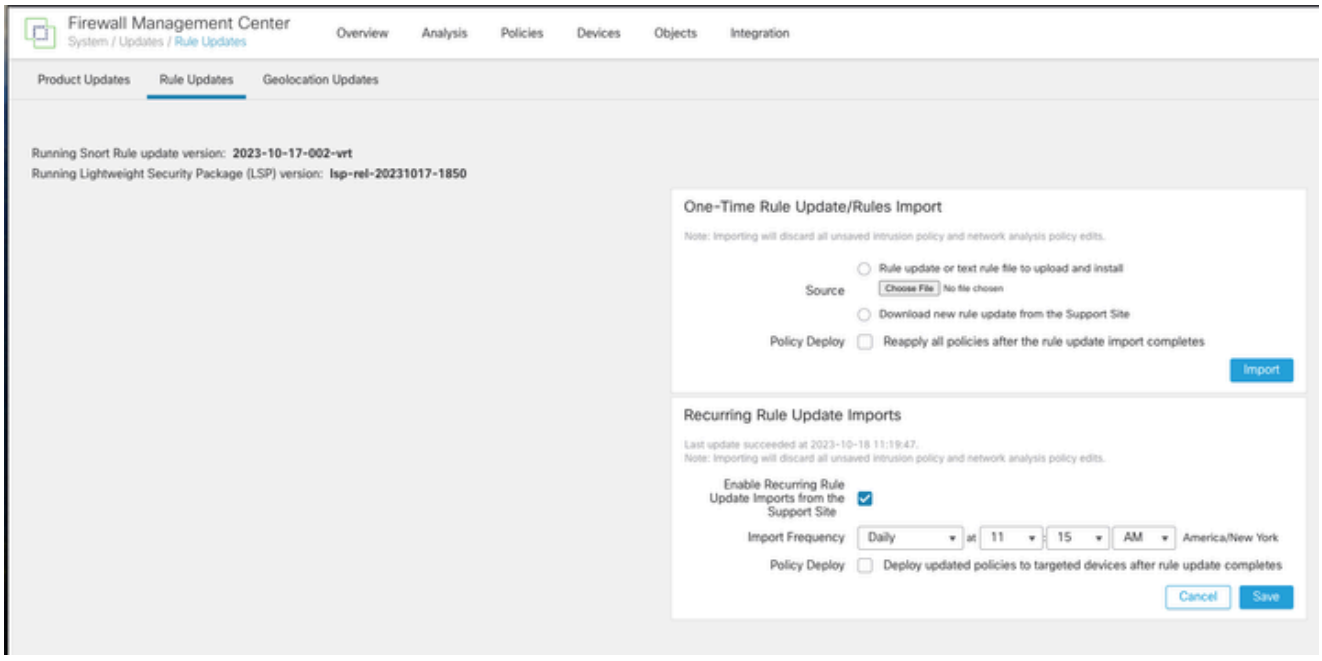
1. Navigeer naar apparaat > Updates (configuratie bekijken)

2. Controleer de inbraakregels en controleer of deze 20231014-1509 of nieuwer zijn



VCC

1. Navigeren naar systeem > updates > regelupdates
2. Controleer of LSP (Running Snort Rule update en Running Lichtgewicht Security Package) (LSP) wordt uitgevoerd met LSP 20231014-1509 of SRU-2023-10-14-001 of hoger.



b. Verzeker de regels die in uw Inbraakbeleid worden toegelaten

Als uw inbraakbeleid is gebaseerd op de ingebouwde beleidslijnen van Talos (connectiviteit over beveiliging, security over connectiviteit, gebalanceerde beveiliging en connectiviteit) zullen deze regels standaard worden ingeschakeld en ingesteld om te dalen.

Als u uw beleid niet baseert op een van de ingebouwde Talos-beleidslijnen. U moet de regelacties handmatig voor deze regels instellen in uw inbraakbeleid. Raadpleeg hiervoor de onderstaande documentatie:

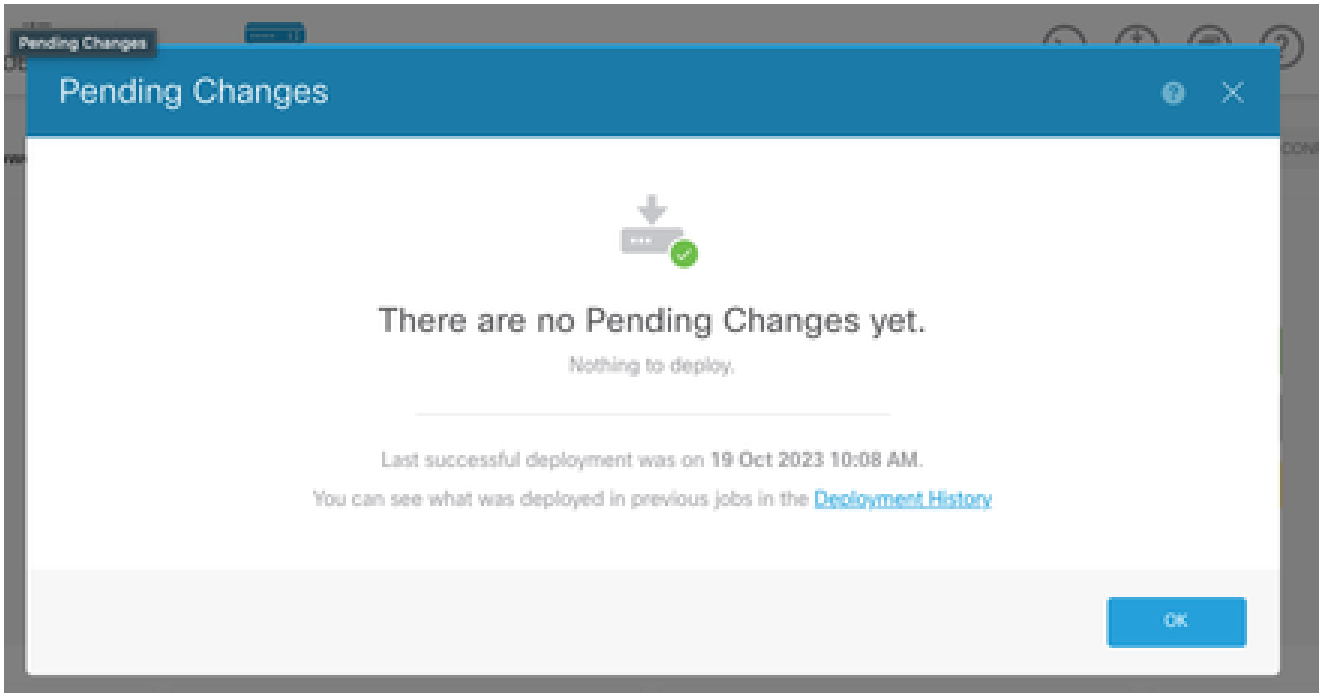
Kleur 3: https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/snort/720/snort3-configuration-guide-v72/tuning-intrusion-policies.html#ID-2237-00000683_snort3

Kleur 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. Zorg ervoor dat uw IPS-beleid is geïmplementeerd op uw FTD-apparaten:

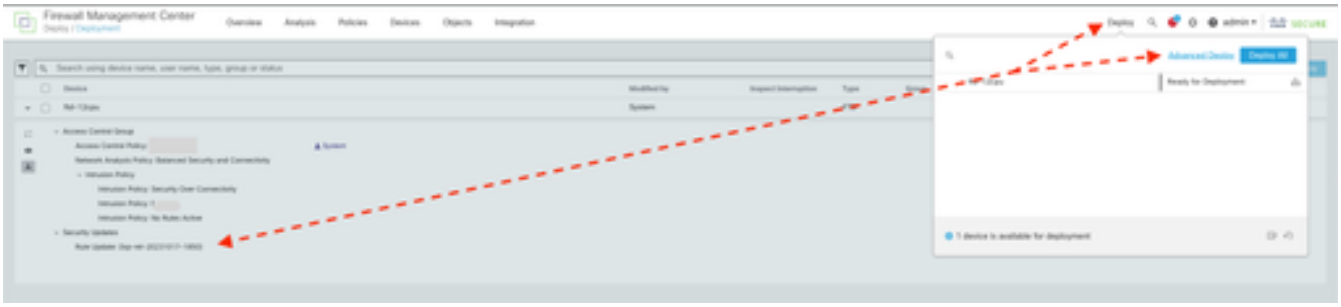
FDM

1. Klik op het implementatiepictogram
2. Zorg ervoor dat er geen wijzigingen in verband met de SRU/LSP in behandeling zijn



VCC

1. Klik op Implementeren > Geavanceerd implementeren
2. Zorg ervoor dat er geen implementaties in behandeling zijn met betrekking tot SRU/LSP



6. Ik heb een Cisco Unified Border Element (CUBE) met Cisco IOS XE. Kan ik http/https server uitschakelen?

De meeste CUBE-implementaties maken geen gebruik van de HTTP/HTTPS-service die met IOS XE is gebundeld en het uitschakelen ervan heeft geen invloed op de functionaliteit. Als u de XMF-gebaseerde media forking functie gebruikt dan moet u een toegangslijst configureren en de toegang tot de HTTP-service beperken om alleen vertrouwde hosts (CUCM/3rd party clients) op te nemen. U kunt hier een configuratievoorbeeld bekijken.

7. Ik heb een Cisco Unified Communications Manager Express (CME) waarop Cisco IOS XE wordt uitgevoerd. Kan ik http/https server uitschakelen?

De CME-oplossing maakt gebruik van HTTP-services naar gebruikersdirectory en extra services naar geregistreerde IP-telefoons. Als u de service uitschakelt, zal deze functionaliteit mislukken. U moet een toegangslijst configureren en de toegang tot de HTTP-service beperken om alleen het IP-telefoonnetwerk te omvatten. U kunt hier een configuratievoorbeeld bekijken.

8. Als ik http/https-server uitschakel, heeft dit gevolgen voor mijn vermogen om mijn apparaten te beheren met Cisco DNA Center?

Het uitschakelen van de HTTP/HTTPS-server heeft geen invloed op de functies voor apparaatbeheer of de bereikbaarheid voor apparaten die worden beheerd met Cisco DNA Center, inclusief apparaten in SDA-omgevingen (Software-Defined Access). Het uitschakelen van de HTTP/HTTPS-server heeft gevolgen voor de functie Application Hosting en voor alle toepassingen van derden die worden gebruikt in de Application Hosting-omgeving van Cisco DNA Center. Deze toepassingen van derden kunnen voor communicatie en functionaliteit vertrouwen op de HTTP/HTTPS-server.

9. Zullen er gevolgen zijn voor Smart Licensing als we HTTP/HTTPS-server uitschakelen op het apparaat?

Over het algemeen maakt Smart Licensing gebruik van de HTTPS-clientfunctionaliteit en heeft het uitschakelen van de HTTP(S)-serverfunctie dus geen invloed op de slimme licentiëring. Het enige scenario waarin de slimme licentiemededeling zou worden belemmerd, is wanneer de externe toepassing CSLU of SSM On-Prem wordt gebruikt en geconfigureerd met RESTCONF om RUM-rapporten van apparaten op te halen.

10. Kan een bedreigingsactor de kwetsbaarheid exploiteren en een lokale gebruiker creëren zelfs als AAA op zijn plaats is?

Ja, wij geloven dat een bedreigingsactor deze kwetsbaarheid kan exploiteren om een lokale gebruiker te creëren ongeacht de authenticatiemethode die u gebruikt. Houd er rekening mee dat de referenties lokaal zijn voor het geëxploiteerde apparaat en niet voor het AAA-systeem.

11. Wat zou de "curl"reactie moeten zijn als ik mijn router als server van CA gebruik en HTTP/S ACL reeds wordt gevormd om machine IP te blokkeren?

'krul'-reactie is 403 verboden zoals hieronder:

(basis) desktop ~ % curl http://<device ip>

<html>

<head><title>403 verboden</title></head>

<Body bgcolor="white">

<h1>403 verboden</h1>

<h> Nginx

</body>

</html>

12. Waar vind ik de informatie over software fix of Software Maintenance Units (SMU's) beschikbaarheid?

Ga naar Software Fix Availability voor Cisco IOS XE Software Web UI Privilege Escalation Vulnerability pagina voor meer informatie.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.