Cisco TAC Technische FAQs für Cisco IOS XE Software Web UI Privilege Eskalation Vulnerability - CVE-2023-20198

Inhalt

Einleitung

Dieses Dokument stellt die technischen FAQs des Cisco Technical Assistance Center zur Eskalationsschwachstelle für die Web-UI der Cisco IOS XE-Software dar. Weitere Informationen finden Sie in der Sicherheitsempfehlung zur Schwachstelle und im Cisco Talos Blog.

Überblick

In diesem Dokument werden die Auswirkungen einer Deaktivierung der Befehle ip http server oder ip http secure-server sowie die Auswirkungen auf andere Funktionen erläutert. Darüber hinaus enthält es Beispiele für die Konfiguration der in der Ankündigung beschriebenen Zugriffslisten, um den Zugriff auf die Web-UI zu beschränken, falls Sie die Funktionen nicht vollständig deaktivieren

können.

1. Ist mein Produkt betroffen?

Betroffen sind nur Produkte mit Cisco IOS XE Software der Versionen 16.x und höher. Nexus-Produkte, ACI, traditionelle IOS-Geräte, IOS XR, Firewalls (ASA/FTD), ISE sind davon nicht betroffen. Im Fall der Identity Services Engine kann die Deaktivierung des http/https-Servers weitere Auswirkungen haben. Weitere Informationen finden Sie im Abschnitt zur ISE.

2. Wie kann ich feststellen, ob auf meinem Produkt Cisco IOS XE ausgeführt wird?

Führen Sie den Befehl show version (Version anzeigen) über die Befehlszeilenschnittstelle (CLI) aus, und Sie sehen den Softwaretyp wie folgt:

switch#show-Version

Cisco IOS XE Software, Version 17.09.03

Cisco IOS Software [Cupertino], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.9.3, VERSION SOFTWARE (fc6)

Technischer Support: http://www.cisco.com/techsupport

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

Zusammengestellt Di 14-Mär-23 18:12 von mcpre

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

Alle Rechte vorbehalten. Bestimmte Komponenten der Cisco IOS-XE-Software sind unter der GNU General Public License (GPL) Version 2.0 lizenziert. Der unter der GPL Version 2.0 lizenzierte Software-Code ist freie Software, die ABSOLUT KEINE GARANTIE bietet. Sie können diesen GPL-Code unter den Bedingungen der GPL Version 2.0 weiterverteilen und/oder ändern. Weitere Informationen finden Sie in der Dokumentation oder in der Datei mit den Lizenzhinweisen zur IOS-XE Software oder unter der entsprechenden URL auf dem Flyer zur IOS-XE Software.

Nur die Softwareversionen 16.x und höher sind von dieser Sicherheitslücke betroffen. Betroffene Softwarebeispiele sind:

16.3.5

16.12.4

17.3.5

17.6.1

17.9.4

Beispiele für IOS XE-Versionen, die NICHT betroffen sind:

3,17 S

3,11,7E

15.6-1.S4

15.2-7.E7

3. Ich verwende die Identity Services Engine (ISE) für die Umleitung von Anwendungsfällen und kann die HTTP-/HTTPS-Server nicht deaktivieren. Was kann ich tun?

Durch das Deaktivieren von ip http server und ip http secure-server lassen sich Anwendungsfälle wie die folgenden vermeiden:

- Geräteabhängige Profilierung
- Statusumleitung und Erkennung
- Gastumleitung
- BYOD-Integration
- MDM-Integration

Für IOS-XE-Geräte, die keinen Zugriff auf die Webui benötigen, wird empfohlen, die folgenden Befehle zu verwenden, um den Zugriff auf die Webui zu verhindern und gleichzeitig die ISE-Weiterleitung von Anwendungsfällen zuzulassen:

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

Wenn der Zugriff auf die Web-UI erforderlich ist, z. B. mit den Catalyst 9800 Controllern, kann der Zugriff auf die Web-UI mithilfe von http-Zugriffsklassen-ACLs eingeschränkt werden: https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-17/221107-filter-traffic-destin...

Die HTTP-Zugriffsklassen-ACLs ermöglichen weiterhin die ISE-Umleitung von Anwendungsfällen, um zu funktionieren.

4. Ich verwende den C9800 Wireless LAN Controller (WLC) und kann die http/http-Server nicht deaktivieren. Was kann ich tun?

Antwort 4: Die Deaktivierung von ip http server und ip http secure-server führt zu einer Unterbrechung der folgenden Anwendungsfälle:

- Zugriff auf die WLC-Webbenutzeroberfläche. Dies gilt unabhängig davon, ob die Wireless-Verwaltungsschnittstelle (WMI), der Service-Port oder eine andere SVI für den Zugriff auf die WebAdmin-GUI verwendet wird.
- Der Einrichtungsassistent von Tag 0 schlägt fehl.
- Web-Authentifizierung - Gastzugriff, unabhängig davon, ob interne Seite des WLC, benutzerdefinierte Web-Auth-Seite, lokale Web-Authentifizierung oder zentrale Web-Authentifizierung nicht mehr umgeleitet werden
- Auf einem C9800-CL schlägt die Erstellung des selbstsignierten Zertifikats fehl.
- RESTCONF-Zugriff
- S3 und CloudWatch
- IOX-App-Hosting auf Wireless Access Points

Um diese Services weiterhin nutzen zu können, müssen Sie wie folgt vorgehen:

(1) HTTP/HTTPS aktiviert lassen

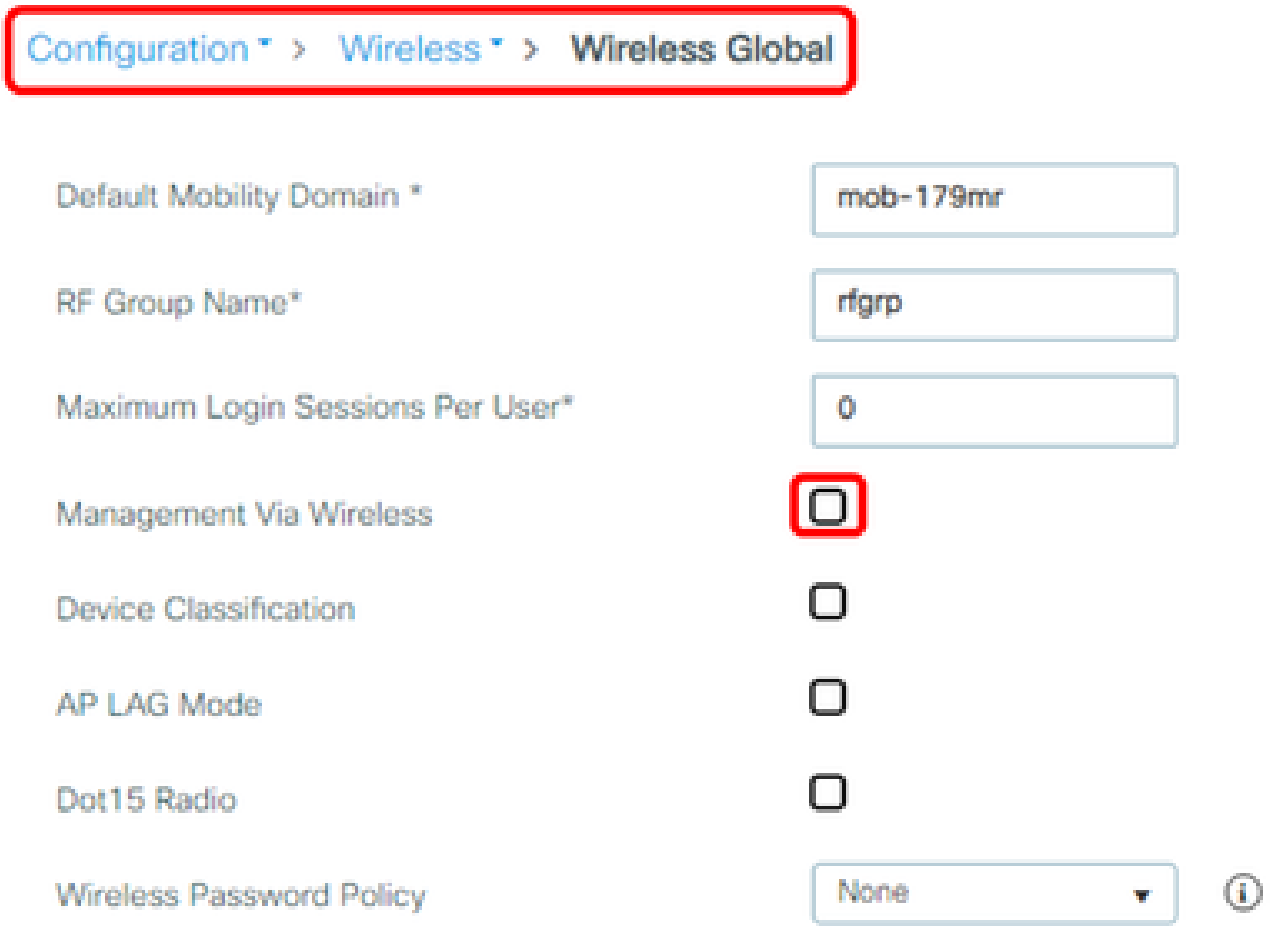
(2) Verwenden Sie eine ACL, um den Zugriff auf den C9800 WLC-Webserver zu beschränken, und zwar nur auf vertrauenswürdige Subnetze/Adressen.
Details zur Konfiguration der Zugriffsliste finden Sie unter:
https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-17/221107-filter-traffic-destined-to-cisco-ios-xe.html

---

Anmerkung:
1. AireOS WLCs sind nicht anfällig.
2. Alle Formfaktoren von C9800 (C9800-80, C9800-40, C9800-L, C9800-CL) einschließlich Embedded Wireless on AP (EWC-AP) und Embedded Wireless on Switch (EWC-SW) sind gefährdet.
3. Die HTTP-ACL blockiert nur den Zugriff auf den HTTP-Server des C9800 WLC. WebAuth-Gastzugriff wird nicht beeinträchtigt, unabhängig davon, ob die interne Seite des WLC, die benutzerdefinierte Web-Auth-Seite, die lokale Web-Authentifizierung oder die zentrale Web-Authentifizierung verwendet wird.
4. Die HTTP-ACL hat auch keine Auswirkungen auf CAPWAP-Steuerung oder Datenverkehr.
5. Stellen Sie sicher, dass nicht vertrauenswürdige Netzwerke wie guest in der HTTP-ACL nicht zugelassen sind.

Wenn Sie Ihren Wireless-Clients den Zugriff auf die WebAdmin-GUI vollständig verweigern möchten, stellen Sie optional sicher, dass "Management Via Wireless" deaktiviert ist.

GUI:



CLI:

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

5. In der Sicherheitsempfehlung wird erwähnt, dass es Snort-Regeln gibt, um diese Schwachstelle zu erkennen und zu blockieren. Wie kann ich bestätigen, dass diese Regeln auf meinem FTD installiert sind und funktionieren?

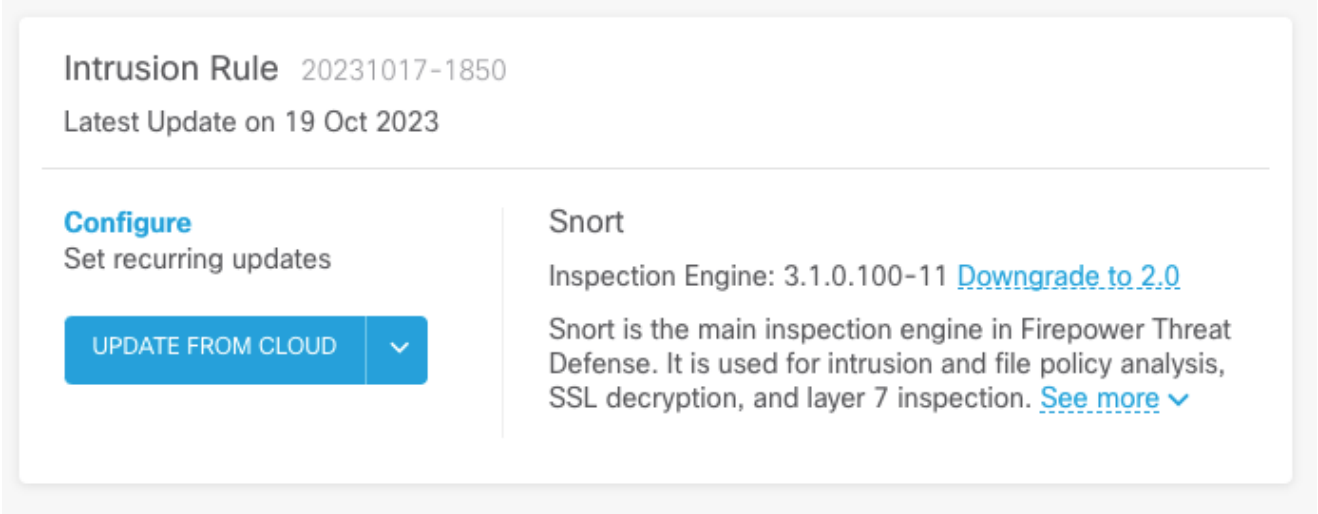
Um sicherzustellen, dass die Snort-Regeln auf Ihrem Gerät installiert sind, stellen Sie sicher, dass entweder LSP 20231014-1509 oder SRU-2023-10-14-001 installiert ist. Überprüfen, ob diese auf FDM- und FMC-verwalteten Geräten anders installiert ist:

a. Stellen Sie sicher, dass Regeln installiert sind:

FDM

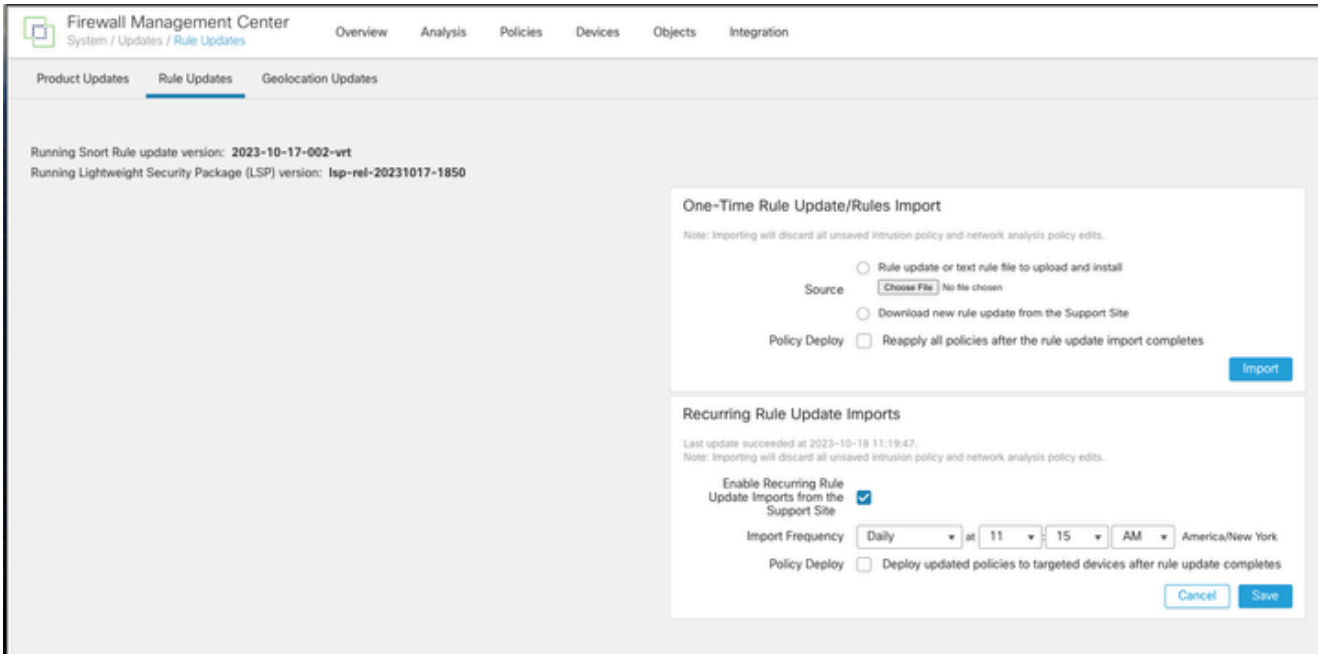
1. Navigieren Sie zu Gerät > Updates (Konfiguration anzeigen).

2. Überprüfen Sie die Angriffsregel, und stellen Sie sicher, dass sie 20231014-1509 oder neuer ist.



FMC

1. Navigieren Sie zu System > Updates > Regelaktualisierungen.
2. Aktivieren Sie Run Snort Rule Update und Running Lightweight Security Package (LSP), und stellen Sie sicher, dass LSP 20231014-1509 oder SRU-2023-10-14-001 oder höher ausgeführt wird.



b. Stellen Sie sicher, dass die Regeln in Ihrer Intrusion Policy aktiviert sind.

Wenn Ihre Angriffsrichtlinien auf den integrierten Richtlinien von Talos basieren (Konnektivität über Sicherheit, Sicherheit über Konnektivität, ausgewogene Sicherheit und Konnektivität), werden diese Regeln aktiviert und standardmäßig deaktiviert.

Wenn Sie Ihre Richtlinie nicht auf einer der integrierten Richtlinien von Talos basieren. Sie müssen die Regelaktionen für diese Regeln in Ihrer Richtlinie für Sicherheitsrisiken manuell

aktivieren. Lesen Sie dazu bitte die Dokumentation unten:

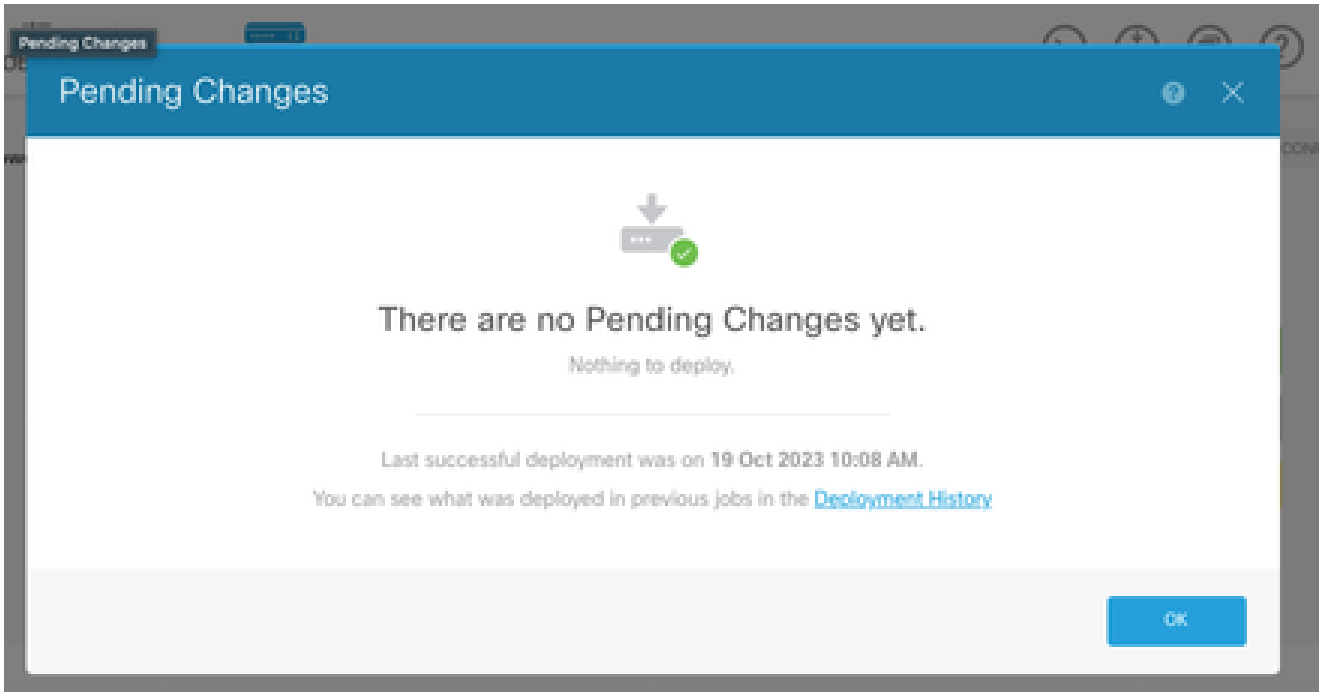
Snort 3: https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/snort/720/snort3-configuration-guide-v72/tuning-intrusion-policies.html#ID-2237-00000683_snort3

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. Stellen Sie sicher, dass IPS-Richtlinien auf Ihren FTD-Geräten bereitgestellt wurden:

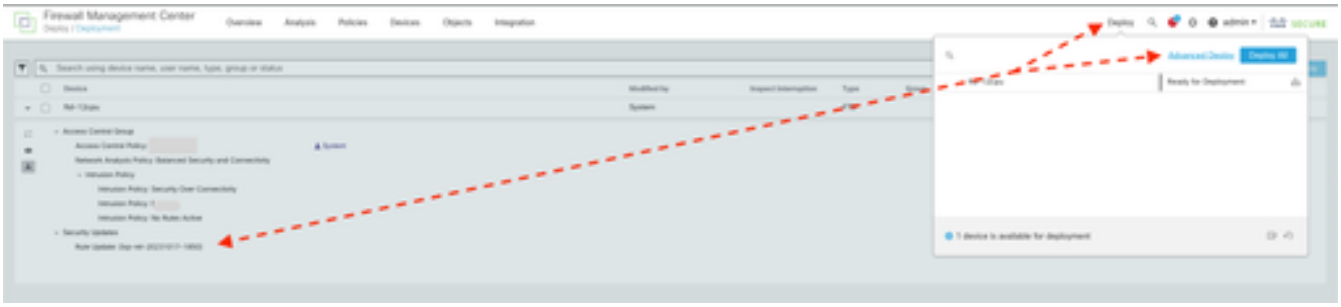
FDM

1. Klicken Sie auf das Bereitstellungssymbol
2. Stellen Sie sicher, dass keine ausstehenden Änderungen am SRU/LSP vorgenommen werden.



FMC

1. Klicken Sie auf Bereitstellen > Erweiterte Bereitstellung
2. Stellen Sie sicher, dass keine ausstehenden Bereitstellungen für SRU/LSP vorliegen.



6. Ich verwende ein Cisco Unified Border Element (CUBE), auf dem Cisco IOS XE ausgeführt wird. Kann ich den http/https-Server deaktivieren?

Die Mehrheit der CUBE-Bereitstellungen verwendet nicht den HTTP/HTTPS-Service im Paket mit IOS XE. Eine Deaktivierung wirkt sich daher nicht auf die Funktionalität aus. Wenn Sie die XMF-basierte Medien-Forking-Funktion verwenden, müssen Sie eine Zugriffsliste konfigurieren und den Zugriff auf den HTTP-Dienst auf vertrauenswürdige Hosts (CUCM-/Drittanbieter-Clients) beschränken. Ein Konfigurationsbeispiel finden Sie hier.

7. Ich habe einen Cisco Unified Communications Manager Express (CME) mit Cisco IOS XE. Kann ich den http/https-Server deaktivieren?

Die CME-Lösung nutzt HTTP-Dienste für das Benutzerverzeichnis und zusätzliche Dienste für registrierte IP-Telefone. Wenn Sie den Dienst deaktivieren, schlägt diese Funktion fehl. Sie müssen eine Zugriffsliste konfigurieren und den Zugriff auf den HTTP-Dienst einschränken, sodass er nur das Subnetz des IP-Telefonnetzes enthält. Ein Konfigurationsbeispiel finden Sie hier.

8. Wenn ich den http/https-Server deaktivieren würde, würde sich dies auf meine Fähigkeit auswirken, meine Geräte mit Cisco DNA Center zu verwalten?

Die Deaktivierung des HTTP-/HTTPS-Servers hat keine Auswirkungen auf die Geräteverwaltungsfunktionen oder die Erreichbarkeit der Geräte, die mit Cisco DNA Center verwaltet werden, einschließlich der Geräte in SDA-Umgebungen (Software-Defined Access). Die Deaktivierung des HTTP-/HTTPS-Servers wirkt sich auf die Anwendungs-Hosting-Funktion und alle Anwendungen von Drittanbietern aus, die in der Anwendungs-Hosting-Umgebung von Cisco DNA Center verwendet werden. Diese Drittanbieteranwendungen nutzen möglicherweise den

HTTP-/HTTPS-Server für Kommunikation und Funktionalität.

9. Wird Smart Licensing beeinträchtigt, wenn wir den HTTP/HTTPS-Server auf dem Gerät deaktivieren?

Im Allgemeinen verwendet Smart Licensing die HTTPS-Client-Funktion, sodass sich die Deaktivierung der HTTP(S)-Serverfunktion nicht auf die Smart Licensing-Vorgänge auswirkt. Das einzige Szenario, in dem die Smart Licensing-Kommunikation beeinträchtigt wäre, ist, wenn die externe CSLU-Anwendung oder SSM On-Prem verwendet und mit RESTCONF konfiguriert wird, um RUM-Berichte von Geräten abzurufen.

10. Kann ein Angreifer die Schwachstelle ausnutzen und einen lokalen Benutzer erstellen, selbst wenn AAA vorhanden ist?

Ja, wir glauben, dass ein Angreifer diese Schwachstelle ausnutzen kann, um einen lokalen Benutzer zu erstellen, unabhängig von der Authentifizierungsmethode, die Sie verwenden. Beachten Sie, dass die Anmeldeinformationen für das ausgebeutete Gerät lokal sind und nicht im AAA-System.

11. Was sollte die "Curl"-Antwort sein, wenn ich meinen Router als CA-Server verwende und die HTTP/S-ACL bereits so konfiguriert ist, dass sie die Computer-IP blockiert?

'curl' Antwort ist 403 verboten wie unten:

(Basis) Desktop ~ % curl http://<Geräte-IP>

<html>

<head><title>403 Verboten</title></head>

<body bgcolor="white">

<h1>403 Verboten</h1>

<hr> nginx

</body>

</html>

12. Wo finde ich Informationen zur Verfügbarkeit von Software Fix oder Software Maintenance Units (SMUs)?

Weitere Informationen finden Sie auf der Seite Software Fix Availability for Cisco IOS XE Software

Web UI Privilege Escalation Vulnerability (Software-Fehlerbehebungsverfügbarkeit für Cisco IOS XE-Software über die Webbenutzeroberfläche).

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.