Domande frequenti tecniche su Cisco TAC per il software Cisco IOS XE Vulnerabilità dell'escalation dei privilegi dell'interfaccia utente Web - CVE-2023-20198

Sommario

Introduzione

Questo documento rappresenta le domande frequenti (FAQ) tecniche del Cisco Technical Assistance Center per la vulnerabilità dell'escalation dei privilegi dell'interfaccia utente Web del software Cisco IOS XE. Ulteriori dettagli sono disponibili nel Security Advisory for the vulnerability e nel blog Cisco Talos.

Panoramica

In questo documento vengono descritte le implicazioni della disabilitazione dei comandi ip http server o ip http secure-server e le altre funzionalità interessate. Fornisce inoltre esempi su come

configurare gli elenchi degli accessi descritti nell'advisory per limitare l'accesso al webui nel caso in cui non sia possibile disabilitare completamente le funzionalità.

1. Il prodotto è interessato?

Il problema riguarda solo i prodotti con software Cisco IOS XE versione 16.x e successive. Nexus Products, ACI, Traditional IOS devices, IOS XR, Firewall (ASA/FTD), ISE non sono interessati. Nel caso di Identity Services Engine, la disabilitazione del server http/https potrebbe comportare altre conseguenze. Per informazioni dettagliate, consultare la sezione ISE.

2. Come posso determinare se il mio prodotto usa Cisco IOS XE?

Eseguire il comando show version dall'interfaccia della riga di comando (CLI) per verificare il tipo di software:

switch#show versione

Software Cisco IOS XE, versione 17.09.03

Software Cisco IOS [Cupertino], software C9800-CL (C9800-CL-K9_IOSXE), versione 17.9.3, SOFTWARE RELEASE (fc6)

Supporto tecnico: http://www.cisco.com/techsupport

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

Data compilazione 14-mar-23 18:12 da mcpre

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

Tutti i diritti sono riservati. Alcuni componenti del software Cisco IOS-XE sono concessi in licenza in base alla GNU General Public License ("GPL") versione 2.0. Il codice software concesso in licenza in base alla versione 2.0 di GPL è un software gratuito che non prevede ALCUNA GARANZIA. È possibile ridistribuire e/o modificare tale codice GPL in base ai termini della versione GPL 2.0. Per ulteriori informazioni, vedere la documentazione o il file delle "Notifiche di licenza" che accompagna il software IOS-XE o l'URL applicabile fornito sul volantino che accompagna il software IOS-XE.

Questa vulnerabilità interessa solo il software versione 16.x e successive. Di seguito sono riportati alcuni esempi di versioni software interessate:

16.3.5

16.12.4

17.3.5

17.6.1

17.9.4

Esempi di versioni di IOS XE NON interessate:

3.17.4 S

3.11.7E

15,6-1,S4

15,2-7,E7

3. Sto utilizzando Identity Services Engine (ISE) per reindirizzare gli scenari di utilizzo e non posso disabilitare i server http/https. Cosa posso fare?

La disattivazione di ip http server e ip http secure-server impedirà il funzionamento di casi di utilizzo come i seguenti:

- Profilatura basata su sensore dispositivo
- Reindirizzamento e rilevamento della postura
- Reindirizzamento guest
- Caricamento BYOD
- Caricamento MDM

Sui dispositivi IOS-XE che non richiedono l'accesso a webui, si consiglia di utilizzare i seguenti comandi per impedire l'accesso a webui e allo stesso tempo permettere ai casi di utilizzo con reindirizzamento ISE:

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

Se è necessario accedere a webui, ad esempio con i controller Catalyst 9800, l'accesso a webui può essere limitato usando gli ACL http con classe di accesso: https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-17/221107-filter-traffic-destin...

Gli ACL http con classe di accesso consentono ancora il funzionamento dei case di utilizzo per il reindirizzamento ISE.

4. Sto utilizzando C9800 Wireless LAN Controller (WLC) e non posso disabilitare i server http/http. Cosa posso fare?

R4. La disabilitazione del server http ip e del server sicuro http ip interromperà i seguenti casi di utilizzo:

- Accesso a WLC WebUI. Ciò è valido sia che si utilizzi l'interfaccia di gestione wireless (WMI) o la porta del servizio o qualsiasi altra SVI per accedere all'interfaccia GUI di WebAdmin.
- L'installazione guidata del giorno 0 non riuscirà.
- Autenticazione Web - Accesso guest: la pagina interna WLC, la pagina personalizzata di autenticazione Web, l'autenticazione Web locale e l'autenticazione Web centrale non verranno più reindirizzate
- In un C9800-CL, la generazione di certificati autofirmati non riuscirà
- Accesso RESTCONF
- S3 e Cloudwatch
- Hosting di applicazioni IOX su punti di accesso wireless

Per continuare a utilizzare questi servizi, è necessario effettuare le seguenti operazioni:

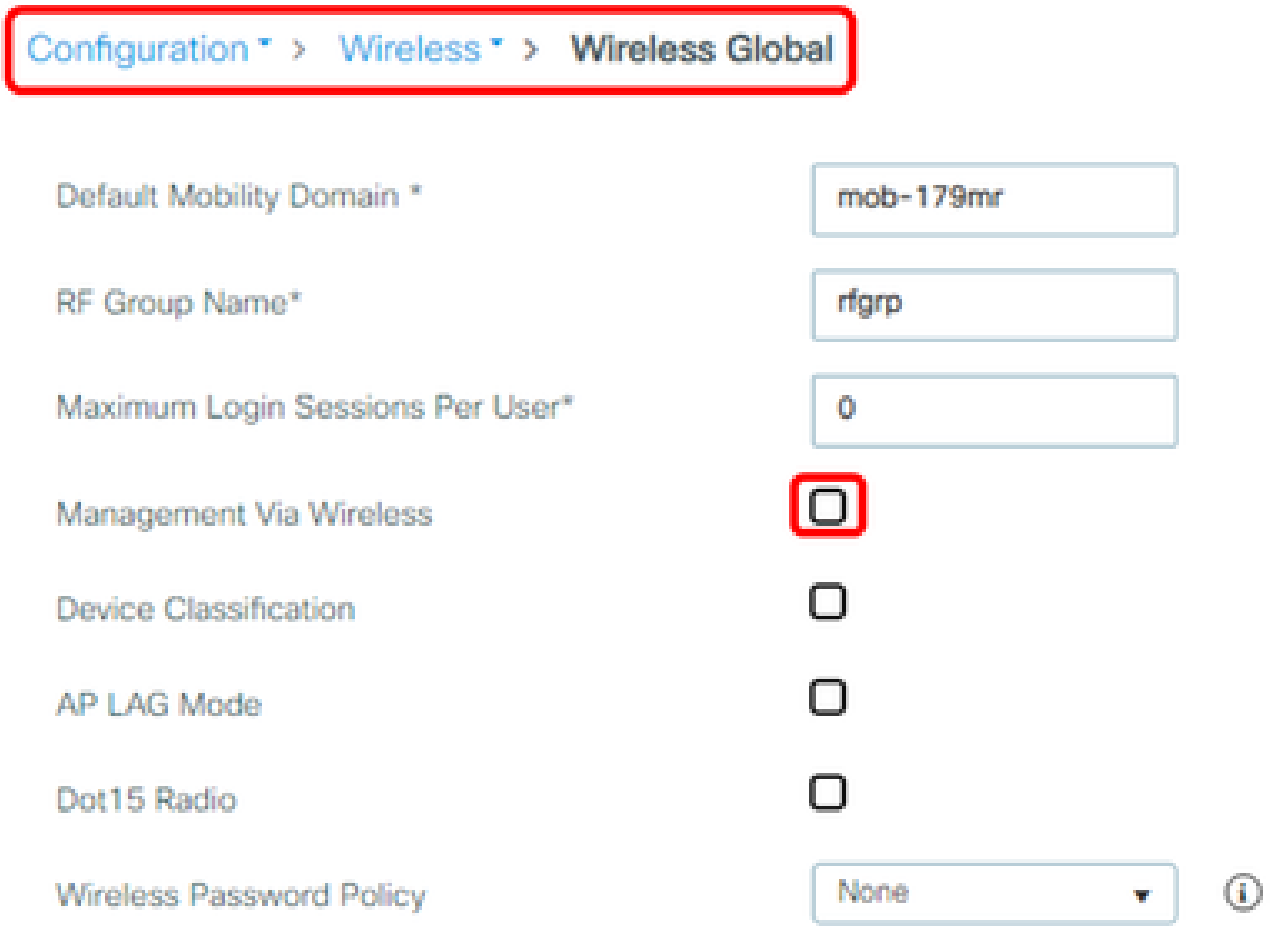
(1) Mantieni HTTP/HTTPS abilitato

(2) Usare un ACL per limitare l'accesso al server Web WLC C9800, solo a subnet/indirizzi attendibili.
Per ulteriori informazioni sulla configurazione dell'elenco degli accessi, consultare: 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.

Nota:
1. I WLC di AireOS non sono vulnerabili
2. Tutti i fattori di forma di C9800 (C9800-80, C9800-40, C9800-L, C9800-CL), tra cui Embedded Wireless on AP (EWC-AP) e Embedded Wireless on Switch (EWC-SW) sono vulnerabili
3. L'ACL HTTP bloccherà l'accesso al server HTTP solo sul WLC del C9800. Non avrà alcun impatto sull'accesso guest WebAuth se si utilizza la pagina interna del WLC, la pagina personalizzata di autenticazione Web, l'autenticazione Web locale o l'autenticazione Web centrale
4. L'ACL HTTP non ha inoltre alcun impatto sul controllo CAPWAP o sul traffico dei dati.
5. Verificare che le reti non attendibili, ad esempio guest, non siano consentite nell'ACL HTTP.

Facoltativamente, se si desidera bloccare completamente l'accesso dei client wireless all'interfaccia utente di WebAdmin, accertarsi che "Gestione tramite wireless" sia disabilitata.

GUI:



CLI:

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

5. Nell'advisory della sicurezza si menziona che ci sono regole snort per rilevare e bloccare questa vulnerabilità. Come posso verificare che queste regole siano installate e funzionino sul mio FTD?

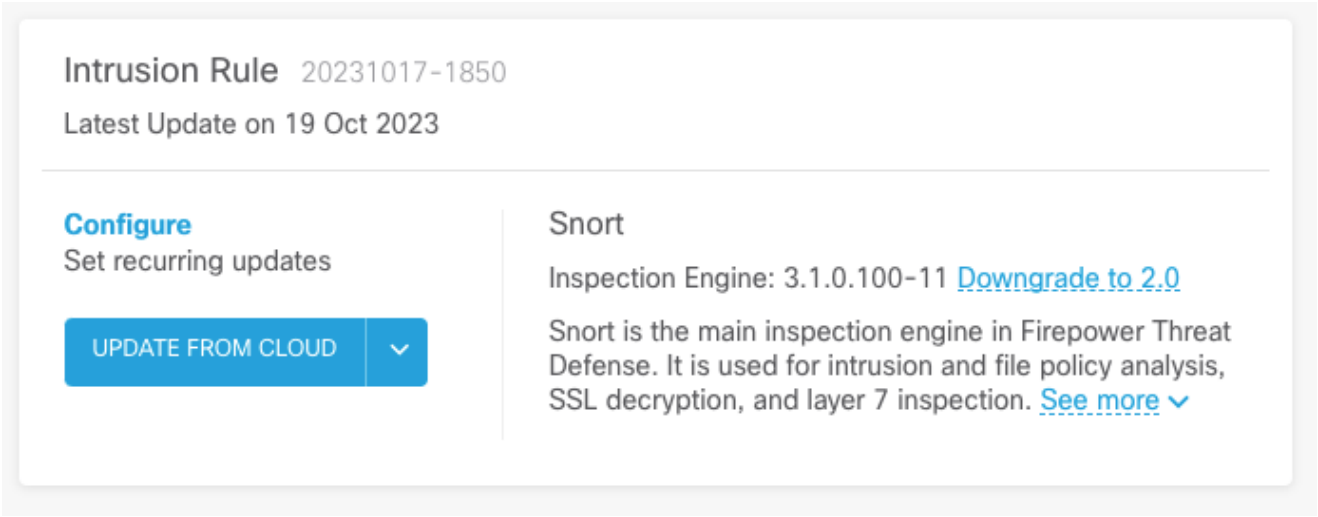
Per accertarsi che le regole di ronzatura siano installate sul dispositivo, verificare di disporre di LSP 20231014-1509 o SRU-2023-10-14-001. Controllo per verificare se l'installazione è diversa nei dispositivi gestiti da FDM e FMC:

a. Verificare che le regole siano installate:

FDM

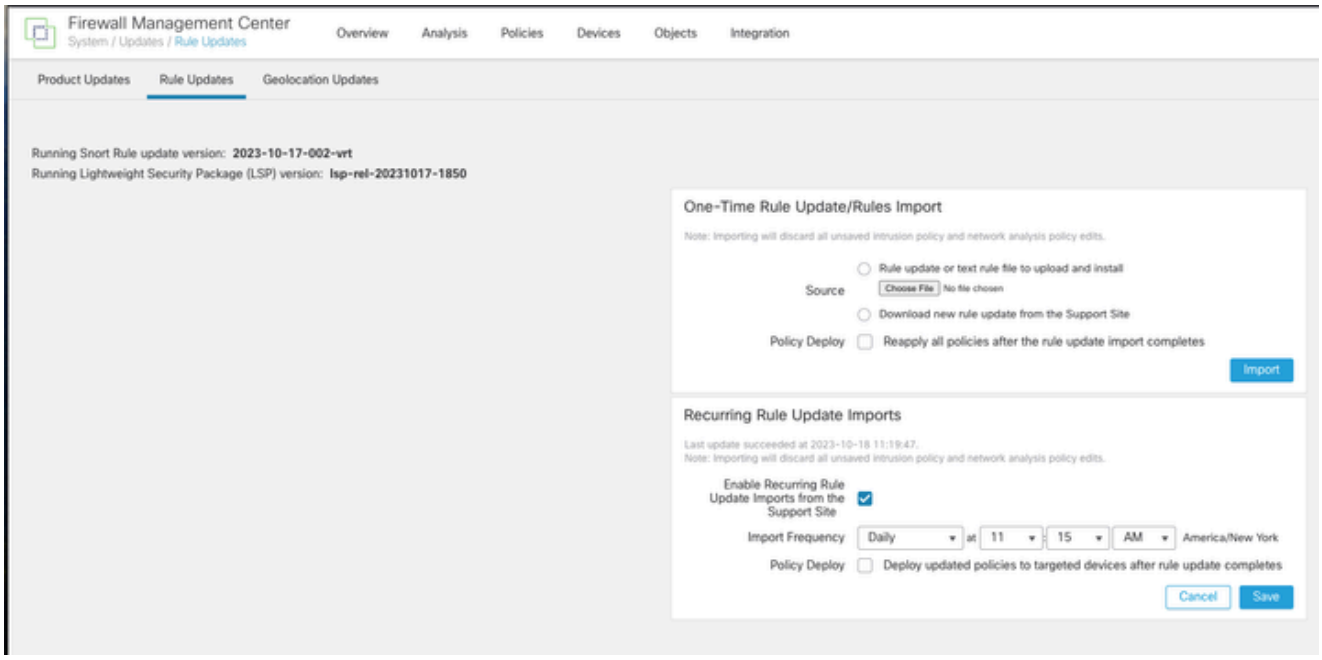
1. Selezionare Periferica > Aggiornamenti (Visualizza configurazione)

2. Controllare la regola per le intrusioni e verificare che sia 20231014-1509 o successiva



CCP

1. Selezionare Sistema > Aggiornamenti > Aggiornamenti regole
2. Verificare che siano in esecuzione l'aggiornamento delle regole di snort e che sia in esecuzione un Lightweight Security Package (LSP) e accertarsi che utilizzino LSP 20231014-1509 o SRU-2023-10-14-001 o versione successiva.



b. Assicurarsi che le regole siano abilitate nella politica sulle intrusioni

Se i criteri per le intrusioni sono basati sui criteri incorporati di Talos (connettività su protezione, protezione su connettività, protezione bilanciata e connettività), queste regole verranno abilitate e impostate per l'eliminazione per impostazione predefinita.

Se non stai basando la tua politica su una delle politiche integrate di Talos. È necessario abilitare l'impostazione manuale delle azioni delle regole per queste regole nei criteri per le intrusioni. A tale scopo, consultare la documentazione riportata di seguito:

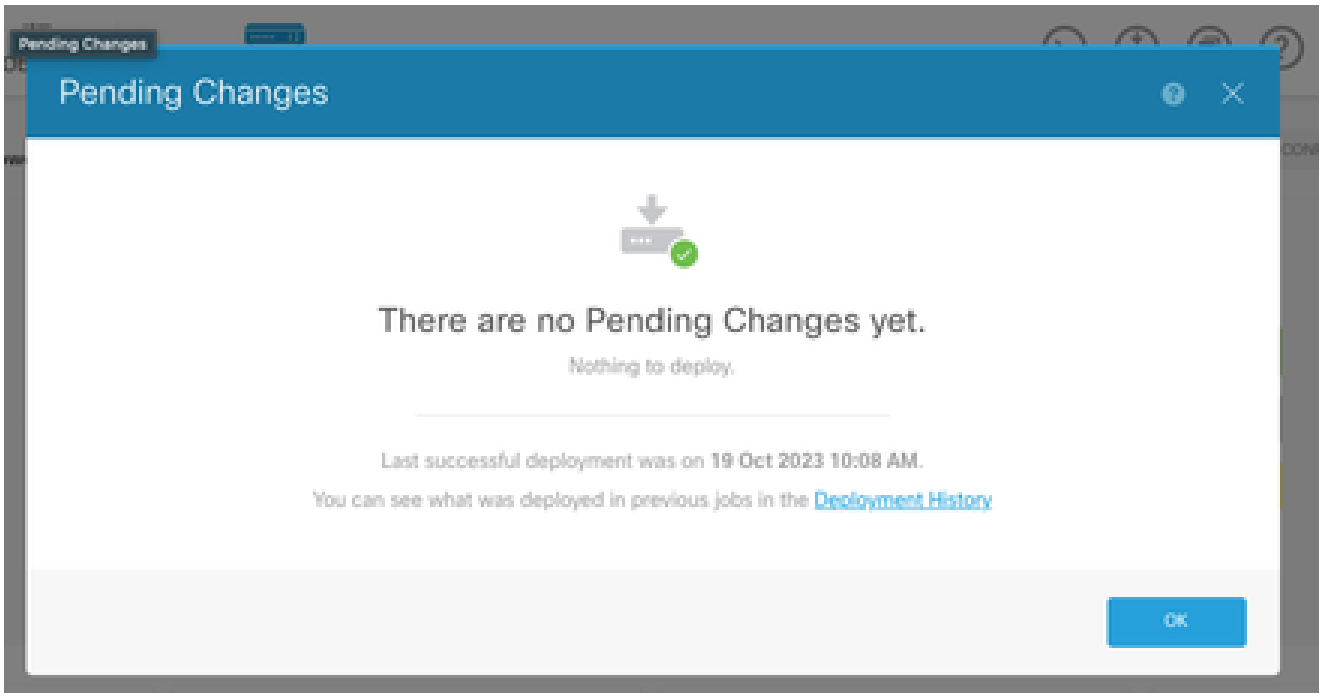
Snort 3 https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/snort/720/snort3-configuration-guide-v72/tuning-intrusion-policies.html#ID-2237-00000683_snort3

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. Verificare che i criteri IPS siano stati distribuiti ai dispositivi FTD:

FDM

1. Fare clic sull'icona di distribuzione
2. Verificare che non vi siano modifiche in sospeso correlate all'unità SRU/LSP



CCP

1. Fare clic su Distribuisci > Distribuzione avanzata

2. Verificare che non vi siano implementazioni in sospeso correlate all'unità SRU/LSP

6. Si dispone di un Cisco Unified Border Element (CUBE) con Cisco IOS XE. È possibile disabilitare il server http/https?

La maggior parte delle distribuzioni CUBE non utilizza il servizio HTTP/HTTPS fornito con IOS XE e la sua disattivazione non influirà sulla funzionalità. Se si utilizza la funzione di forking dei supporti basata su XMF, sarà necessario configurare un elenco degli accessi e limitare l'accesso al servizio HTTP in modo da includere solo gli host attendibili (client CUCM/di terze parti). Qui è possibile visualizzare un esempio di configurazione.

7. Si dispone di un Cisco Unified Communications Manager Express (CME) con Cisco IOS XE. È possibile disabilitare il server http/https?

La soluzione CME utilizza i servizi HTTP per le directory utente e i servizi aggiuntivi per i telefoni IP registrati. Se si disabilita il servizio, questa funzionalità non sarà disponibile. È necessario configurare un elenco degli accessi e limitare l'accesso al servizio HTTP in modo da includere solo la subnet della rete telefonica IP. Qui è possibile visualizzare un esempio di configurazione.

8. La disabilitazione del server http/https influisce sulla possibilità di gestire i dispositivi con Cisco DNA Center?

La disattivazione del server HTTP/HTTPS non influisce sulle funzionalità di gestione dei dispositivi né sulla raggiungibilità per i dispositivi gestiti con Cisco DNA Center, inclusi quelli in ambienti SDA (Software-Defined Access). La disabilitazione del server HTTP/HTTPS avrà un impatto sulla funzionalità di hosting delle applicazioni e su tutte le applicazioni di terze parti utilizzate nell'ambiente di hosting delle applicazioni di Cisco DNA Center. Queste applicazioni di terze parti possono fare affidamento sul server HTTP/HTTPS per la comunicazione e la funzionalità.

9. La disabilitazione del server HTTP/HTTPS sul dispositivo avrà un impatto su Smart Licensing?

In generale, Smart Licensing utilizza la funzionalità Client HTTPS e pertanto la disattivazione della funzionalità server HTTP(S) non ha alcun impatto sulle operazioni di Smart Licensing. L'unico scenario in cui la comunicazione di Smart Licensing risulterebbe compromessa è quando l'applicazione esterna CSLU o SSM in locale viene utilizzata e configurata con RESTCONF per recuperare i report RUM dai dispositivi.

10. È possibile sfruttare la vulnerabilità e creare un utente locale anche se è presente il server AAA?

Sì, riteniamo che un soggetto pericoloso possa sfruttare questa vulnerabilità per creare un utente locale indipendentemente dal metodo di autenticazione utilizzato. Le credenziali saranno locali per il dispositivo utilizzato e non per il sistema AAA.

11. Quale dovrebbe essere la risposta 'curl' se si utilizza il router come server CA e l'ACL HTTP/S è già configurato per bloccare l'IP del computer?

la risposta 'curl' è 403 vietata come indicato di seguito:

(base) desktop ~ % curl http://<ip dispositivo>

<html>

<head><title>403 Vietato</title></head>

<body bgcolor="white">

<h1>403 Non consentito</h1>

<hr> ginx

</body>

</html>

12. Dove è possibile trovare le informazioni sulla disponibilità di aggiornamenti software o unità di manutenzione software (SMU)?

Per ulteriori informazioni, visitare la pagina Disponibilità della correzione software per il software Cisco IOS XE, Escalation Vulnerabilità dell'interfaccia utente Web.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).