Cisco TAC Technical FAQs for Cisco IOS XE Software Web UI Privilege Escalation Vulnerability - CVE-2023-20198

Contents

Introduction

This document represents the Cisco Technical Assistance Center's Technical FAQ for the Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. Additional details are available in the security advisory for the vulnerability and the Cisco Talos blog.

Overview

This document outlines the implications of disabling the ***ip http server*** or ***ip http secure-server*** commands and what other functionalities are affected by doing so. Additionally, it provides examples on how to configure the access-lists outlined in the advisory to limit access to the webui in the event you are unable to completely disable the features.

1. Is my product affected?

Only products running Cisco IOS XE Software with versions 16.x and above are affected. Nexus Products,

ACI, Traditional IOS devices, IOS XR, Firewalls (ASA/FTD), ISE are not affected. In the case of Identity Services Engine, there might be other implications of disabling the http/https server. Please see the ISE section.

2. How can I determine if my product is running Cisco IOS XE?

Execute the command show version from the command line interface (CLI) and you will see the type of software like this:

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, RELEASE SOFTWARE (fc6)

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

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

Compiled Tue 14-Mar-23 18:12 by mcpre

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

All rights reserved. Certain components of Cisco IOS-XE software are licensed under the GNU General Public License ("GPL") Version 2.0. The software code licensed under GPL Version 2.0 is free software that comes with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such GPL code under the terms of GPL Version 2.0. For more details, see the documentation or "License Notice" file accompanying the IOS-XE software, or the applicable URL provided on the flyer accompanying the IOS-XE software.

Only software versions 16.x and greater are affected by this vulnerability. Example software versions which are affected are:

16.3.5

16.12.4

17.3.5

17.6.1

17.9.4

Examples of IOS XE versions which are NOT affected:

3.17.4S

3.11.7E

15.6-1.S4

15.2-7.E7

3. I am using Identity Services Engine (ISE) redirect use cases

and can't disable the http/https servers. What can I do?

Disabling ip http server and ip http secure-server will prevent use cases like the following from working:

- Device Sensor based Profiling
- Posture Redirect and Discovery
- Guest Redirect
- BYOD Onboarding
- MDM Onboarding

On IOS-XE devices that don't require access to the webui, it is recommended to use the following commands to prevent access to the webui while still allowing the ISE redirect use cases:

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

If access to the webui is needed, such as with the Catalyst 9800 controllers, access to the webui can be restricted by using http access-class ACLs: https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-17/221107-filter-traffic-destin...

http access-class ACLs still allow for the ISE redirect use cases to function.

4. I am using C9800 Wireless LAN Controller (WLC) and cannot disable the http/http servers. What can I do?

A4. Disabling ip http server and ip http secure-server will break the following use cases:
- Access to the WLC WebUI. This is true whether Wireless Management Interface (WMI) or Service Port or any other SVI is being used to access the WebAdmin GUI.
- Day 0 Setup wizard will fail.
- Web-Authentication - Guest Access whether WLC Internal page, Custom Web-Auth page, Local Web Authentication, Central Web Authentication will stop getting redirected
- On a C9800-CL, Self-Signed Certificate generation will fail
- RESTCONF access
- S3 and Cloudwatch
- IOX App-hosting on Wireless Access Points

In order to continue using these services you will need to do the following steps:

(1) Keep HTTP/HTTPS enabled

(2) Use an ACL to limit access to C9800 WLC web server, only to trusted subnets / addresses. Details on configuring the access-list can be found: 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.

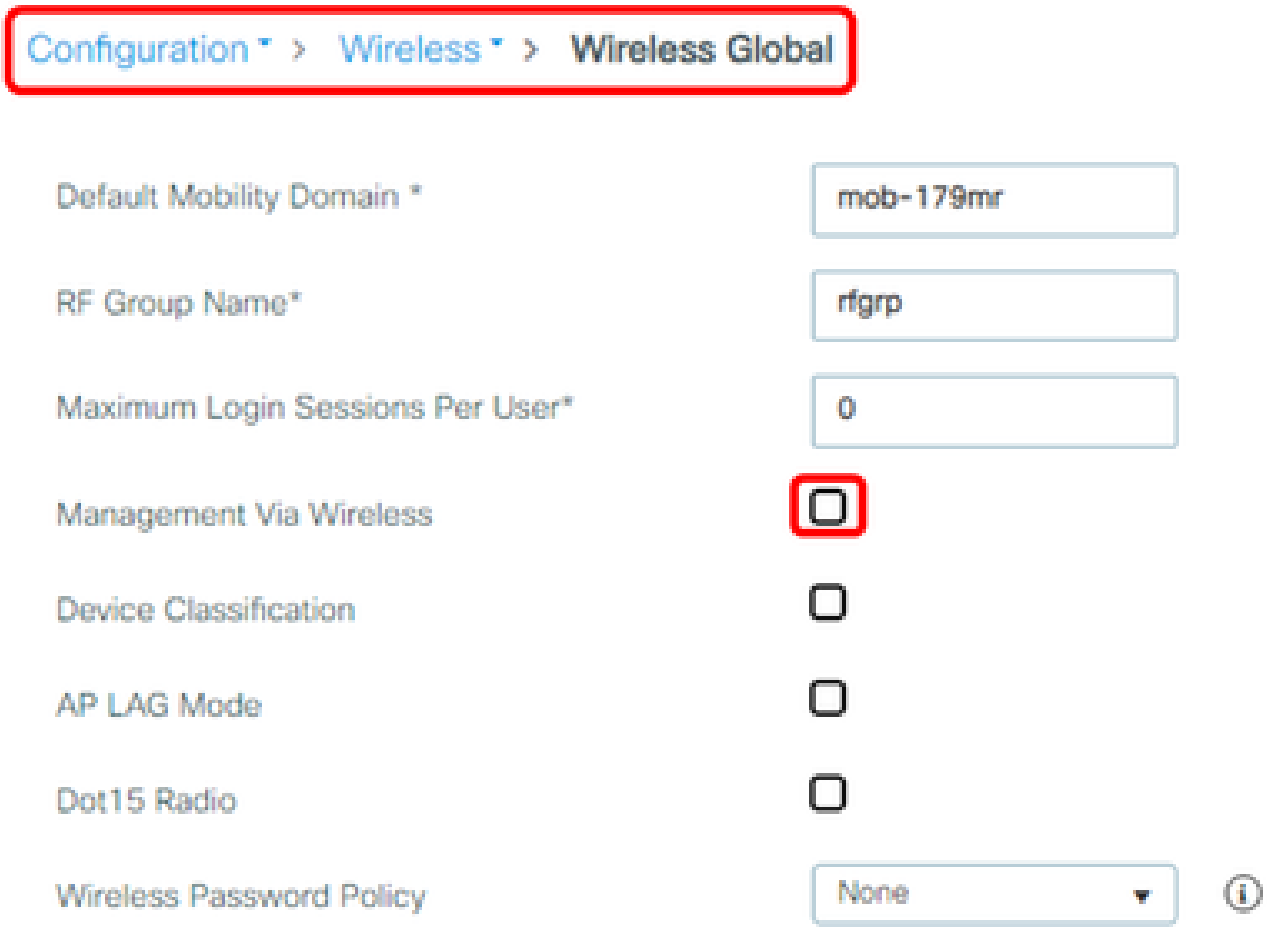
Note:
1. AireOS WLCs are not vulnerable
2. All form factors of C9800 (C9800-80, C9800-40, C9800-L, C9800-CL) including Embedded Wireless on AP (EWC-AP) and Embedded Wireless on Switch (EWC-SW) are vulnerable
3. The HTTP ACL will only block access to HTTP Server on the C9800 WLC. It will not impact WebAuth Guest Access whether using the WLC Internal page, Custom Web-Auth page, Local Web

---

Authentication, or Central Web Authentication
4. The HTTP ACL also has no impact on CAPWAP Control or Data traffic.
5. Ensure untrusted networks like guest are not permitted in the HTTP ACL.

Optionally, if you want to completely block your wireless clients from accessing the WebAdmin GUI, then make sure "Management Via Wireless" is disabled.

GUI:



CLI:

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

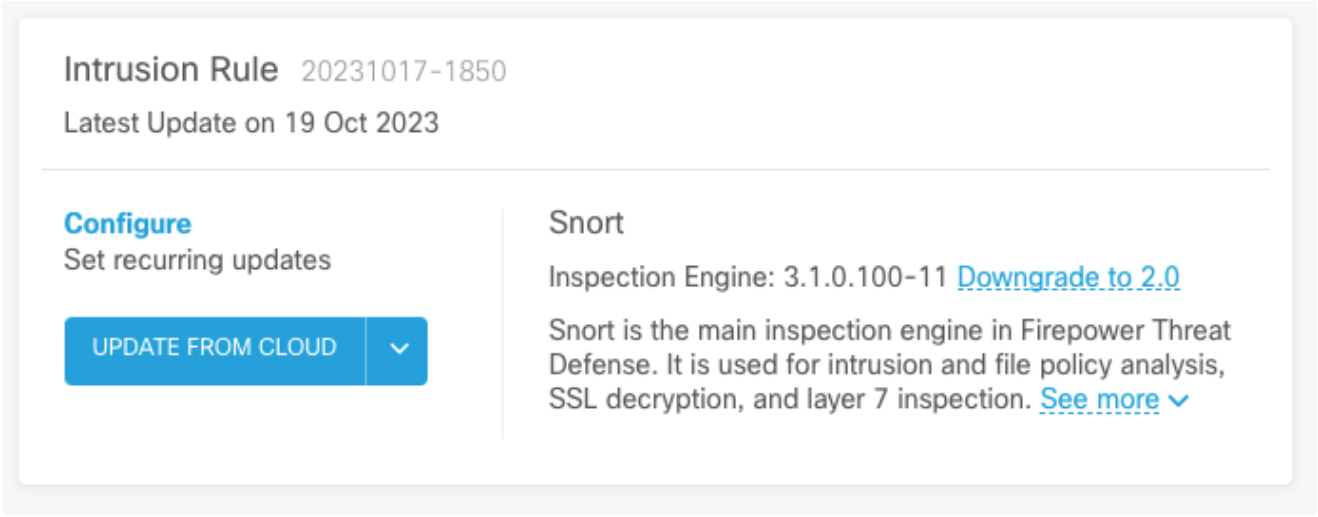
5. In the security advisory it mentions there are snort rules to detect and block this vulnerability. How do I confirm that these rules are installed and working on my FTD?

To ensure that the Snort rules are installed on your device, check to ensure that you have either LSP 20231014-1509 or SRU-2023-10-14-001. Checking whether this is installed is different on FDM and FMC managed devices:

a. Ensure rules are installed:

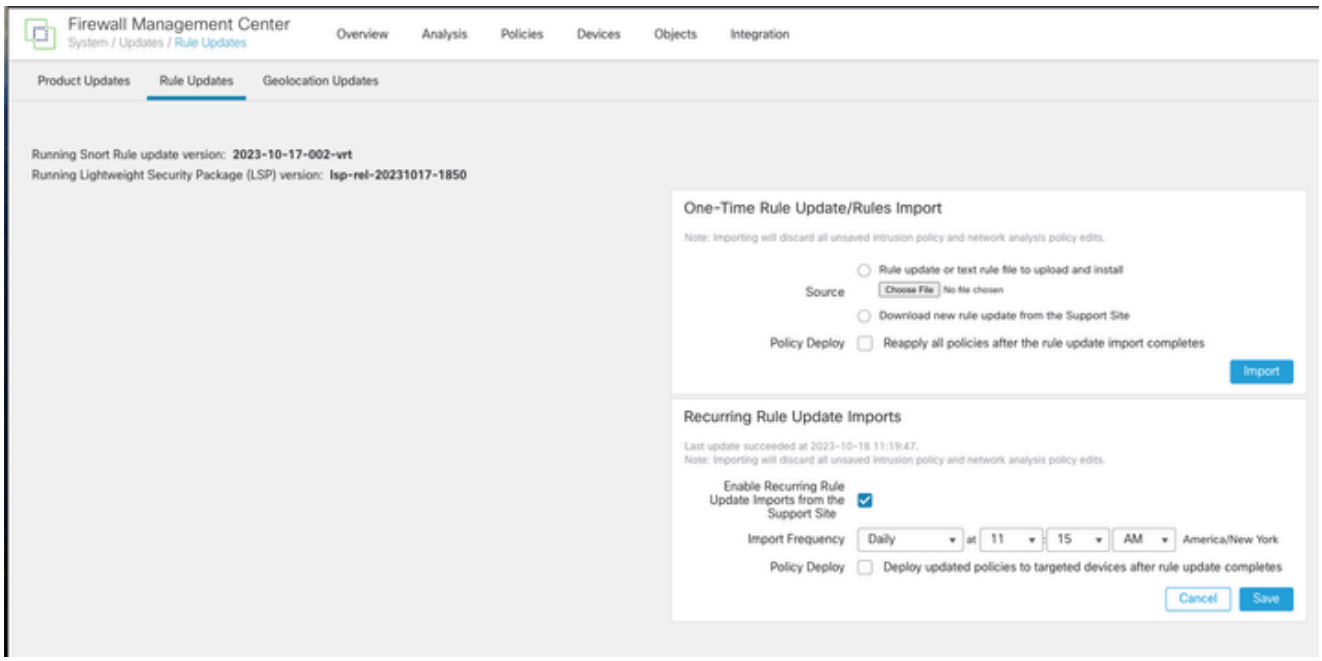
FDM

1. Navigate to Device > Updates (View Configuration)
2. Check Intrusion Rule and ensure that it is **20231014-1509** or newer



FMC

1. Navigate to System > Updates > Rule Updates
2. Check Running Snort Rule update and Running Lightweight Security Package (LSP) and ensure they are running LSP 20231014-1509 or SRU-2023-10-14-001 or higher.



b. Ensure the rules enabled in your Intrusion Policy

If your Intrusion Policies are based off of the Talos built-in policies (connectivity over security, security over connectivity, balanced security and connectivity) these rules will be enabled and set to drop by default.

If you are not basing your policy on one of the Talos Built-in policies. You will need to enable set the rule actions manually for these rules in your Intrusion Policy. To do so please review the documentation below:

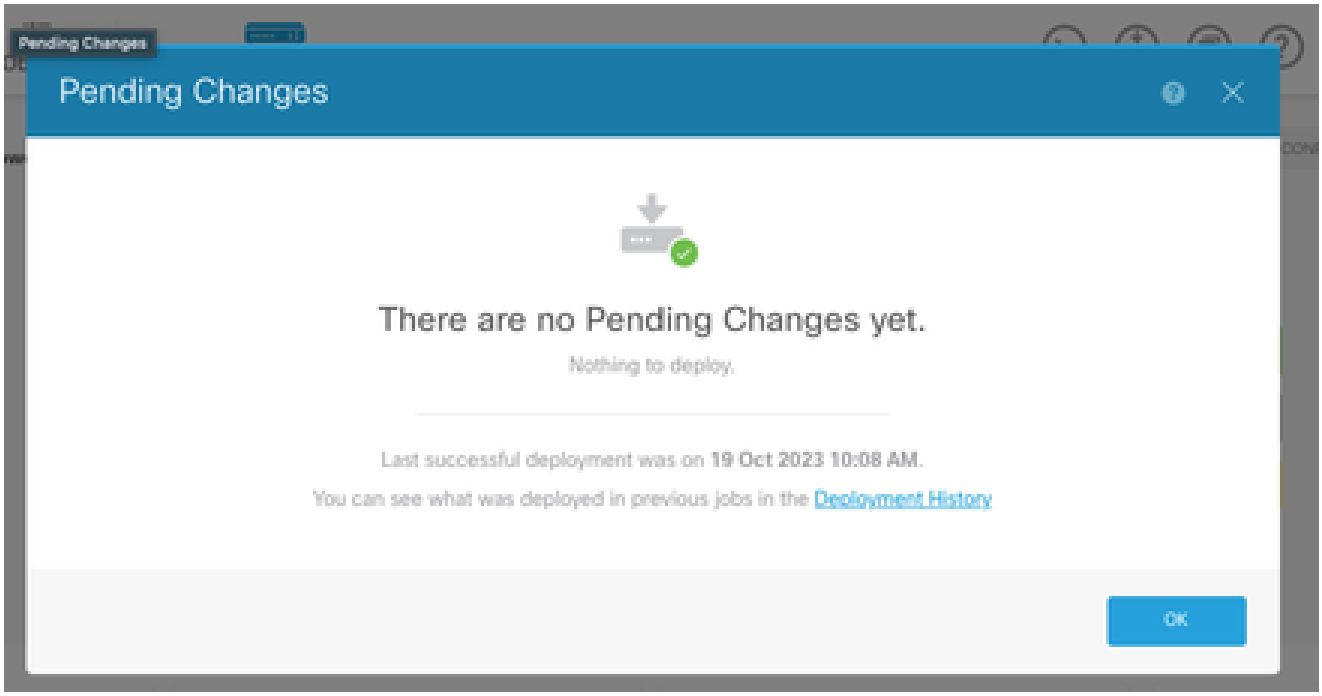
Snort 3: https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/snort/720/snort3-configuration-guide-v72/tuning-intrusion-policies.html#ID-2237-00000683_snort3

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. Ensure you IPS policies have been deployed to your FTD devices:

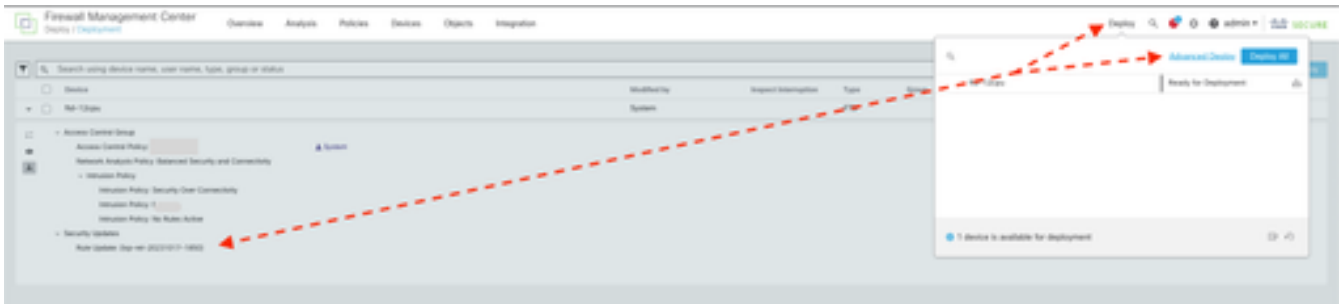
FDM

1. Click on the deploy icon
2. Ensure there are no pending changes related to the SRU/LSP



FMC

1. Click on Deploy > Advanced Deploy
2. Ensure there are no pending deployments related to SRU/LSP



6. I have a Cisco Unified Border Element (CUBE) running Cisco IOS XE. Can I disable http/https server?

The majority of CUBE deployments do not use the HTTP/HTTPS service bundled with IOS XE and disabling it will not impact functionality. If you are using the XMF-based media forking feature then you will need to configure an access-list and restrict access to the HTTP service to only include trusted hosts (CUCM/3rd party clients). You can view a configuration example here.

7. I have a Cisco Unified Communications Manager Express (CME) running Cisco IOS XE. Can I disable http/https server?

The CME solution uses HTTP services to user directory and additional services to registered IP phones. Disabling the service will cause this functionality to fail. You will need to configure an access-list and restrict access to the HTTP service to only include the IP phone network subnet. You can view a configuration example here.

8. If I disable http/https server will this impact my ability to manage my devices with Cisco DNA Center?

Disabling the HTTP/HTTPS server will not affect the device management functionalities or reachability for devices managed with Cisco DNA Center, including those in SDA (Software-Defined Access) environments. Disabling the HTTP/HTTPS server will have an impact on the Application Hosting feature, and any third-party applications being used within Cisco DNA Center's Application Hosting environment. These third-party applications might rely on the HTTP/HTTPS server for communication and functionality.

9. Will there be an impact to Smart Licensing if we disable HTTP/HTTPS server on the device?

In general, Smart Licensing uses HTTPS Client functionality and so disabling HTTP(S) server feature does not have impact to Smart Licensing operations. The only scenario where Smart Licensing communication would be impaired is when CSLU external application or SSM On-Prem is being used and configured with RESTCONF to retrieve RUM reports from devices.

10. Can a threat actor exploit the vulnerability and create a local

user even if AAA is in place?

Yes, we believe a threat actor can exploit this vulnerability to create a local user regardless of the authentication method you use. Please note that the credentials will be local to the exploited device and not into the AAA system.

11. What should be the 'curl' response if I am using my router as CA server and HTTP/S ACL is already configured to block machine IP?

'curl' response is 403 forbidden as below:

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

<html>

<head><title>403 Forbidden</title></head>

<body bgcolor="white">

*** <h1>403 Forbidden</h1> ***

***<hr> nginx ***

</body>

</html>

12. Where can I find the information on software fix or Software Maintenance Units (SMUs) availability?

Please visit Software Fix Availability for Cisco IOS XE Software Web UI Privilege Escalation Vulnerability page for further information.