Cisco IOS XE軟體Web UI許可權提升漏洞的Cisco TAC技術常見問題解答 — CVE-2023-20198

目錄

簡介

本文檔介紹Cisco技術支援中心關於Cisco IOS XE軟體Web UI許可權提升漏洞的技術常見問題。 有關漏洞的安全咨詢和Cisco Talos部落格中提供了更多詳細資訊。

概觀

本文檔概述了禁用ip http server或ip http secure-server命令的含義以及這樣做會對哪些其他功能產生影響。 此外，它還提供如何配置建議中概述的訪問清單的示例，以便在無法完全禁用功能的情況下限制對webui的訪問。

1. 我的產品受影響嗎

只有運行Cisco IOS XE軟體（版本16.x及更高版本）的產品才會受到影響。 Nexus產品、ACI、傳統IOS裝置、IOS XR、防火牆(ASA/FTD)和ISE不受影響。對於身份服務引擎，禁用http/https伺服器可能會產生其他影響。 請參閱ISE部分。

2. 如何判斷我的產品是否正在運行Cisco IOS XE?

從命令列介面(CLI)執行命令show version，您會看到如下所示的軟體型別：

switch#show version

Cisco IOS XE軟體版本17.09.03

Cisco IOS軟體[Cupertino],C9800-CL軟體(C9800-CL-K9_IOSXE)，版本17.9.3，發行版軟體(fc6)

技術支援：http://www.cisco.com/techsupport

2023年3月14日（星期二）編譯18:12 by mcpre

Cisco IOS-XE軟體，

只有軟體版本16.x及更高版本會受到此漏洞的影響。 受影響的軟體版本示例包括：

16.3.5

16.12.4

17.3.5

17.6.1

17.9.4

不受影響的IOS XE版本示例：

3.17.4秒

3.11.7E

15.6-1.S4

15.2-7.E7

3. 我正在使用身份服務引擎(ISE)重定向使用案例，無法禁用http/https伺服器。我能做什麼？

禁用ip http server和ip http secure-server將阻止以下用例工作：

- 基於裝置感測器的分析
- 狀態重定向和發現
- 訪客重新導向
- BYOD自註冊
- MDM自註冊

在不需要訪問webui的IOS-XE裝置上，建議使用以下命令阻止訪問webui，同時仍允許ISE重定向使用案例：

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

如果需要存取webui（例如使用Catalyst 9800控制器），可以使用http存取類ACL限制存取webui:https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-17/221107-filter-traffic-destin...

http訪問類ACL仍允許ISE重定向使用案例發揮作用。

4.我使用C9800無線LAN控制器(WLC)，無法停用http/http伺服器。我能做什麼？

A4。 禁用ip http server和ip http secure-server將中斷以下使用案例：
— 訪問WLC WebUI。無論是否使用無線管理介面(WMI)、服務埠或任何其他SVI來訪問WebAdmin GUI，情況都是如此。
— 第0天安裝嚮導將失敗。
- Web驗證 — 訪客存取是否WLC內部頁面、自訂Web驗證頁面、本地Web驗證、中央Web驗證將停止重新導向
— 在C9800-CL上，自簽名證書生成將失敗
- RESTCONF訪問
- S3和Cloudwatch
— 無線接入點上的IOX應用託管

為了繼續使用這些服務，您需要執行以下步驟：

(1)保持啟用HTTP/HTTPS

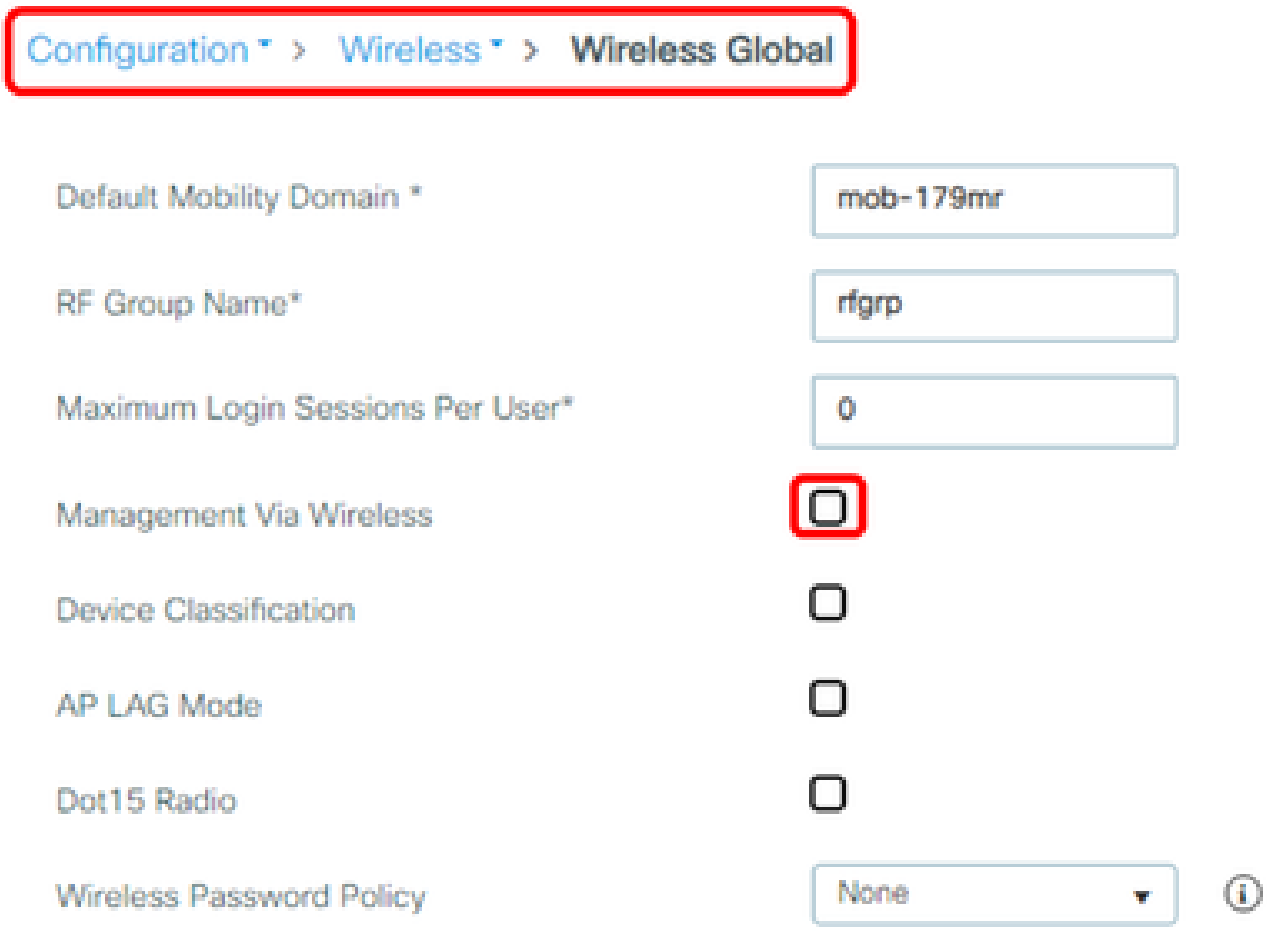
(2)使用ACL來限制對C9800 WLC Web伺服器的訪問，但僅限於受信任的子網/地址。
有關配置訪問清單的詳細資訊，請參閱： https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-17/221107-filter-traffic-destined-to-cisco-ios-xe.html。

附註：
1. AireOS WLC不易受攻擊
2. C9800(C9800-80、C9800-40、C9800-L、C9800-CL)的所有外形規格(包括AP上的嵌入式無線(EWC-AP)和交換機上的嵌入式無線(EWC-SW))都易受攻擊
3. HTTP ACL只會阻止對C9800 WLC上HTTP伺服器的訪問。無論使用WLC內部頁面、自訂

Web-Auth頁面、本地Web驗證還是中央Web驗證，都不會影響WebAuth訪客存取
4. HTTP ACL對CAPWAP控制或資料流量也沒有影響。
5.確保HTTP ACL中不允許訪問者等不受信任的網路。

或者，如果要完全阻止無線客戶端訪問WebAdmin GUI，請確保禁用「通過無線進行管理」。

GUI:



CLI:

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

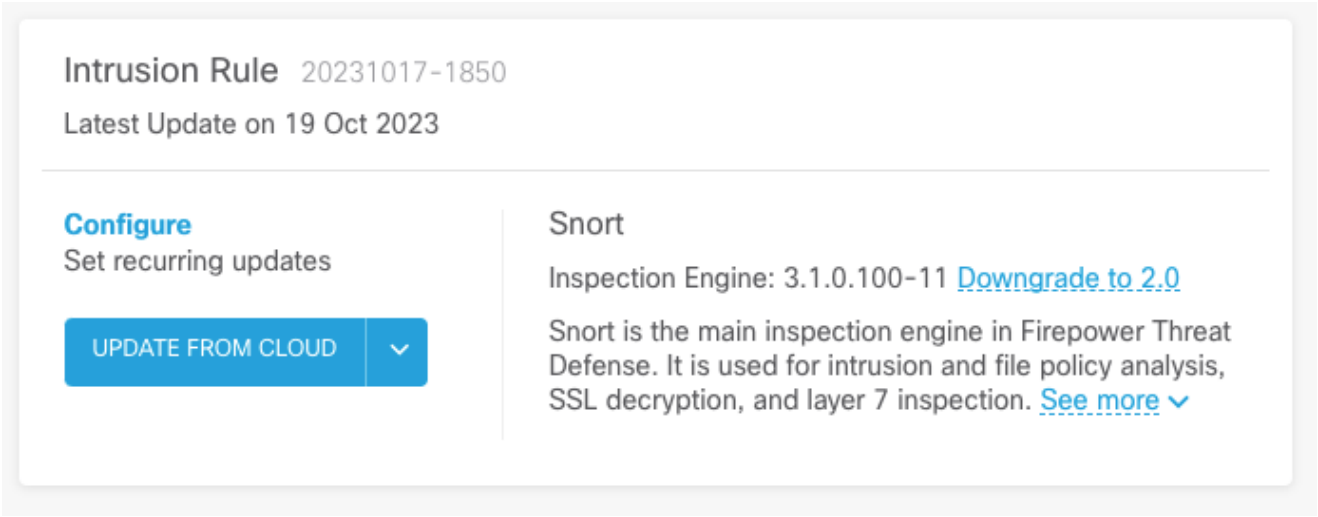
5. 在安全諮詢中，它提到存在檢測和阻止此漏洞的snort規則。如何確認已在我的FTD上安裝並運行這些規則？

要確保您的裝置上安裝了Snort規則，請檢查以確保您擁有LSP 20231014-1509或SRU-2023-10-14-001。檢查FDM和FMC受管裝置上是否安裝了此程式有所不同：

a.確保安裝規則：

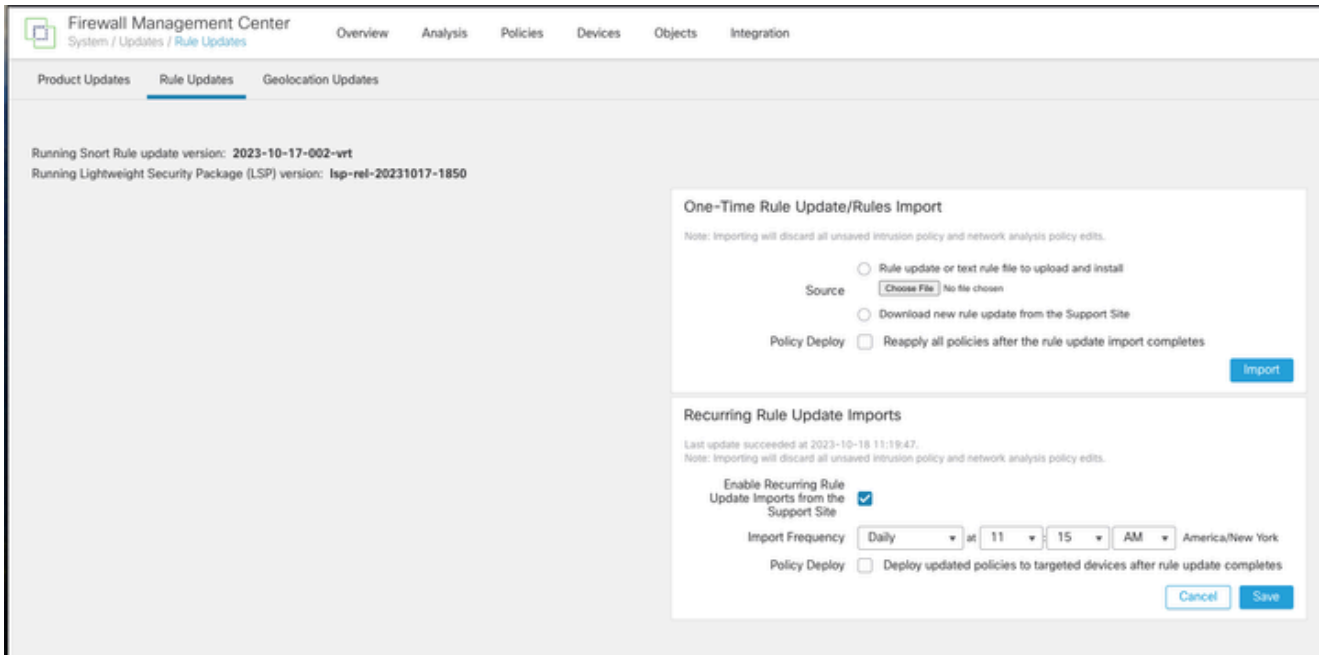
FDM

1. 導航到Device > Updates(View Configuration)
2. 檢查入侵規則並確保其為20231014-1509或更高版本



FMC

1. 導航到System > Updates > Rule Updates
2. 檢查運行Snort規則更新和運行輕量級安全包(LSP)，並確保它們運行LSP 20231014-1509或SRU-2023-10-14-001或更高版本。



b.確保入侵策略中啟用的規則

如果您的入侵策略基於Talos內建策略（通過安全實現連線、通過連線實現安全、平衡安全和連線），則這些規則將處於啟用狀態，並在預設情況下設定為丟棄。

如果您沒有將策略基於其中一個Talos內建策略。您需要為入侵策略中的這些規則啟用手動設定規則操作。 為此，請查閱以下文檔：

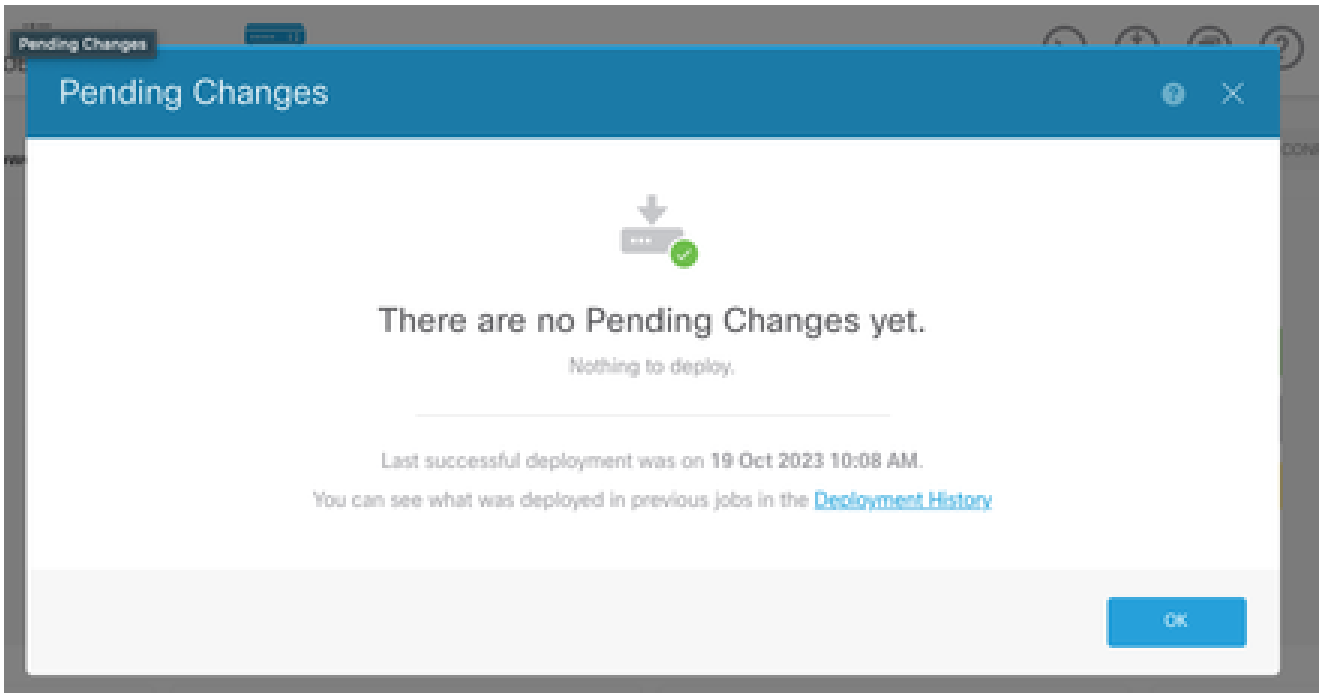
Snort 3: https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/snort/720/snort3-configuration-guide-v72/tuning-intrusion-policies.html#ID-2237-00000683_snort3

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.確保IPS策略已部署到FTD裝置：

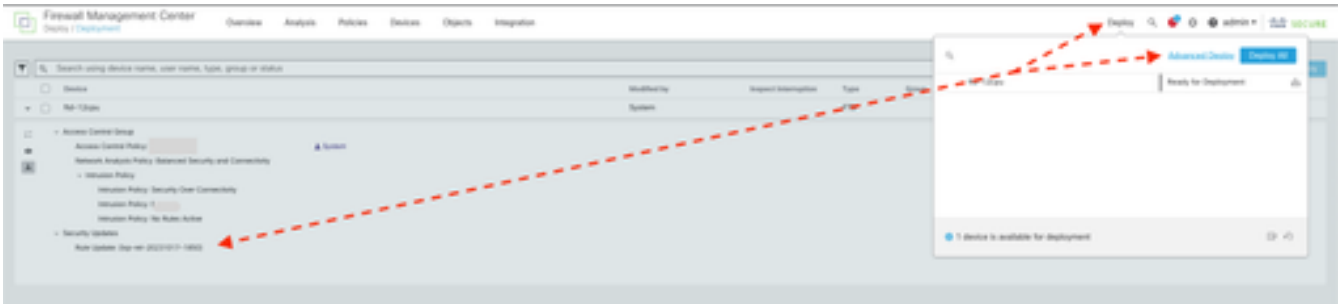
FDM

1. 點選部署圖示
2. 確保沒有與SRU/LSP相關的掛起更改



FMC

1. 點選Deploy > Advanced Deploy
2. 確保沒有與SRU/LSP相關的掛起部署



6. 我擁有運行Cisco IOS XE的Cisco Unified Border Element(CUBE)。是否可以禁用http/https伺服器？

大多數CUBE部署不使用與IOS XE捆綁在一起的HTTP/HTTPS服務，禁用該服務不會影響功能。如果您使用基於XMF的媒體分流功能，則需要配置訪問清單並將對HTTP服務的訪問限製為僅包括受信任的主機（CUCM/第三方客戶端）。 您可以在此處檢視配置示例。

7. 我擁有運行Cisco IOS XE的Cisco Unified Communications Manager Express(CME)。是否可以禁用http/https伺服器？

CME解決方案對使用者目錄使用HTTP服務，對註冊的IP電話使用其他服務。禁用該服務將導致此功能失敗。您需要配置訪問清單並將對HTTP服務的訪問限製為僅包括IP電話網路子網。您可以在此處檢視配置示例。

8. 如果我禁用http/https伺服器，是否會影響我使用Cisco DNA Center管理裝置的能力？

禁用HTTP/HTTPS伺服器不會影響通過Cisco DNA Center管理的裝置(包括SDA（軟體定義訪問）環境中的裝置)的裝置管理功能或可達性。禁用HTTP/HTTPS伺服器將影響應用託管功能，以及Cisco DNA Center的應用託管環境中正在使用的任何第三方應用。這些第三方應用程式可能依靠HTTP/HTTPS伺服器進行通訊和功能。

9. 如果我們在裝置上禁用HTTP/HTTPS伺服器，是否會影響智慧許可？

通常，智慧許可使用HTTPS客戶端功能，因此禁用HTTP(S)伺服器功能不會影響智慧許可操作。智慧許可通訊受損的唯一情況是使用CSLU外部應用程式或SSM On-Prem並配置了RESTCONF以從裝置檢索RUM報告。

10. 威脅實施者能否利用漏洞並建立本地使用者（即使AAA已到位）？

是的，我們相信威脅實施者可以利用此漏洞建立本地使用者，而不管您使用何種身份驗證方法。請注意，憑證將位於受攻擊裝置的本地位置，而不是AAA系統中。

11. 如果我使用路由器作為CA伺服器，並且HTTP/S ACL已配置為阻止電腦IP，那麼「curl」響應應該是什麼？

「curl」響應被禁止403，如下所示：

（基本）案頭~ % curl http://<裝置ip>

<html>

<head><title>403禁止</title></head>

<body bgcolor="white">

<h1>403 Forbidden</h1>

<hr> nginx

</body>

</html>

12.在哪裡可以找到有關軟體修復或軟體維護單元(SMU)可用性的

資訊？

如需詳細資訊，請參閱Software Fix Availability for Cisco IOS XE Software Web UI Privilege Escalation Vulnerability頁面。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。