Cisco IOS XE软件Web UI权限提升漏洞 — CVE-2023-20198的Cisco TAC技术常见问题解答

目录

简介

本文档介绍Cisco技术支持中心关于Cisco IOS XE软件Web UI权限提升漏洞的技术常见问题。 漏洞安全建议和Cisco Talos博客中提供了更多详细信息。

概述

本文档概述了禁用ip http server或ip http secure-server命令的含义以及这样做会对哪些其他功能产生影响。 此外，它还提供了有关如何配置建议中概述的访问列表的示例，以便在无法完全禁用功能的情况下限制对webui的访问。

1. 我的产品受影响吗

只有运行Cisco IOS XE软件版本16.x及更高版本的产品才会受到影响。 Nexus产品、ACI、传统IOS设备、IOS XR、防火墙(ASA/FTD)和ISE不受影响。对于身份服务引擎，禁用http/https服务器可能会产生其他影响。 请参阅ISE部分。

2. 如何确定我的产品是否正在运行Cisco IOS XE?

从命令行界面(CLI)执行命令show version，您将看到如下所示的软件类型：

switch#show version

思科IOS XE软件，版本17.09.03

Cisco IOS软件[Cupertino],C9800-CL软件(C9800-CL-K9_IOSXE)，版本17.9.3，发行版软件(fc6)

技术支持：http://www.cisco.com/techsupport

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

2023年3月14日（星期二）18:12由麦克普雷编译

Cisco IOS-XE软件，版权所有(c)2005-2023 Cisco Systems， Inc.

保留所有权利。Cisco IOS-XE软件的某些组件根据GNU通用公共许可证(“GPL”)版本2.0获得许可。根据GPL版本2.0许可的软件代码是附带绝对无担保的免费软件。您可以根据GPL版本2.0条款重新分发和/或修改此类GPL代码。有关详细信息，请参阅IOS-XE软件随附的文档或“许可证通知”文件，或IOS-XE软件随附的传单上提供的适用URL。

此漏洞仅影响软件版本16.x及更高版本。 受影响的软件版本示例如下：

16.3.5

16.12.4

17.3.5

17.6.1

17.9.4

不受影响的IOS XE版本示例：

3.17.4秒

3.11.7E

15.6-1.S4

15.2-7.E7

3. 我正在使用身份服务引擎(ISE)重定向使用案例，无法禁用http/https服务器。我该怎么办？

禁用ip http server和ip http secure-server将阻止以下使用案例正常工作：

- 基于设备传感器的分析
- 状况重定向和发现
- 访客重定向
- BYOD自注册
- MDM自注册

在不需要访问webui的IOS-XE设备上，建议使用以下命令阻止访问webui，同时仍允许ISE重定向使用案例：

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

如果需要访问webui，例如使用Catalyst 9800控制器，可使用http access-class ACL限制对webui的访问：https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-17/221107-filter-traffic-destin...

http access-class ACL仍然允许ISE重定向使用案例发挥作用。

4.我使用C9800无线局域网控制器(WLC)，无法禁用http/http服务器。我该怎么办？

A4。 禁用ip http server和ip http secure-server将中断以下使用案例：
— 访问WLC WebUI。无论是否使用无线管理接口(WMI)、服务端口或任何其他SVI来访问WebAdmin GUI，情况都是如此。
— 第0天安装向导将失败。
- Web-Authentication — 访客访问WLC内部页面、自定义Web-Auth页面、本地Web身份验证、中央Web身份验证是否将停止被重定向
— 在C9800-CL上，自签名证书生成将失败
- RESTCONF访问
- S3和Cloudwatch
— 无线接入点上的IOX应用托管

要继续使用这些服务，您需要执行以下步骤：

(1)保持启用HTTP/HTTPS

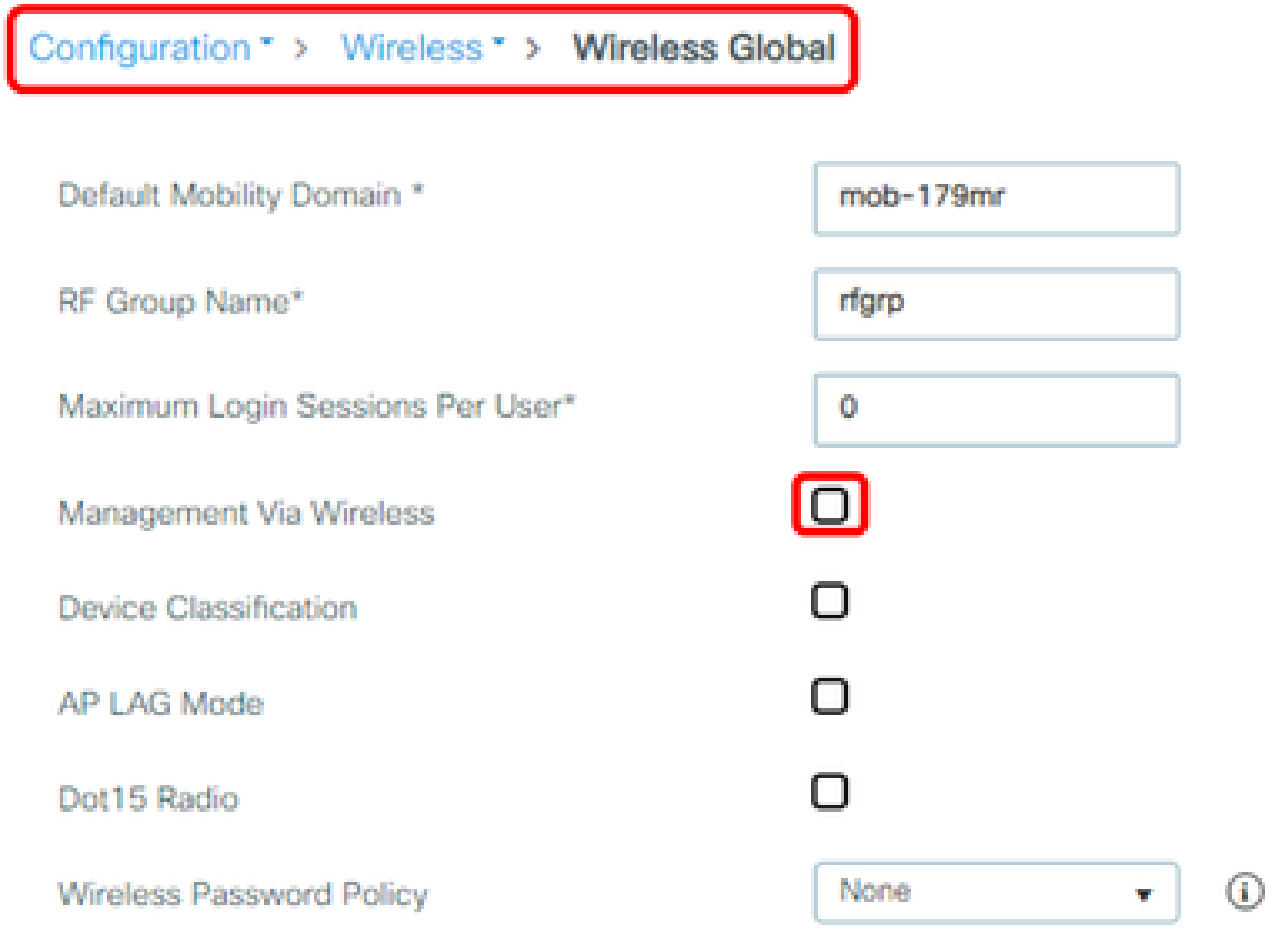
(2)使用ACL来限制对C9800 WLC Web服务器的访问，仅限制对受信任子网/地址的访问。有关配置访问列表的详细信息，请参阅： https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-17/221107-filter-traffic-destined-to-cisco-ios-xe.html。

注意：
1. AireOS WLC不易受攻击
2. C9800(C9800-80、C9800-40、C9800-L、C9800-CL)的所有外形规格(包括AP上的嵌入式无线(EWC-AP)和交换机上的嵌入式无线(EWC-SW))都易受攻击
3. HTTP ACL将仅阻止对C9800 WLC上HTTP服务器的访问。无论使用WLC内部页面、自定

义Web-Auth页面、本地Web身份验证还是集中Web身份验证，都不会影响Web身份验证访客访问
4. HTTP ACL对CAPWAP控制或数据流量也没有影响。
5.确保HTTP ACL中不允许访客等不受信任的网络。

或者，如果要完全阻止无线客户端访问WebAdmin GUI，请确保禁用“通过无线进行管理”。

GUI:



CLI：

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

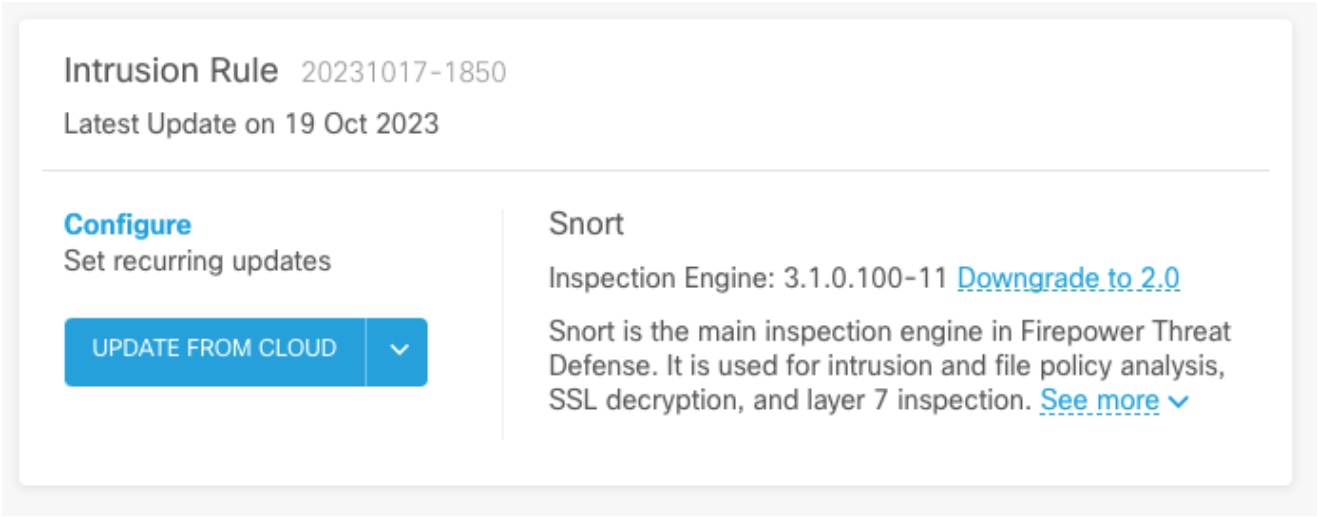
5. 安全公告中提到有检测和阻止此漏洞的snort规则。如何确认这些规则已安装并且正在我的FTD上运行？

要确保您的设备上安装了Snort规则，请检查以确保您有LSP 20231014-1509或SRU-2023-10-14-001。检查FDM和FMC受管设备上是否安装了此控件是不同的：

a.确保规则已安装：

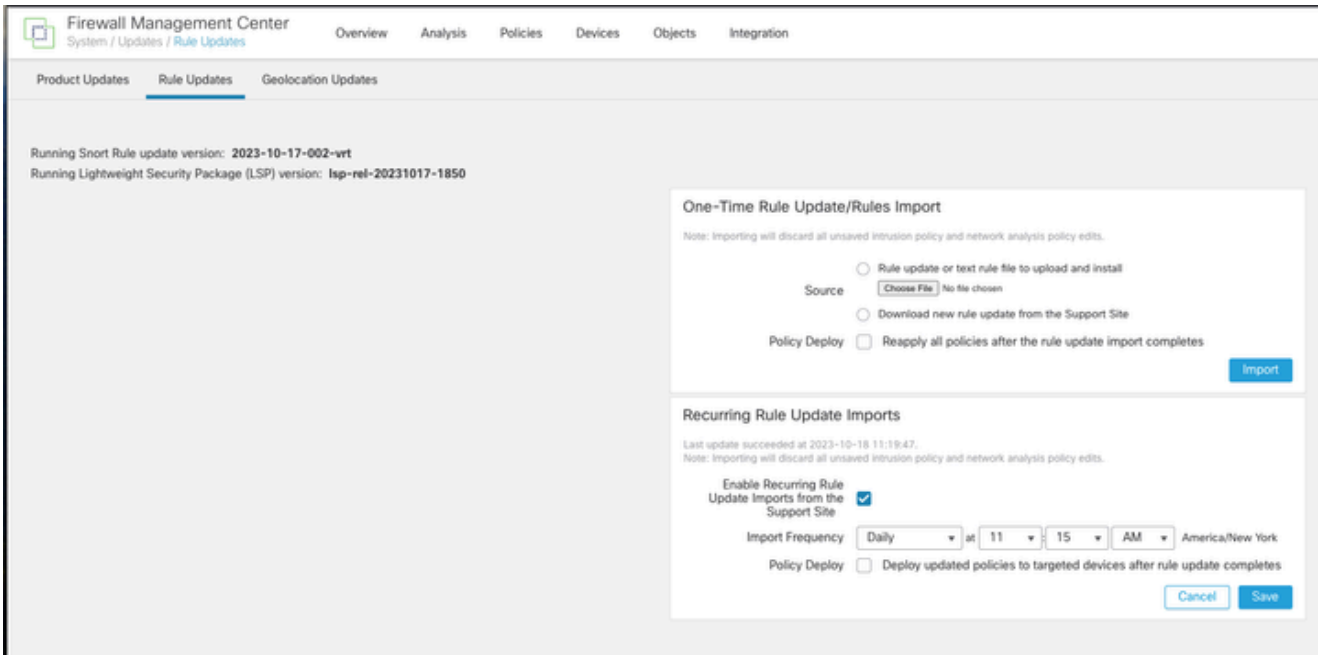
FDM

1. 导航到Device > Updates(View Configuration)
2. 检查入侵规则并确保其为20231014-1509或更高版本



FMC

1. 导航到System > Updates > Rule Updates
2. 检查运行Snort规则更新和运行轻量级安全包(LSP)，并确保它们正在运行LSP 20231014-1509或SRU-2023-10-14-001或更高版本。



b.确保入侵策略中启用的规则

如果您的入侵策略基于Talos内置策略（通过安全实现连接、通过连接实现安全、通过连接实现平衡的安全性和连接），则这些规则将被启用，默认情况下会被设置为丢弃。

如果策略不是基于某个Talos内置策略。您需要启用在入侵策略中为这些规则手动设置规则操作。为此，请查看以下文档：

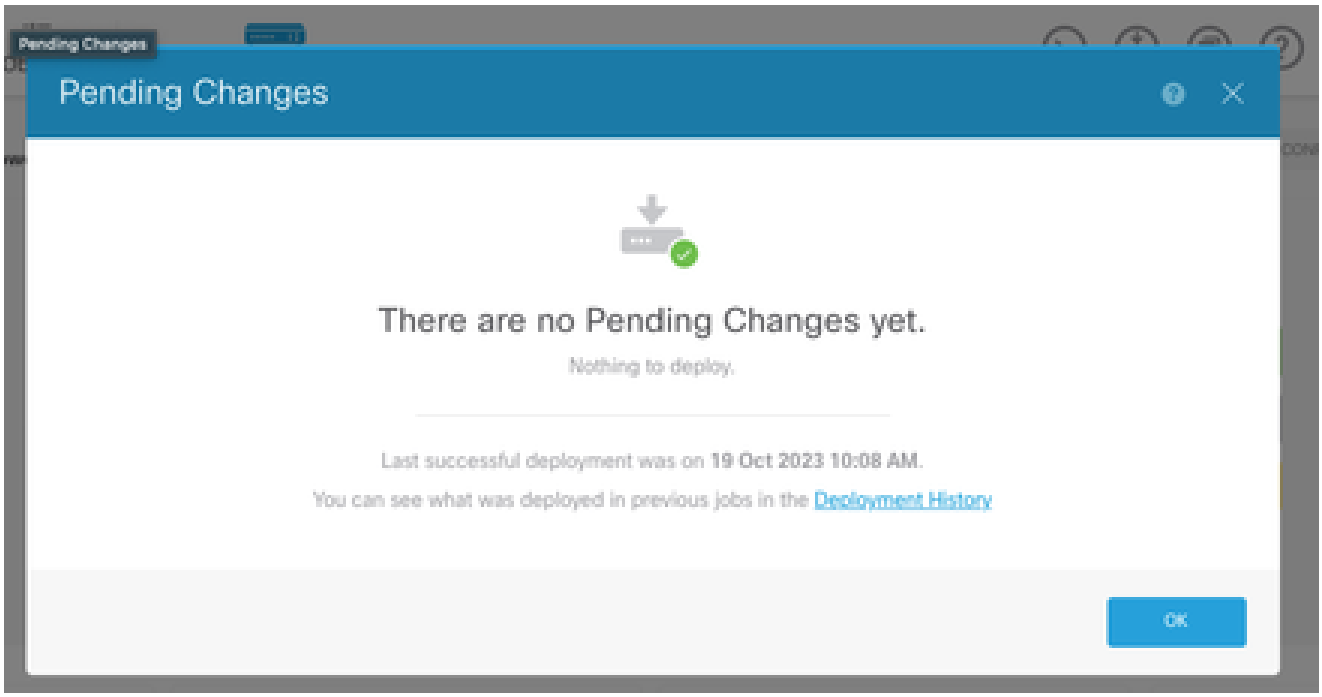
Snort 3: https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/snort/720/snort3-configuration-guide-v72/tuning-intrusion-policies.html#ID-2237-00000683_snort3

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.确保IPS策略已部署到FTD设备：

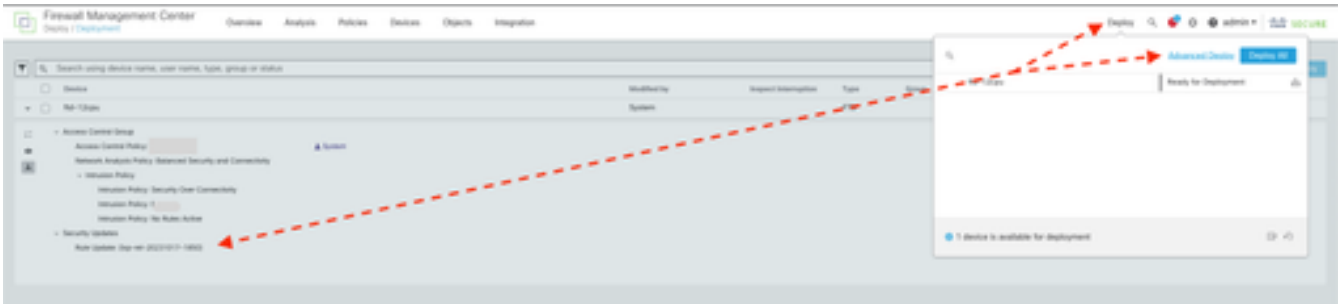
FDM

1. 点击部署图标
2. 确保没有与SRU/LSP相关的挂起更改



FMC

1. 点击部署(Deploy)>高级部署(Advanced Deploy)
2. 确保没有与SRU/LSP相关的挂起部署



6. 我有一个运行Cisco IOS XE的思科统一边界元素(CUBE)。是否可以禁用http/https服务器？

大多数CUBE部署不使用与IOS XE捆绑的HTTP/HTTPS服务，禁用该服务不会影响功能。如果您使用基于XMF的媒体分流功能，则需要配置访问列表并将对HTTP服务的访问限制为仅包括受信任的主机（CUCM/第三方客户端）。 您可以在此处查看配置示例。

7. 我拥有运行Cisco IOS XE的Cisco Unified Communications Manager Express(CME)。是否可以禁用http/https服务器？

CME解决方案对用户目录使用HTTP服务，对注册的IP电话使用其他服务。禁用该服务将导致此功能失败。您需要配置访问列表并将对HTTP服务的访问限制为仅包括IP电话网络子网。您可以在此处查看配置示例。

8. 如果我禁用http/https服务器，是否会影响我使用Cisco DNA Center管理设备的能力？

禁用HTTP/HTTPS服务器不会影响通过Cisco DNA Center管理的设备(包括SDA（软件定义访问）环境中的设备)的设备管理功能或可达性。禁用HTTP/HTTPS服务器将影响应用托管功能，以及Cisco DNA Center的应用托管环境中正在使用的任何第三方应用。这些第三方应用程序可能依靠HTTP/HTTPS服务器进行通信和功能。

9. 如果在设备上禁用HTTP/HTTPS服务器，是否会影响智能许可？

通常，智能许可使用HTTPS客户端功能，因此禁用HTTP(S)服务器功能不会影响智能许可操作。智能许可通信受损的唯一情况是，使用CSLU外部应用或SSM内部配置并使用RESTCONF从设备检索RUM报告。

10. 威胁实施者能否利用漏洞并创建本地用户（即使已部署AAA）？

是的，我们相信威胁实施者可以利用此漏洞创建本地用户，无论您使用何种身份验证方法。请注意，凭证将位于受攻击设备的本地，而不是AAA系统。

11. 如果我使用路由器作为CA服务器，并且HTTP/S ACL已配置为阻止计算机IP，那么“curl”响应应该是什么？

“curl”响应为403被禁止，如下所示：

（基础）桌面~ % curl http://<device ip>

<html>

<head><title>403禁止访问</title></head>

<body bgcolor="white">

<h1>403禁止访问</h1>

<hr> nginx

</body>

</html>

12.在哪里可以找到有关软件修复或软件维护单元(SMU)可用性的

信息？

有关详细信息，请访问Cisco IOS XE软件Web UI权限提升漏洞的软件修复可用性页。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。