Cisco IOS XE Software 웹 UI 권한 에스컬레이션 취약성에 대한 Cisco TAC 기술 FAQ - CVE-2023-20198

목차

소개

개요

1. 제품이 영향을 받습니까?

2. 제품이 Cisco IOS XE를 실행 중인지 확인하려면 어떻게 해야 합니까?

3. ISE(Identity Services Engine) 리디렉션 사용 사례이며 http/https 서버를 비활성화할 수 없습니다. 내가 뭘 할 수 있을까?

4. C9800 WLC(Wireless LAN Controller)를 사용하고 있으며 http/http 서버를 비활성화할 수 없습니다. 내가 뭘 할 수 있을까?

5. Security Advisory에서는 이러한 취약성을 탐지하고 차단하는 Snort 규칙이 있다고 언급합니다. 이 규칙이 설치되어 있고 FTD에서 작동하는지 확인하려면 어떻게 해야 합니까?

6. Cisco IOS XE를 실행하는 CUBE(Cisco Unified Border Element)가 있습니다. http/https 서버를 비활성화할 수 있습니까?

7. Cisco IOS XE를 실행하는 Cisco CME(Unified Communications Manager Express)가 있습니다. http/https 서버를 비활성화할 수 있습니까?

8. http/https 서버를 비활성화하면 Cisco DNA Center를 사용하여 디바이스를 관리할 수 있는 기능에 영향을 미칩니까?

9. 디바이스에서 HTTP/HTTPS 서버를 비활성화하면 Smart Licensing에 영향이 미칩니까?

10. AAA가 있는 경우에도 위협 행위자가 취약성을 악용하여 로컬 사용자를 생성할 수 있습니까?

11. 라우터를 CA 서버로 사용하고 있고 HTTP/S ACL이 이미 컴퓨터 IP를 차단하도록 구성되어 있는 경우 'curl' 응답은 어떻게 해야 합니까?

12. 소프트웨어 픽스 또는 SMU(Software Maintenance Unit) 가용성에 대한 정보는 어디에서 찾을 수 있습니까?

소개

이 문서는 Cisco IOS XE Software 웹 UI 권한 에스컬레이션 취약성에 대한 Cisco Technical Assistance Center의 기술 FAQ를 나타냅니다. 자세한 내용은 취약성에 대한 보안 권고 및 Cisco Talos 블로그를 참조하십시오.

개요

이 문서에서는 ip http server 또는 ip http secure-server 명령 비활성화의 의미와 이로 인해 영향을 받는 다른 기능에 대해 간략하게 설명합니다. 또한 기능을 완전히 비활성화할 수 없는 경우 webui에 대한 액세스를 제한하기 위해 권고에 설명된 액세스 목록을 구성하는 방법에 대한 예제를 제공합니다.

1. 내 제품이 영향을 받습니까?

버전 16.x 이상에서 Cisco IOS XE Software를 실행하는 제품만 영향을 받습니다. Nexus 제품, ACI, 기존 IOS 디바이스, IOS XR, 방화벽(ASA/FTD), ISE는 영향을 받지 않습니다. Identity Services Engine의 경우 http/https 서버를 비활성화하는 다른 의미가 있을 수 있습니다. ISE 섹션을 참조하십시오.

2. 제품이 Cisco IOS XE를 실행 중인지 확인하려면 어떻게 해야 합니까?

CLI(Command Line Interface)에서 show version 명령을 실행하면 다음과 같은 소프트웨어 유형이 표시됩니다.

switch#show version

Cisco IOS XE Software, 버전 17.09.03

Cisco IOS 소프트웨어 [Cupertino], C9800-CL 소프트웨어(C9800-CL-K9_IOSXE), 버전 17.9.3, 릴리스 소프트웨어(fc6)

기술 지원: 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 소프트웨어, Copyright (c) 2005-2023 by cisco Systems, Inc.

All rights reserved. Cisco IOS-XE 소프트웨어의 특정 구성 요소는 GNU General Public License("GPL") 버전 2.0에 따라 라이센스가 부여됩니다. GPL 버전 2.0에 따라 라이센스가 부여된 소프트웨어 코드는 절대적으로 보증이 없는 무료 소프트웨어입니다. GPL 버전 2.0의 약관에 따라 이러한 GPL 코드를 재배포 및/또는 수정할 수 있습니다. 자세한 내용은 IOS-XE 소프트웨어와 함께 제공되는 문서 또는 "라이센스 공지" 파일 또는 IOS-XE 소프트웨어와 함께 제공되는 전단지에 제공된 해당 URL을 참조하십시오.

소프트웨어 버전 16.x 이상만 이 취약성의 영향을 받습니다. 영향을 받는 소프트웨어 버전의 예는 다음과 같습니다.

16.3.5

16.12.4

17.3.5

17.6.1

17.9.4

영향을 받지 않는 IOS XE 버전의 예:

3.17.4초

3.11.7E

15.6-1.S4

15.2-7.E7

3 . ISE(Identity Services Engine) 리디렉션 사용 사례를 사용하고 있으며 http/https 서버를 비활성화할 수 없습니다. 내가 뭘 할 수 있을까?

ip http server 및 ip http secure-server를 비활성화하면 다음과 같은 사용 사례가 작동하지 않습니다 .

- 장치 센서 기반 프로파일링
- 상태 리디렉션 및 검색
- 게스트 리디렉션
- BYOD 온보드
- MDM 온보딩

Webui에 액세스할 필요가 없는 IOS-XE 디바이스에서는 ISE 리디렉션 사용 사례를 계속 허용하면서 다음 명령을 사용하여 webui에 대한 액세스를 차단하는 것이 좋습니다.

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

Catalyst 9800 컨트롤러와 같이 webui에 대한 액세스가 필요한 경우 http 액세스 클래스 ACL(https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-17/221107-filter-traffic-destin)을 사용하여 webui에 대한 액세스를 제한할 수 있습니다.

http access-class ACL은 여전히 ISE 리디렉션 사용 사례를 작동할 수 있도록 허용합니다.

4. C9800 WLC(Wireless LAN Controller)를 사용하고 있으며 http/http 서버를 비활성화할 수 없습니다. 내가 뭘 할 수 있을까?

A4. ip http server 및 ip http secure-server를 비활성화하면 다음 활용 사례가 중단됩니다.
- WLC WebUI에 액세스합니다. WMI(Wireless Management Interface) 또는 서비스 포트나 다른 SVI를 사용하여 WebAdmin GUI에 액세스하는 경우에도 마찬가지입니다.
- Day 0 설정 마법사가 실패합니다.
- 웹 인증 - 게스트 액세스 WLC 내부 페이지, 사용자 지정 웹 인증 페이지, 로컬 웹 인증, 중앙 웹 인증의 리디렉션 중지 여부
- C9800-CL에서 자체 서명 인증서 생성이 실패합니다.

- RESTCONF 액세스
- S3 및 Cloudwatch
- 무선 액세스 포인트에서 IOX 애플리케이션 호스팅

이 서비스를 계속 사용하려면 다음 단계를 수행해야 합니다.

(1) HTTP/HTTPS 활성화 유지

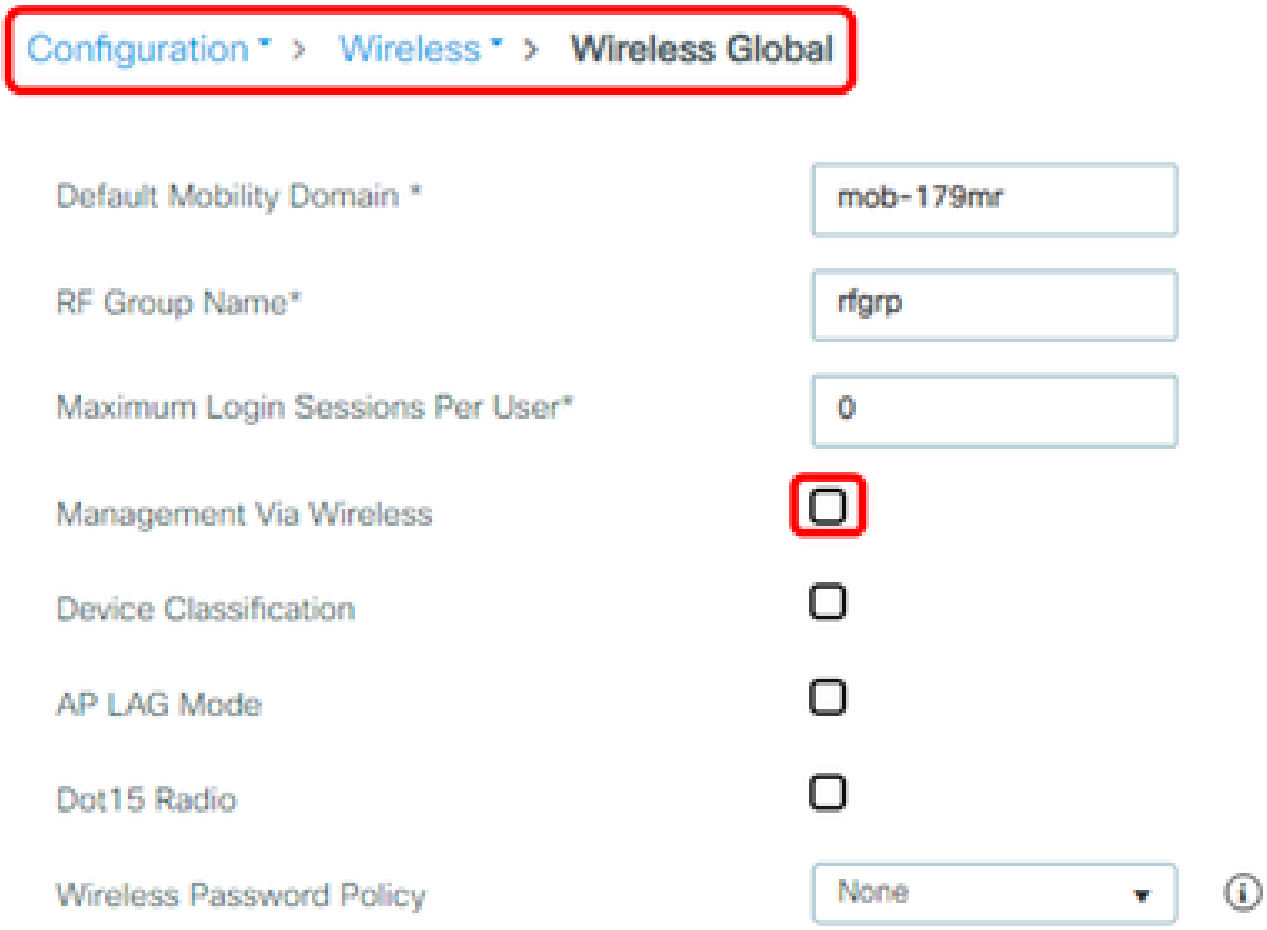
(2) ACL을 사용하여 C9800 WLC 웹 서버에 대한 액세스를 제한합니다(신뢰할 수 있는 서브넷/주소로만 제한).
액세스 목록 구성에 대한 자세한 내용은 다음을 참조하십시오.
https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-17/221107-filter-traffic-destined-to-cisco-ios-xe.html

---

참고:
1. AireOS WLC는 취약하지 않음
2. EWC-AP(Embedded Wireless on AP) 및 EWC-SW(Embedded Wireless on Switch)를 포함한 C9800(C9800-80, C9800-40, C9800-L, C9800-CL)의 모든 폼 팩터는 취약합니다
3. HTTP ACL은 C9800 WLC의 HTTP 서버에 대한 액세스만 차단합니다. WLC 내부 페이지, 사용자 지정 웹 인증 페이지, 로컬 웹 인증 또는 중앙 웹 인증 중 어떤 것을 사용하든 간에 WebAuth 게스트 액세스에 영향을 주지 않습니다
4. HTTP ACL은 CAPWAP 제어 또는 데이터 트래픽에도 영향을 미치지 않습니다.
5. 게스트와 같이 신뢰할 수 없는 네트워크가 HTTP ACL에서 허용되지 않는지 확인합니다.

선택적으로, 무선 클라이언트가 WebAdmin GUI에 액세스하는 것을 완전히 차단하려면 "무선을 통한 관리"가 비활성화되어 있는지 확인합니다.

GUI:



CLI:

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

5. 보안 자문에서는 이 취약성을 탐지하고 차단하는 snort 규칙이 있다고 언급합니다. 이 규칙이 설치되어 있고 FTD에서 작동하는지 확인하려면 어떻게 해야 합니까?

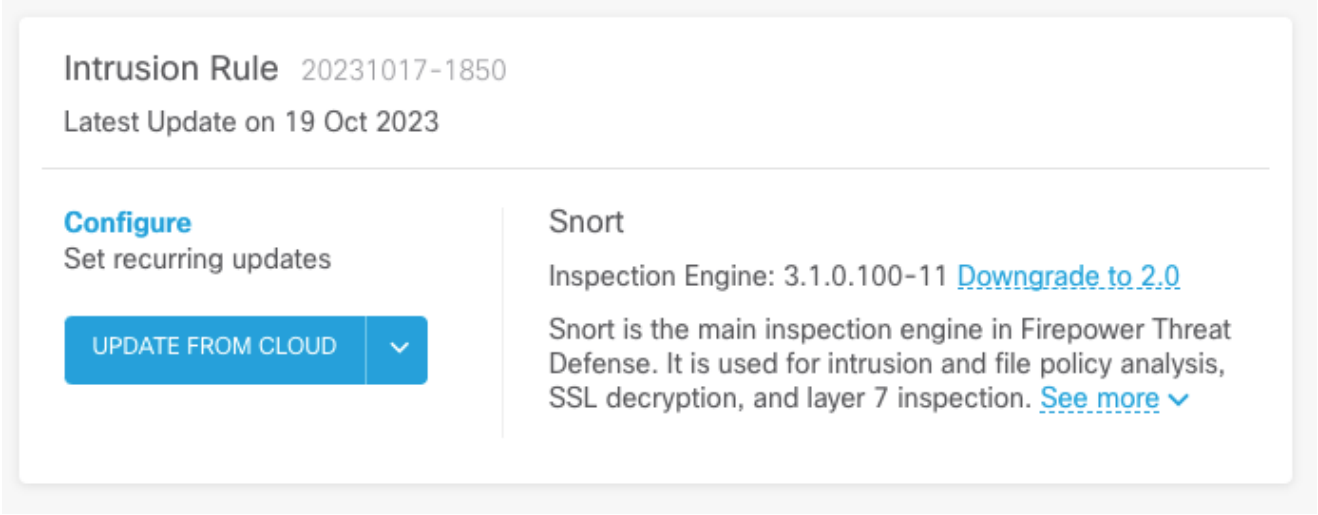
디바이스에 Snort 규칙이 설치되었는지 확인하려면 LSP 20231014-1509 또는 SRU-2023-10-14-001이 있는지 확인합니다. FDM 및 FMC 관리 디바이스에서 이 기능이 설치되어 있는지 확인하는 것이 다릅니다.

a. 규칙이 설치되어 있는지 확인합니다.

FDM

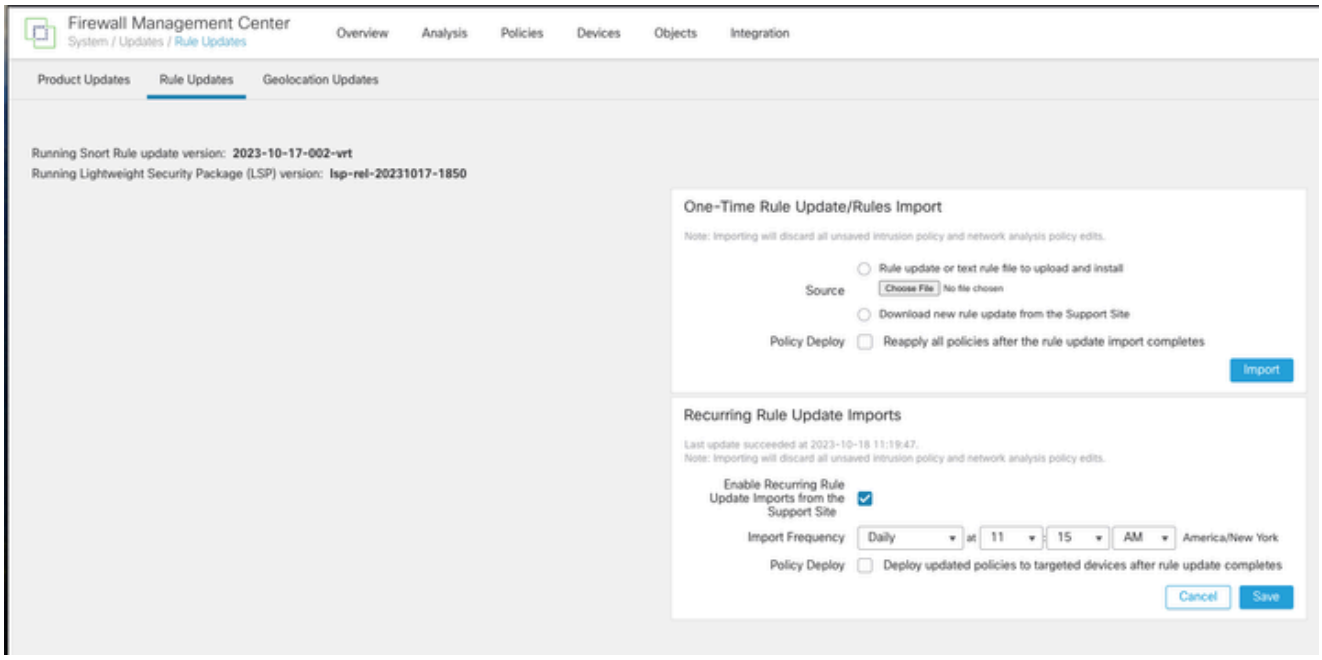
1. Device(디바이스) > Updates(업데이트)로 이동합니다(View Configuration(컨피그레이션 보기)).

2. Intrusion Rule(침입 규칙)을 확인하고 20231014-1509 이상인지 확인합니다



FMC

1. System(시스템) > Updates(업데이트) > Rule Updates(규칙 업데이트)로 이동합니다
2. Running Snort Rule update and Running Lightweight Security Package (LSP)(Snort 규칙 업데이트 실행 및 LSP 실행)를 확인하고 LSP 20231014-1509 또는 SRU-2023-10-14-001 이상을 실행하고 있는지 확인합니다.



b. 침입 정책에서 규칙이 활성화되었는지 확인합니다.

침입 정책이 Talos 기본 제공 정책(Connectivity over Security, Security over Connectivity, Balanced Security and Connectivity)을 기반으로 하는 경우 이러한 규칙은 기본적으로 활성화되고 삭제로 설정됩니다.

Talos 기본 제공 정책 중 하나를 기반으로 하지 않는 경우 침입 정책에서 이러한 규칙에 대해 규칙 작업을 수동으로 설정해야 합니다. 이렇게 하려면 아래 문서를 검토하십시오.

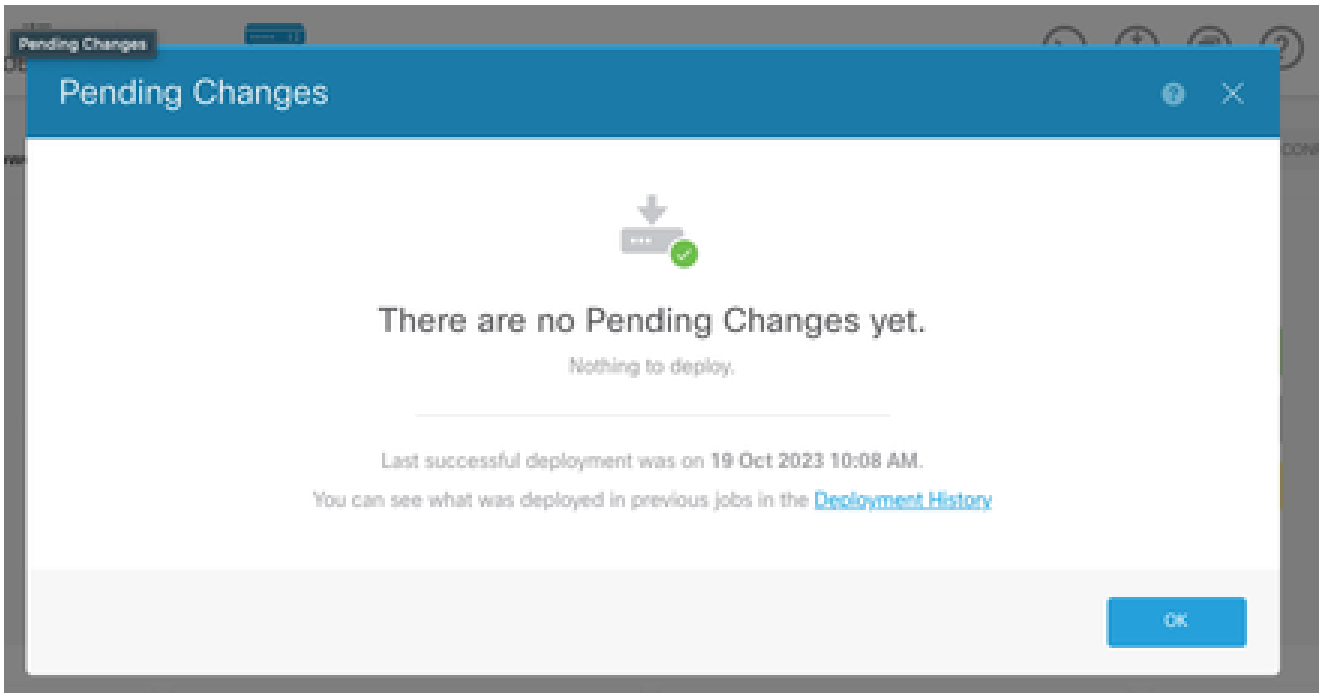
Snort 3: https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/snort/720/snort3-configuration-guide-v72/tuning-intrusion-policies.html#ID-2237-00000683_snort3

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. IPS 정책이 FTD 디바이스에 구축되었는지 확인합니다.

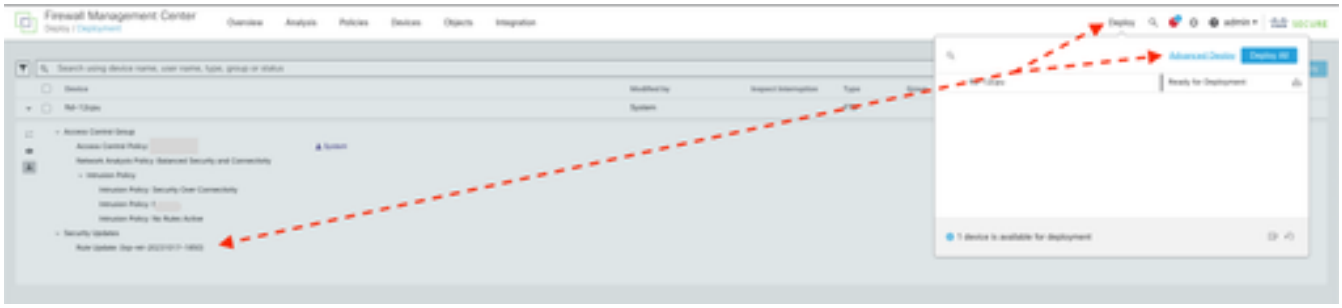
FDM

1. 구축 아이콘 클릭
2. SRU/LSP와 관련된 보류 중인 변경 사항이 없는지 확인합니다.



FMC

1. Deploy(구축) > Advanced Deploy(고급 구축)를 클릭합니다
2. SRU/LSP와 관련된 보류 중인 구축이 없는지 확인합니다.



6. Cisco IOS XE를 실행 중인 Cisco CUBE(Unified Border Element)가 있습니다. http/https 서버를 비활성화할 수 있습니까?

대부분의 CUBE 구축은 IOS XE와 함께 번들로 제공되는 HTTP/HTTPS 서비스를 사용하지 않으므로 이를 비활성화해도 기능에 영향을 주지 않습니다. XMF 기반 미디어 포킹 기능을 사용하는 경우 액세스 목록을 구성하고 HTTP 서비스에 대한 액세스를 제한하여 신뢰할 수 있는 호스트(CUCM/서드파티 클라이언트)만 포함하도록 해야 합니다. 여기서 컨피그레이션 예를 볼 수 있습니다.

7 . Cisco IOS XE를 실행하는 Cisco CME(Unified Communications Manager Express)가 있습니다. http/https 서버를 비활성화할 수 있습니까?

CME 솔루션은 사용자 디렉토리에 대한 HTTP 서비스와 등록된 IP 전화에 대한 추가 서비스를 사용

합니다. 서비스를 비활성화하면 이 기능이 실패합니다. 액세스 목록을 구성하고 HTTP 서비스에 대한 액세스를 제한하여 IP 전화 네트워크 서브넷만 포함하도록 해야 합니다. 여기서 컨피그레이션 예를 볼 수 있습니다.

8. http/https 서버를 비활성화하면 Cisco DNA Center를 사용하여 디바이스를 관리하는 기능에 영향을 미칩니까?

HTTP/HTTPS 서버를 비활성화해도 SDA(Software-Defined Access) 환경을 비롯하여 Cisco DNA Center로 관리되는 디바이스의 디바이스 관리 기능 또는 연결 기능에는 영향을 주지 않습니다. HTTP/HTTPS 서버를 비활성화하면 애플리케이션 호스팅 기능 및 Cisco DNA Center의 애플리케이션 호스팅 환경에서 사용되는 모든 타사 애플리케이션에 영향을 미칩니다. 이러한 서드파티 애플리케이션은 통신 및 기능을 위해 HTTP/HTTPS 서버에 의존할 수 있습니다.

9 . 디바이스에서 HTTP/HTTPS 서버를 비활성화하면 Smart Licensing에 영향이 미칩니까?

일반적으로 Smart Licensing은 HTTPS 클라이언트 기능을 사용하므로 HTTP(S) 서버 기능을 비활성화해도 Smart Licensing 작업에 영향을 주지 않습니다. Smart Licensing 통신이 손상된 유일한 시나리오는 CSLU 외부 애플리케이션 또는 SSM 온프레미스(On-Prem)를 사용하고 디바이스에서 RUM 보고서를 검색하도록 RESTCONF와 함께 구성하는 경우입니다.

10. AAA가 있는 경우에도 위협 행위자가 취약성을 악용하고 로컬 사용자를 생성할 수 있습니까?

예. 위협 행위자가 이 취약성을 악용하여 사용하는 인증 방법에 관계없이 로컬 사용자를 생성할 수 있습니다. 자격 증명은 AAA 시스템이 아니라 익스플로잇된 디바이스의 로컬이 됩니다.

11. 라우터를 CA 서버로 사용하고 있고 HTTP/S ACL이 이미 컴퓨터 IP를 차단하도록 구성되어 있는 경우 'curl' 응답은 어떻게 해야 합니까?

'curl' 응답은 다음과 같이 403을 사용할 수 없습니다.

(기본) 데스크톱 ~ % curl http://<장치 ip>

<html>

<head><title>403 금지</title></head>

<body bgcolor="white">

<h1>403 금지</h1>

<hr> nginx

</body>

</html>

12. 소프트웨어 픽스 또는 SMU(Software Maintenance Unit) 가용성에 대한 정보는 어디에서 찾을 수 있습니까?

자세한 내용은 Software Fix Availability for Cisco IOS XE Software 웹 UI Privilege Escalation Vulnerability(Cisco IOS XE 소프트웨어의 소프트웨어 수정 가용성) 페이지를 참조하십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.