Perguntas frequentes técnicas do Cisco TAC para a vulnerabilidade de escalação de privilégios da interface de usuário da Web do software Cisco IOS XE - CVE-2023-20198

Contents

Introdução

Overview

1. Meu produto é afetado?

2. Como posso determinar se meu produto está executando o Cisco IOS XE?

3. Estou usando casos de uso de redirecionamento do Identity Services Engine (ISE) e não posso desabilitar os servidores http/https. O que eu posso fazer?

4. Estou usando a controladora Wireless LAN (WLC) C9800 e não posso desabilitar os servidores http/http. O que eu posso fazer?

5. No aviso de segurança, ele menciona que há regras de snort para detectar e bloquear essa vulnerabilidade. Como confirmo se essas regras estão instaladas e funcionando no meu FTD?

6. Tenho um Cisco Unified Border Element (CUBE) executando o Cisco IOS XE. Posso desativar o servidor http/https?

7. Tenho um Cisco Unified Communications Manager Express (CME) executando o Cisco IOS XE. Posso desativar o servidor http/https?

8. Se eu desativar o servidor http/https, minha capacidade de gerenciar meus dispositivos com o Cisco DNA Center será afetada?

9. Haverá um impacto no Smart Licensing se desabilitarmos o servidor HTTP/HTTPS no dispositivo?

10. Um fator de ameaça pode explorar a vulnerabilidade e criar um usuário local mesmo que o AAA esteja em vigor?

11. Qual deverá ser a resposta 'curl' se eu estiver usando meu roteador como servidor de CA e se a ACL HTTP/S já estiver configurada para bloquear o IP da máquina?

12. Onde posso encontrar as informações sobre a disponibilidade das unidades de manutenção de software (SMUs) ou reparo de software?

Introdução

Este documento representa as Perguntas Frequentes Técnicas do Cisco Technical Assistance Center para a Vulnerabilidade de Escalação de Privilégios da Interface do Usuário Web do Software Cisco IOS XE. Detalhes adicionais estão disponíveis no consultivo de segurança para a vulnerabilidade e no blog do Cisco Talos.

Overview

Este documento descreve as implicações da desativação dos comandos ip http server ou ip http

secure-server e que outras funcionalidades são afetadas por isso. Além disso, ele fornece exemplos de como configurar as listas de acesso destacadas no consultivo para limitar o acesso ao webui no caso de você não conseguir desativar completamente os recursos.

1. Meu produto é afetado?

Somente os produtos que executam o software Cisco IOS XE com versões 16.x e superiores são afetados. Os produtos Nexus, ACI, dispositivos IOS tradicionais, IOS XR, firewalls (ASA/FTD), ISE não são afetados. No caso do Identity Services Engine, pode haver outras implicações de desabilitar o servidor http/https. Consulte a seção ISE.

2. Como posso determinar se meu produto está executando o Cisco IOS XE?

Execute o comando show version a partir da interface de linha de comando (CLI) e você verá o tipo de software como este:

switch#show version

Software Cisco IOS XE, versão 17.09.03

Software Cisco IOS [Cupertino], Software C9800-CL (C9800-CL-K9_IOSXE), Versão 17.9.3, SOFTWARE DE VERSÃO (fc6)

Suporte técnico: http://www.cisco.com/techsupport

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

Compilado em inglês 14-mar-23 18:12 por mcpre

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

Todos os direitos reservados. Determinados componentes do software Cisco IOS-XE são licenciados sob a GNU General Public License ("GPL") Versão 2.0. O código de software licenciado sob a GPL Versão 2.0 é um software gratuito que vem com ABSOLUTELY NO WARRANTY. Você pode redistribuir e/ou modificar esse código GPL sob os termos da GPL Versão 2.0. Para obter mais detalhes, consulte a documentação ou o arquivo de "Aviso de Licença" que acompanha o software IOS-XE, ou a URL aplicável fornecida no folheto que acompanha o software IOS-XE.

Somente as versões de software 16.x e posteriores são afetadas por essa vulnerabilidade. Exemplos de versões de software afetadas são:

16.3.5

16.12.4

17.3.5

17.6.1

17.9.4

Exemplos de versões do IOS XE que NÃO são afetadas:

3,17,4S

3,11,7E

15.6-1.S4

15.2-7.E7

3. Estou usando casos de uso de redirecionamento do Identity Services Engine (ISE) e não posso desabilitar os servidores http/https. O que eu posso fazer?

Desabilitar o ip http server e o ip http secure-server impedirá que casos de uso como o seguinte funcionem:

- Criação de perfis baseada no sensor de dispositivos
- Redirecionamento e descoberta de postura
- Redirecionamento de Convidado
- Integração de BYOD
- Integração de MDM

Em dispositivos IOS-XE que não exigem acesso ao webui, é recomendável usar os seguintes comandos para impedir o acesso ao webui enquanto ainda permite os casos de uso de redirecionamento do ISE:

- ip http ative-session-modules none
- ip http secure-ative-session-modules none

Se o acesso ao webui for necessário, como com os controladores Catalyst 9800, o acesso ao webui pode ser restrito usando ACLs de classe de acesso http: https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-17/221107-filter-traffic-destin...

As ACLs de classe de acesso http ainda permitem que os casos de uso de redirecionamento do ISE funcionem.

4. Estou usando a controladora Wireless LAN (WLC) C9800 e não posso desabilitar os servidores http/http. O que eu posso fazer?

A4. Desabilitar o ip http server e o ip http secure-server interromperá os seguintes casos de uso:

- Acesso à WebUI da WLC. Isso ocorre quando a Interface de Gerenciamento Sem Fio (WMI), a Porta de Serviço ou qualquer outra SVI está sendo usada para acessar a GUI do WebAdmin.
- O Assistente para configuração do dia 0 falhará.
- Autenticação da Web - Acesso de convidado se a página interna da WLC, a página de autenticação da Web personalizada, a autenticação da Web local e a autenticação da Web central deixarem de ser redirecionadas
- Em uma C9800-CL, a geração do certificado autoassinado falhará
- acesso RESTCONF
- S3 e Cloudwatch
- Hospedagem de aplicativos IOX em access points sem fio

Para continuar usando esses serviços, você precisará executar as seguintes etapas:

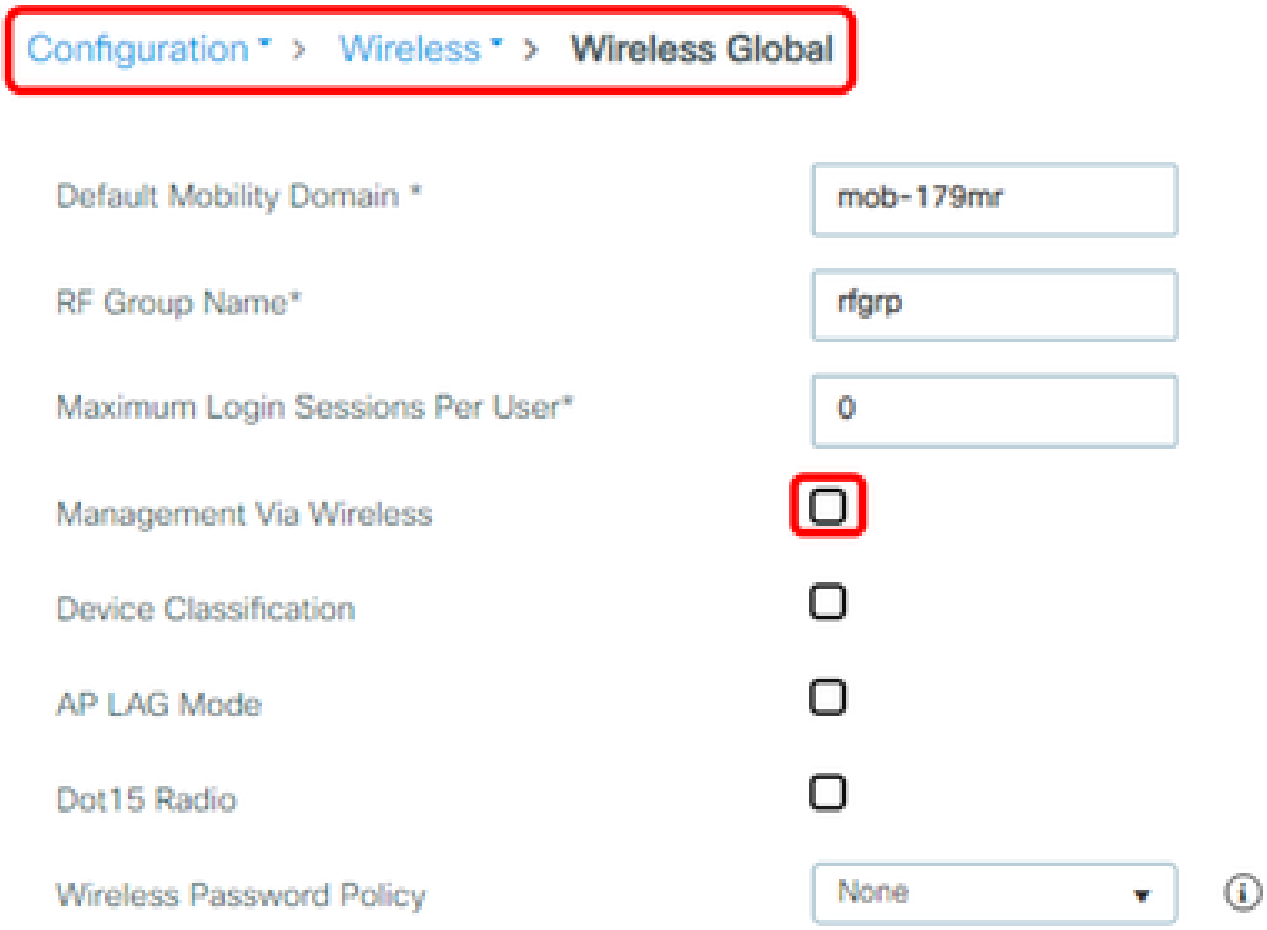
(1) Manter HTTP/HTTPS habilitado

(2) Use uma ACL para limitar o acesso ao servidor web da WLC C9800, somente a sub-redes / endereços confiáveis.
Detalhes sobre a configuração da lista de acesso podem ser encontrados: 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. As WLCs AireOS não são vulneráveis
2. Todos os formatos de C9800 (C9800-80, C9800-40, C9800-L, C9800-CL), incluindo Wireless on AP incorporado (EWC-AP) e Wireless on Switch incorporado (EWC-SW), são vulneráveis
3. A ACL HTTP apenas bloqueará o acesso ao servidor HTTP na WLC C9800. Ele não afetará o acesso de convidado WebAuth usando a página interna da WLC, a página de autenticação da Web personalizada, a autenticação da Web local ou a autenticação da Web central
4. A ACL HTTP também não tem impacto no controle CAPWAP ou tráfego de dados.
5. Certifique-se de que redes não confiáveis, como convidado, não sejam permitidas na ACL HTTP.

Opcionalmente, se você quiser bloquear completamente seus clientes sem fio de acessarem a GUI do WebAdmin, certifique-se de que o "Gerenciamento via Wireless" esteja desativado.

GUI:



CLI:

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

5. No aviso de segurança, ele menciona que há regras de snort para detectar e bloquear essa vulnerabilidade. Como confirmo se essas regras estão instaladas e funcionando no meu FTD?

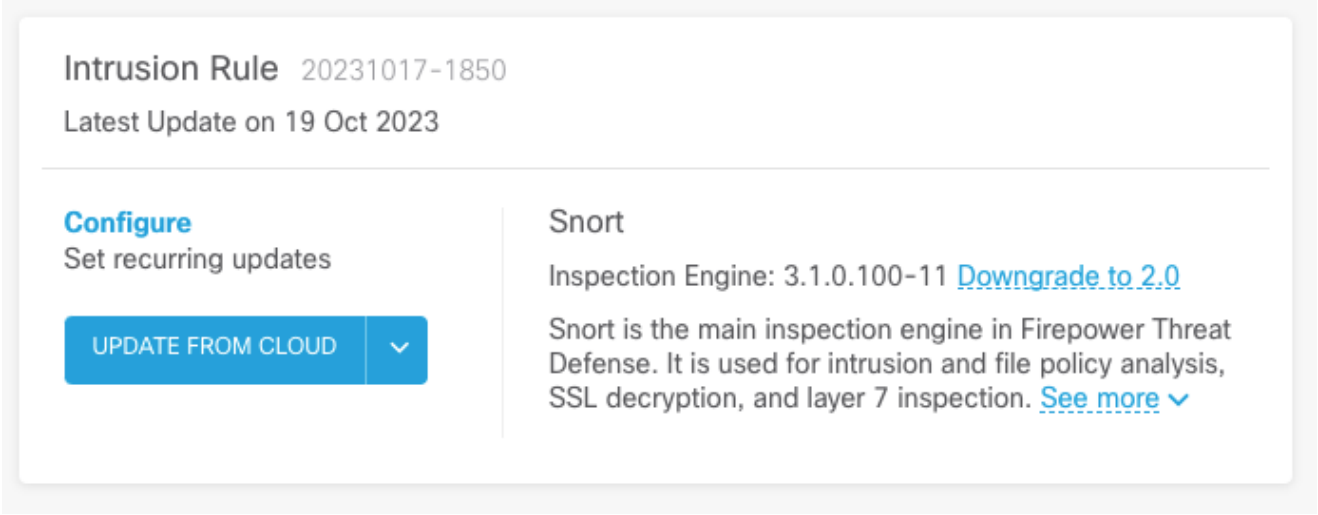
Para garantir que as regras do Snort estejam instaladas no dispositivo, verifique se você tem o LSP 20231014-1509 ou o SRU-2023-10-14-001. Verificar se isso está instalado é diferente nos dispositivos gerenciados do FDM e do FMC:

a. Verifique se as regras estão instaladas:

FDM

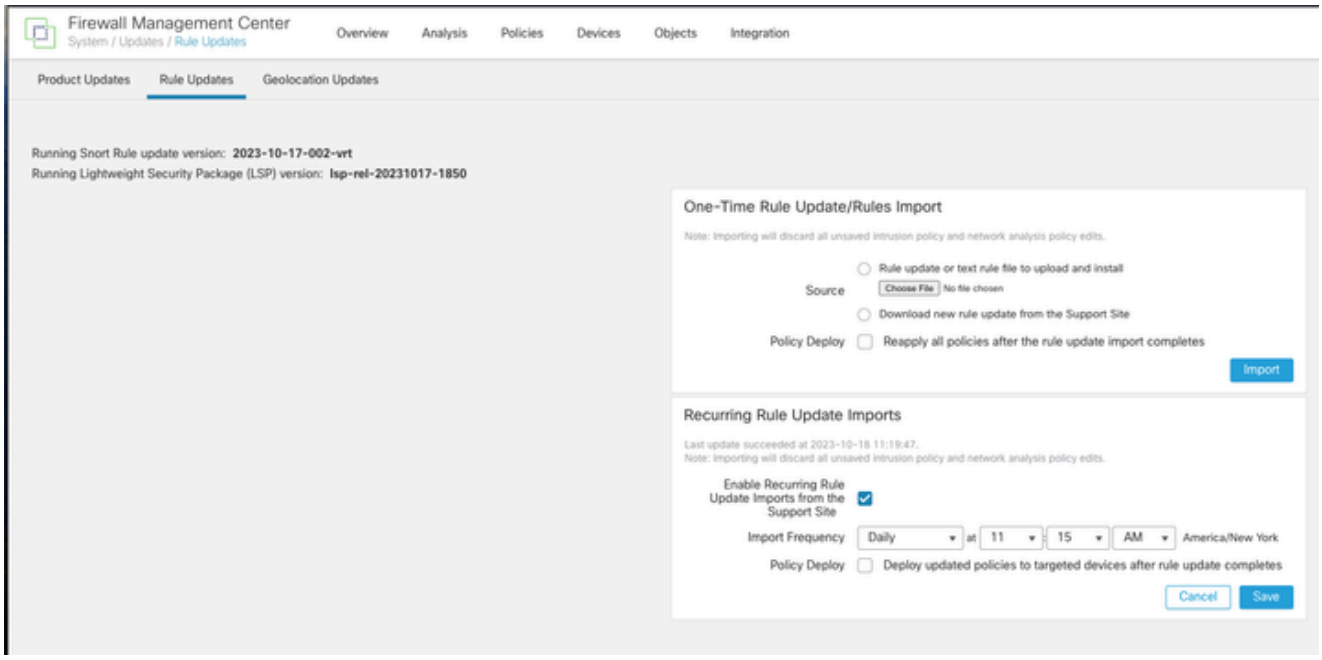
1. Navegue até Dispositivo > Atualizações (Exibir configuração)

2. Verifique a regra de intrusão e certifique-se de que ela seja 20231014-1509 ou mais recente



CVP

1. Navegue até Sistema > Atualizações > Atualizações de Regras
2. Verifique Running Snort Rule update and Running Lightweight Security Package (LSP) e certifique-se de que eles estejam executando o LSP 20231014-1509 ou SRU-2023-10-14-001 ou superior.



b. Certifique-se de que as regras estejam ativadas na sua Política de intrusão

Se suas Políticas de intrusão forem baseadas nas políticas internas do Talos (conectividade sobre segurança, segurança sobre conectividade, segurança equilibrada e conectividade), essas regras serão habilitadas e definidas para serem descartadas por padrão.

Se você não estiver baseando sua política em uma das políticas incorporadas do Talos. Você precisará ativar as ações de definição de regras manualmente para essas regras na sua Política de intrusão. Para fazer isso, revise a documentação abaixo:

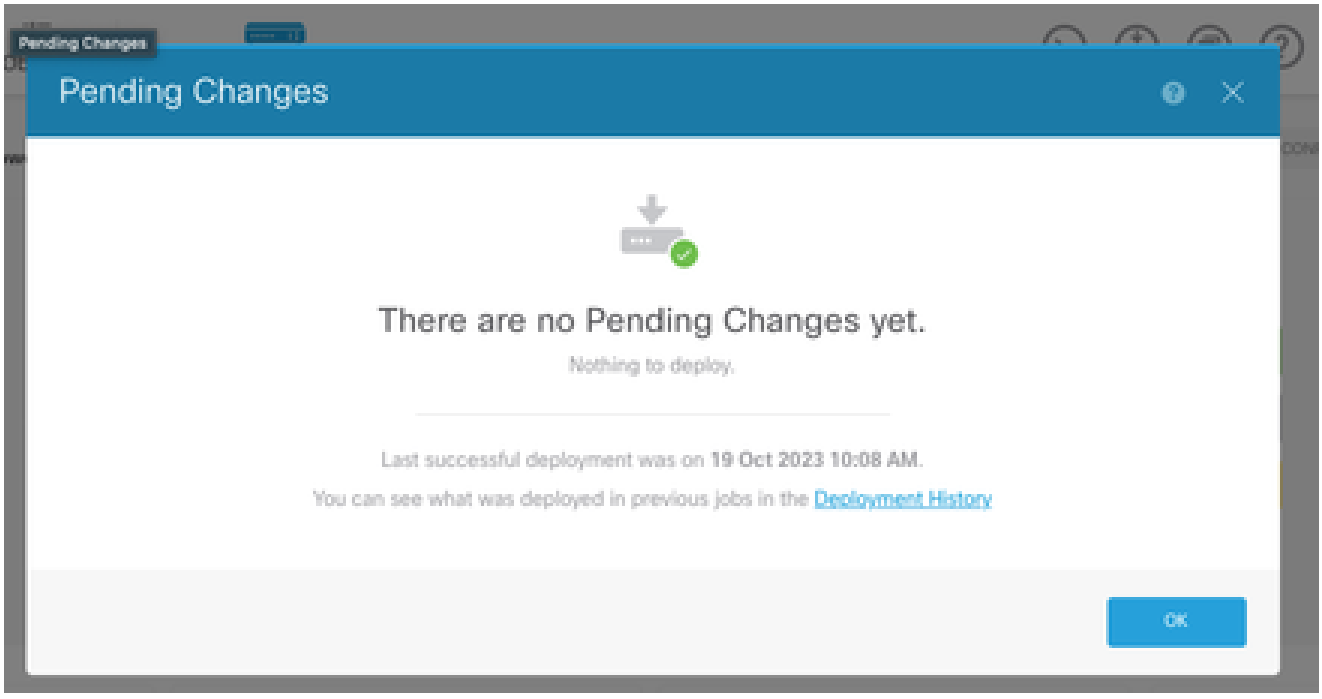
Snort 3 https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/snort/720/snort3-configuration-guide-v72/tuning-intrusion-policies.html#ID-2237-00000683_snort3

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. Certifique-se de que suas políticas de IPS foram implantadas em seus dispositivos de FTD:

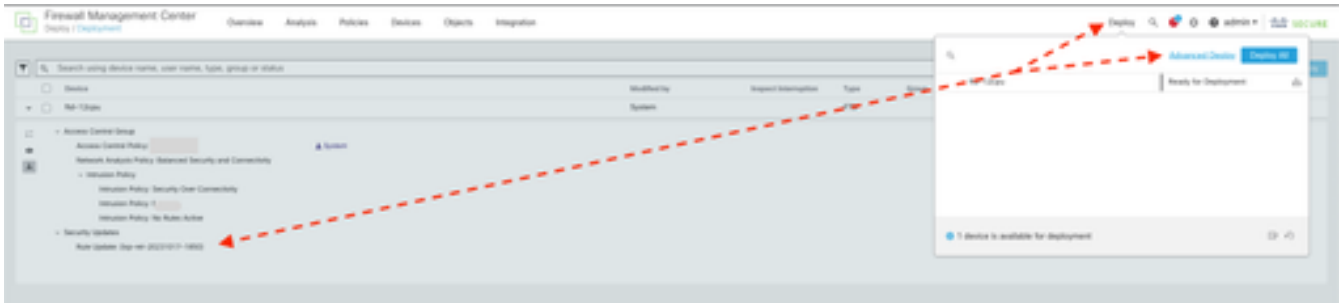
FDM

1. Clique no ícone de implantação
2. Verifique se não há alterações pendentes relacionadas ao SRU/LSP



CVP

1. Clique em Implantar > Implantação avançada
2. Verifique se não há implantações pendentes relacionadas a SRU/LSP



6. Tenho um Cisco Unified Border Element (CUBE) executando o Cisco IOS XE. Posso desativar o servidor http/https?

A maioria das implantações do CUBE não usa o serviço HTTP/HTTPS incluído no IOS XE e desativá-lo não afetará a funcionalidade. Se estiver usando o recurso bifurcação de mídia baseada em XMF, você precisará configurar uma lista de acesso e restringir o acesso ao serviço HTTP para incluir somente hosts confiáveis (CUCM/clientes de terceiros). Você pode ver um exemplo de configuração aqui.

7. Tenho um Cisco Unified Communications Manager Express (CME) executando o Cisco IOS XE. Posso desativar o servidor http/https?

A solução CME usa serviços HTTP para o diretório de usuário e serviços adicionais para telefones IP registrados. A desativação do serviço fará com que essa funcionalidade falhe. Você precisará configurar uma lista de acesso e restringir o acesso ao serviço HTTP para incluir apenas a sub-rede da rede do telefone IP. Você pode ver um exemplo de configuração aqui.

8. Se eu desativar o servidor http/https, minha capacidade de gerenciar meus dispositivos com o Cisco DNA Center será afetada?

Desabilitar o servidor HTTP/HTTPS não afetará as funcionalidades de gerenciamento de dispositivos nem a acessibilidade para dispositivos gerenciados com o Cisco DNA Center, incluindo aqueles em ambientes SDA (Software-Defined Access). Desabilitar o servidor HTTP/HTTPS terá um impacto sobre o recurso de Hospedagem de Aplicativos e qualquer aplicativo de terceiros que esteja sendo usado no ambiente de Hospedagem de Aplicativos do Cisco DNA Center. Esses aplicativos de terceiros podem confiar no servidor HTTP/HTTPS para comunicação e funcionalidade.

9. Haverá um impacto no Smart Licensing se desabilitarmos o servidor HTTP/HTTPS no dispositivo?

Em geral, o Smart Licensing usa a funcionalidade do cliente HTTPS e, portanto, desabilitar o recurso de servidor HTTP(S) não tem impacto nas operações do Smart Licensing. O único cenário em que a comunicação do Smart Licensing seria prejudicada é quando o aplicativo externo CSLU ou SSM On-Prem está sendo usado e configurado com RESTCONF para recuperar relatórios RUM dos dispositivos.

10. Um agente de ameaças pode explorar a vulnerabilidade e criar um usuário local mesmo que o AAA esteja em vigor?

Sim, acreditamos que um agente de ameaças possa explorar essa vulnerabilidade para criar um usuário local, independentemente do método de autenticação usado. Observe que as credenciais serão locais para o dispositivo explorado e não para o sistema AAA.

11. Qual deve ser a resposta 'curl' se eu estiver usando meu roteador como servidor de CA e a ACL HTTP/S já estiver configurada para bloquear o IP da máquina?

A resposta 'curl' é 403 proibida conforme abaixo:

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

<html>

<head><title>403 Proibido</title></head>

<body bgcolor="white">

<h1>403 Proibido</h1>

<hr> nginx

</body>

</html>

12. Onde posso encontrar as informações sobre a disponibilidade das unidades de manutenção de software (SMUs) ou reparo de software?

Visite a página Disponibilidade de correções de software para vulnerabilidade de escalação de

privilégios de UI da Web do software Cisco IOS XE para obter mais informações.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.