Cisco IOS XEソフトウェアのWeb UIにおける権限昇格の脆弱性に関するCisco TACテクニカルFAQ - CVE-2023-20198

内容

はじめに

概要

1.製品に影響がありますか？

2.製品がCisco IOS XEを実行しているかどうかは、どのようにして確認できますか。

3. Identity Services Engine(ISE)リダイレクトのユースケースを使用していて、http/httpsサーバを無効にできません。どうしたらよいですか。

4. C9800ワイヤレスLANコントローラ(WLC)を使用していて、http/httpサーバを無効にできません。どうしたらよいですか。

5.セキュリティアドバイザリで、この脆弱性を検出してブロックするSnortルールがあることを指摘しています。これらのルールがインストールされ、FTDで動作していることを確認するにはどうすればよいですか。

6. Cisco IOS XEを実行するCisco Unified Border Element(CUBE)を使用しています。http/httpsサーバを無効にできますか。

7. Cisco IOS XEを実行するCisco Unified Communications Manager Express(CME)を所有しています。http/httpsサーバを無効にできますか。

8. http/httpsサーバを無効にすると、Cisco DNA Centerでデバイスを管理する機能に影響しますか。

9.デバイスでHTTP/HTTPSサーバを無効にすると、スマートライセンスに影響しますか？

10. AAAが設定されていても、攻撃者はこの脆弱性を不正利用してローカルユーザを作成できますか。

11. CAサーバとしてルータを使用していて、HTTP/S ACLがすでにマシンIPをブロックするように設定されている場合、「curl」応答はどうなりますか。

12.ソフトウェア修正またはソフトウェアメンテナンスユニット(SMU)のアベイラビリティに関する情報はどこにありますか。

はじめに

このドキュメントは、Cisco IOS XEソフトウェアのWeb UIにおける権限昇格の脆弱性に関するCisco Technical Assistance Center(TAC)の技術FAQを示しています。 脆弱性に関するセキュリティアドバイザリとCisco Talosブログで詳細を確認できます。

概要

このドキュメントでは、ip http serverコマンドまたはip http secure-serverコマンドを無効にした場合の影響と、その結果として影響を受けるその他の機能について説明します。 また、機能を完全に無効にできない場合にwebuiへのアクセスを制限するために、アドバイザリで説明されているアクセスリストを設定する方法の例を示します。

1.　製品に影響はありますか。

この脆弱性の影響を受けるのは、バージョン16.x以降のCisco IOS XEソフトウェアを実行している製品だけです。 Nexus製品、ACI、従来型IOSデバイス、IOS XR、ファイアウォール(ASA/FTD)、ISEは影響を受けません。Identity Services Engineの場合は、http/httpsサーバを無効にすることによって、別の影響が生じる可能性があります。 「ISE」セクションを参照してください。

2.　使用している製品がCisco IOS XEを実行しているかどうかは、どのようにして確認できますか。

コマンドラインインターフェイス(CLI)からコマンドshow versionを実行すると、次のようなタイプのソフトウェアが表示されます。

スイッチ#show version

Cisco IOS XEソフトウェア、バージョン17.09.03

Cisco IOSソフトウェア[Cupertino]、C9800-CLソフトウェア(C9800-CL-K9_IOSXE)、バージョン17.9.3、リリースソフトウェア(fc6)

テクニカルサポート：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.Cisco IOS-XEソフトウェアの一部のコンポーネントは、GNU General Public License(「GPL」)バージョン2.0に基づいてライセンスされています。GPLバージョン2.0でライセンスされたソフトウェアコードは無償ソフトウェアであり、保証は一切付属しません。このようなGPLコードは、GPLバージョン2.0の条件に基づいて再配布または変更できます。詳細については、IOS-XEソフトウェアに付属のマニュアルまたは「ライセンス通知」ファイル、またはIOS-XEソフトウェアに付属のチラシに記載されている該当するURLを参照してください。

この脆弱性の影響を受けるのは、ソフトウェアバージョン16.x以降のみです。 該当するソフトウェアバージョンの例を次に示します。

16.3.5

16.12.4

17.3.5

17.6.1

17.9.4

該当しないIOS XEバージョンの例：

3.17.4秒

3.11.7E

15.6 ~ 1.S4

15.2 ~ 7.E7

を選択します。　Identity Services Engine(ISE)リダイレクトのユースケースを使用していて、http/httpsサーバを無効にできません。どうしたらよいですか。

ip http serverとip http secure-serverを無効にすると、次のようなユースケースが機能しなくなります。

- デバイスセンサーベースのプロファイリング
- ポスチャのリダイレクトと検出
- ゲストリダイレクト
- BYODオンボーディング
- MDMオンボーディング

WebUIへのアクセスを必要としないIOS XEデバイスでは、次のコマンドを使用してWebUIへのアクセスを防止し、ISEリダイレクトのユースケースを許可することをお勧めします。

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

Catalyst 9800コントローラなどでWebUIへのアクセスが必要な場合は、http access-class ACLを使用してWebUIへのアクセスを制限できます。https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-17/221107-filter-traffic-destin...

httpアクセスクラスACLでは、ISEリダイレクトのユースケースを機能させることができます。

4. C9800ワイヤレスLANコントローラ(WLC)を使用していて、http/httpサーバを無効にできません。どうしたらよいですか。

A4. ip http serverとip http secure-serverを無効にすると、次のような場合に使用できなくなります。
　　- WLC WebUIへのアクセス。これは、WebAdmin GUIへのアクセスにワイヤレス管理インターフェイス(WMI)、サービスポート、またはその他のSVIが使用されているかどうかを示します。

　　- Day 0セットアップウィザードが失敗します。
　　- Web認証 – WLC内部ページ、カスタムWeb認証ページ、ローカルWeb認証、中央Web認証

のいずれでゲストアクセスがリダイレクトされなくなる
- C9800-CLで自己署名証明書の生成が失敗する
- RESTCONFアクセス
- S3とCloudwatch
– ワイヤレスアクセスポイントでのIOXアプリケーションホスティング

これらのサービスを引き続き使用するには、次の手順を実行する必要があります。

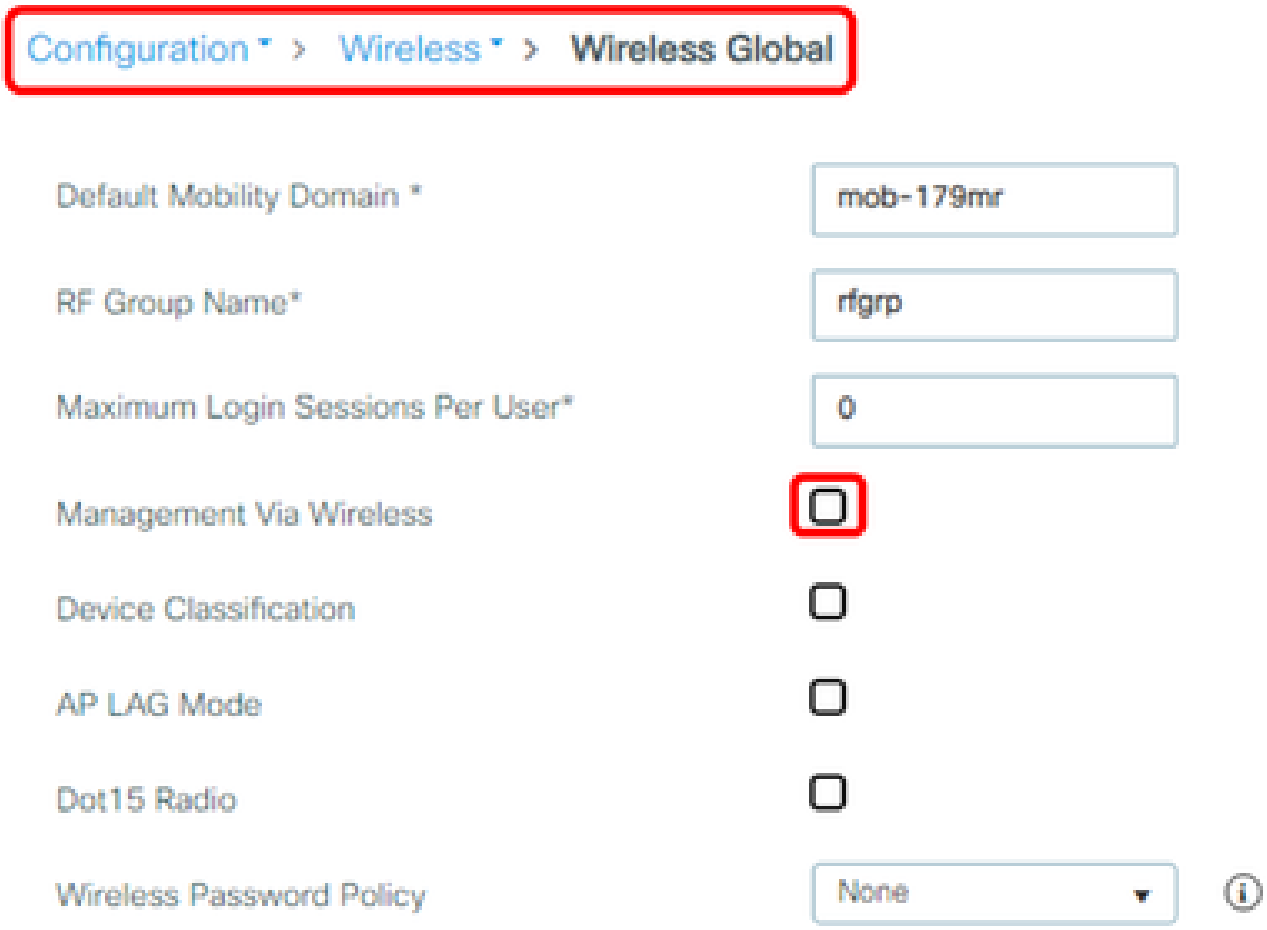
(1) HTTP/HTTPSを有効にする

(2) ACLを使用して、C9800 WLC Webサーバへのアクセスを、信頼できるサブネット/アドレスのみに制限する。
アクセスリストの設定の詳細については、次のドキュメントを参照してください。
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 にアクセスしてください。

注：
1. AireOS WLCには脆弱性はありません
2. Embedded Wireless on AP(EWC-AP)およびEmbedded Wireless on Switch(EWC-SW)を含むすべてのC9800(C9800-80、C9800-40、C9800-L、C9800-CL)に脆弱性が存在します
3. HTTP ACLは、C9800 WLC上のHTTPサーバへのアクセスのみをブロックします。WLCの内部ページ、カスタムWeb認証ページ、ローカルWeb認証、または中央Web認証のいずれを使用していても、WebAuthゲストアクセスには影響しません
4. HTTP ACLは、CAPWAP制御またはデータトラフィックにも影響しません。
5. guestなどの信頼できないネットワークがHTTP ACLで許可されていないことを確認します。

オプションで、ワイヤレスクライアントがWebAdmin GUIにアクセスするのを完全にブロックする場合は、「ワイヤレス経由の管理」が無効になっていることを確認します。

GUI：



CLI：

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

5. セキュリティアドバイザリで、この脆弱性を検出してブロックするSnortルールがあることを指摘しています。これらのルールがインストールされ、FTDで動作していることを確認するにはどうすればよいですか。

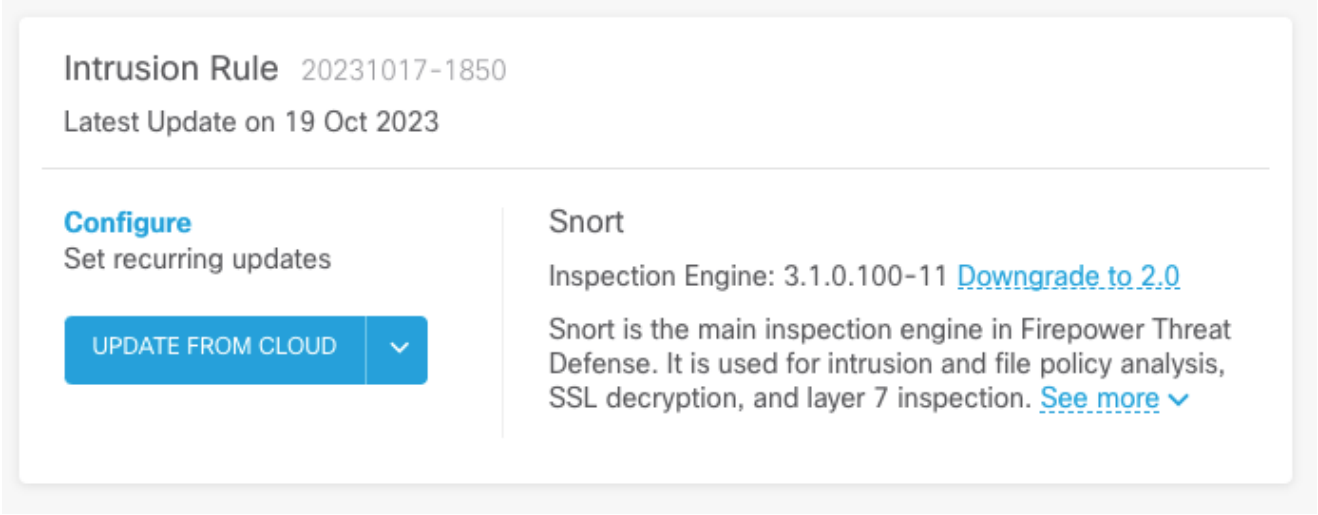
Snortルールがデバイスにインストールされていることを確認するには、LSP 20231014-1509またはSRU-2023-10-14-001がインストールされていることを確認します。これがインストールされているかどうかは、FDMおよびFMC管理対象デバイスで次のように異なります。

a.ルールがインストールされていることを確認します。

FDM

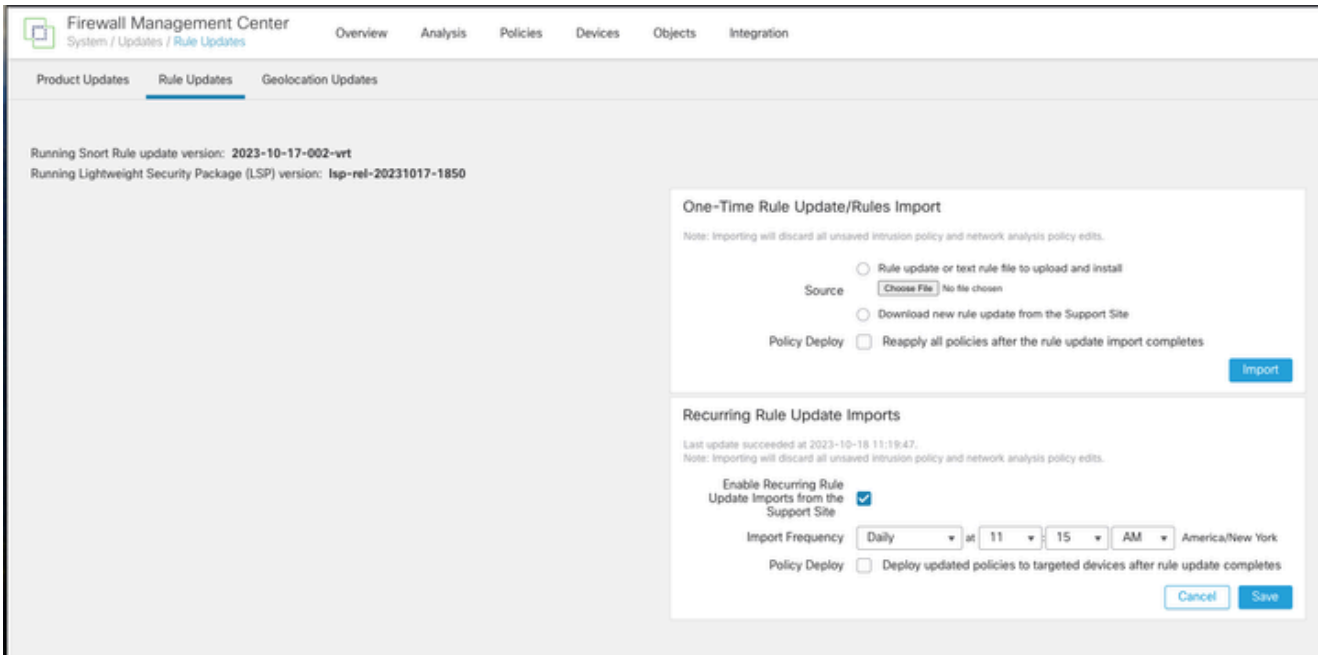
1. Device > Updates (View Configuration)に移動します。

2. 侵入ルールをチェックし、20231014-1509以降であることを確認します



FMC

1. System > Updates > Rule Updatesの順に移動します
2. Running Snort Rule Update(SRU)およびRunning Lightweight Security Package(LSP)をチェックし、LSP 20231014-1509またはSRU-2023-10-14-001以降が実行されていることを確認します。



b.侵入ポリシーでルールが有効になっていることを確認します。

侵入ポリシーがターロスの組み込みポリシー（セキュリティを介した接続、接続を介したセキュリティ、バランスのとれたセキュリティと接続）に基づいている場合、これらのルールは有効になり、既定でドロップするように設定されます。

Talosの組み込みポリシーのいずれかに基づいていない場合。侵入ポリシーでこれらのルールに対するルールアクションを手動で設定できるようにする必要があります。 詳細については、次のドキュメントを参照してください。

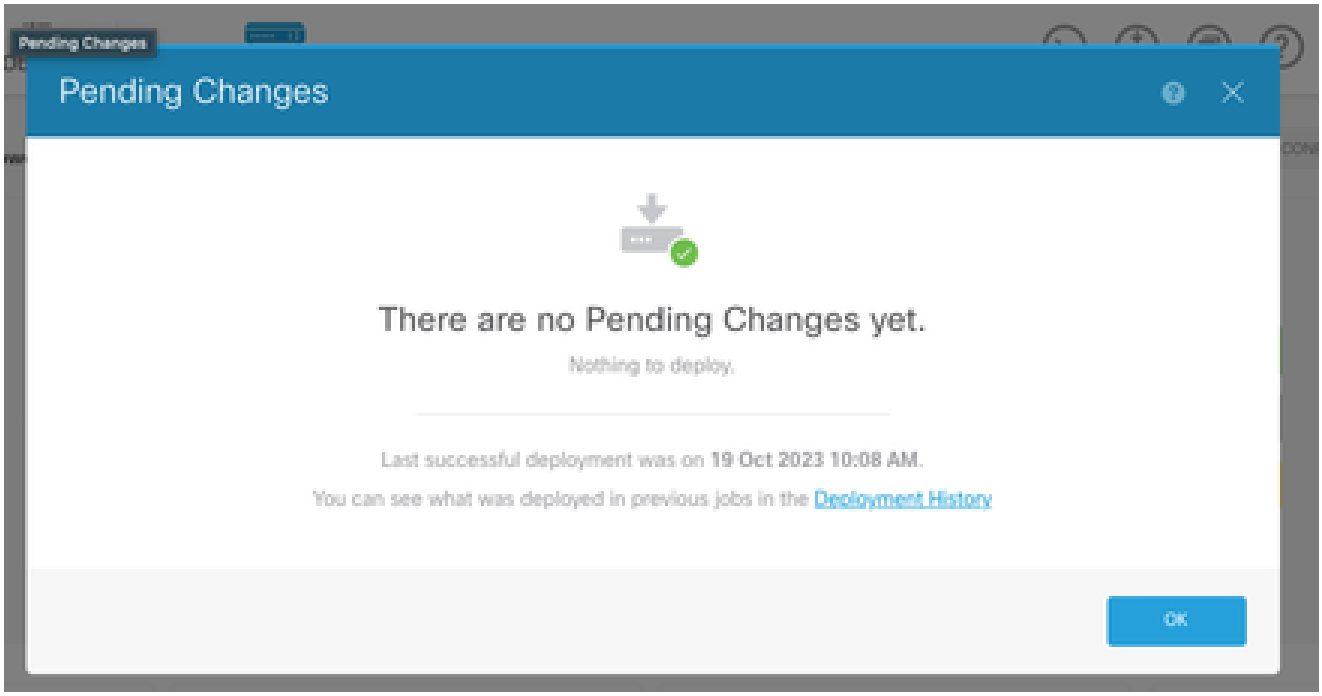
Snort 3: https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/snort/720/snort3-configuration-guide-v72/tuning-intrusion-policies.html#ID-2237-00000683_snort3

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. FTDデバイスにIPSポリシーが展開されていることを確認します。

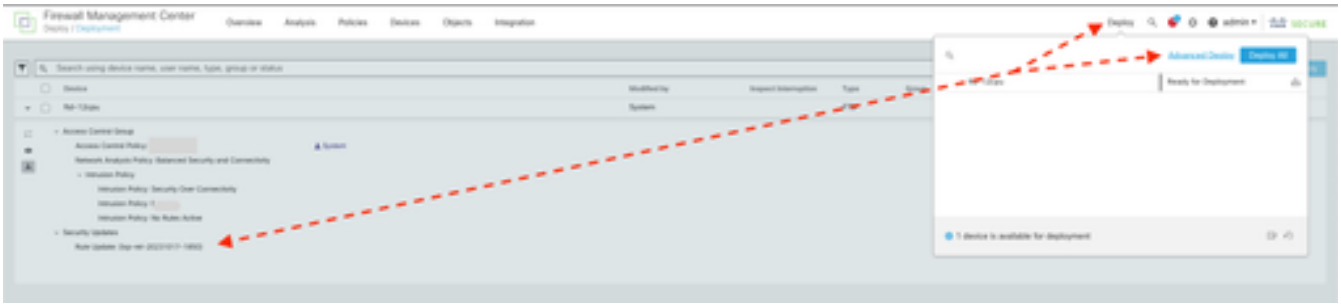
FDM

1. 展開アイコンをクリックします。
2. SRU/LSPに関連する保留中の変更がないことを確認します。



FMC

1. 「配備」 > 「拡張配備」の順にクリックします。
2. SRU/LSPに関連する保留中の展開がないことを確認します。



6. Cisco IOS XEを実行するCisco Unified Border Element(CUBE)を所有しています。http/httpsサーバを無効にできますか。

ほとんどのCUBE導入では、IOS XEにバンドルされているHTTP/HTTPSサービスを使用しないため、これを無効にしても機能に影響はありません。XMFベースのメディアフォーク機能を使用している場合は、アクセスリストを設定し、信頼できるホスト（CUCM/サードパーティのクライアント）だけを含むようにHTTPサービスへのアクセスを制限する必要があります。 ここで設定例を確認できます。

7. Cisco IOS XEを実行するCisco Unified Communications Manager Express(CME)を所有しています。http/httpsサーバを無効にできますか。

CMEソリューションは、ユーザディレクトリへのHTTPサービスと、登録済みIP電話への追加サービスを使用します。サービスを無効にすると、この機能は失敗します。アクセスリストを設定し、IP Phoneネットワークサブネットのみを含むようにHTTPサービスへのアクセスを制限する必要があります。ここで設定例を確認できます。

8. http/httpsサーバを無効にすると、Cisco DNA Centerでのデバイスの管理に影響しますか。

HTTP/HTTPSサーバを無効にしても、SDA(Software-Defined Access)環境を含め、Cisco DNA Centerで管理されているデバイスのデバイス管理機能や到達可能性には影響しません。HTTP/HTTPSサーバを無効にすると、アプリケーションホスティング機能、およびCisco DNA Centerのアプリケーションホスティング環境内で使用されているサードパーティ製アプリケーションに影響を与えます。これらのサードパーティアプリケーションは、通信と機能をHTTP/HTTPSサーバに依存する可能性があります。

9. デバイスでHTTP/HTTPSサーバを無効にすると、スマート

ライセンスに影響がありますか。

一般的に、Smart LicensingはHTTPSクライアント機能を使用するため、HTTP(S)サーバ機能を無効にしてもSmart Licensingの動作には影響しません。 スマートライセンスコミュニケーションが損なわれる唯一のシナリオは、CSLU外部アプリケーションまたはSSMオンプレミスが使用され、RESTCONFを使用してデバイスからRUMレポートを取得するように設定されている場合です。

10. AAAが設定されていても、攻撃者はこの脆弱性を不正利用してローカルユーザを作成できますか。

はい。使用する認証方式に関係なく、攻撃者がこの脆弱性を不正利用してローカルユーザを作成する可能性があると考えられます。クレデンシャルは、AAAシステムではなく、不正利用されたデバイスに対してローカルであることに注意してください。

11 . ルータをCAサーバとして使用していて、HTTP/S ACLがすでにマシンIPをブロックするように設定されている場合、「curl」応答はどうなるでしょうか。

'curl'応答は次のように403で禁止されています：

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

<html>

<head><title>403禁止</title></head>

<body bgcolor="white">

<h1>403禁止</h1>

<hr> nginx

</body>

</html>

12.ソフトウェア修正またはソフトウェアメンテナンスユニット(SMU)のアベイラビリティに関する情報はどこにありますか。

詳細については、「Cisco IOS XEソフトウェアWeb UIの特権昇格の脆弱性に対するソフトウェア修正プログラムの提供状況」ページを参照してください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。