Cisco IOS XE ソフトウェア Web UI 機能における複数の脆弱性

アドバイザリーID : cisco-sa-iosxe-webui-privesc-j22SaA4z
初公開日 : 2023-10-16 15:00
最終更新日 : 2023-11-01 15:44
バージョン 2.6 : Final
CVSSスコア : 10.0
回避策 : No workarounds available
Cisco バグ ID : CSCwh87343

CVE-2023-20198
CVE-2023-20273

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

シスコは、Cisco IOS XE ソフトウェアの Web UI 機能で観測されたエクスプロイトに関する進行中の調査の最新情報を提供しています。修正済みリリースのリストを更新し、ソフトウェアチェッカーを追加します。

修正情報については、このアドバイザリの「修正済みソフトウェア」のセクションを参照してください。

シスコの調査から、攻撃者がこれまで知られていなかった 2 つの問題をエクスプロイトしていることが判明しました。

攻撃者は、最初に CVE-2023-20198 をエクスプロイトして初期アクセス権を取得し、特権 15 のコマンドを発行してローカルユーザーとパスワードの組み合わせを作成しました。これにより、ユーザーは通常のユーザーアクセス権でログインできるようになりました。

次に、攻撃者は Web UI 機能の別のコンポーネントをエクスプロイトし、新しいローカルユーザーを利用して権限を root に昇格させ、ファイルシステムにインプラントを書き込みました。シスコはこの問題に CVE-2023-20273 を割り当てました。

- CVE-2023-20198 に割り当てられた CVSS スコアは 10.0 です。
- CVE-2023-20273 に割り当てられた CVSS スコアは 7.2 です。

これらの CVE は両方とも CSCwh87343 によって追跡されています。

これらの脆弱性の攻撃ベクトルを封じる手順については、このアドバイザリの「推奨事項」セク

ションを参照してください。

このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

該当製品

脆弱性のある製品

これらの脆弱性は、Web UI 機能が有効になっている場合、Cisco IOS XE ソフトウェアに影響を与えます。Web UI 機能は、ip http server コマンドまたは ip http secure-server コマンドによって有効化されます。

HTTP サーバ設定の確認

システムで HTTP サーバー機能が有効になっているかどうかを確認するには、そのシステムにログインし、CLI で show running-config | include ip http server|secure|active コマンドを使用して、グローバル コンフィギュレーションに ip http server コマンドまたは ip http secure-server コマンドがあるかどうかを確認します。どちらかのコマンドが含まれている場合は、HTTP サーバー機能が有効になっています。

以下に、show running-config | include ip http server|secure|active コマンドの出力を示しています。

```
<#root>

Router#

show running-config | include ip http server|secure|active


ip http server
ip http secure-server
```

注：システム設定に、これらのコマンドのいずれかまたは両方が含まれている場合は、Web UI 機能が有効になっています。

ip http server コマンドが存在し、設定に ip http active-session-modules none も含まれている場合、これらの脆弱性が HTTP 経由でエクスプロイトされることはありません。

Ip http secure-server コマンドが存在し、設定に ip http secure-active-session-modules none が含まれている場合、これらの脆弱性が HTTPS 経由でエクスプロイトされることはありません。

脆弱性を含んでいないことが確認された製品

シスコは、これらの脆弱性が次のシスコ製品に影響を与えないことを確認しました。

- 適応型セキュリティ アプライアンス（ASA）ソフトウェア
- Firepower Threat Defense（FTD）ソフトウェア
- Identity Services Engine（ISE）
- IOS ソフトウェア
- リリース 16 より前の IOS XE ソフトウェア
- NX-OS ソフトウェア

詳細

Web UI は組み込み GUI ベースのシステム管理ツールです。システムをプロビジョニングしたり、システムの導入および管理性を簡素化したり、ユーザー体験を向上させたりする機能を提供します。デフォルトのイメージが用意されているため、何かを有効にしたりシステムにライセンスをインストールしたりする必要はありません。Web UI を使用すれば、CLI の専門知識がなくても、設定を構築し、システムのモニタリングとトラブルシューティングを行うことができます。

セキュリティ侵害の痕跡

システムが侵害された可能性があるかどうかを判断するには、以下のチェックを実行します。

システムログをチェックして、「user」が「cisco_tac_admin」、「cisco_support」、またはネットワーク管理者が認識していないローカルユーザーに設定されている ログメッセージがないか確認します。

```
<#root>

%SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as

user

 on line

%SEC_LOGIN-5-WEBLOGIN_SUCCESS: Login Success [user:

user

] [Source: source_IP_address] at 03:42:13 UTC Wed Oct 11 2023
```

注：ユーザーが Web UI にアクセスしたインスタンスごとに、%SYS-5-CONFIG_P メッセージがログに表示されます。このメッセージに新しいユーザー名または不明なユーザー名が含まれていないか確認してください。

システムのログで次のメッセージをチェックし、filename が、ファイルのインストール時の通常

の操作に関連していない不明なファイル名でないかどうかを確認します。

<#root>

%WEBUI-6-INSTALL_OPERATION_INFO: User: *username*, Install Operation: ADD

filename

Cisco Talos では、インプラントの存在を確認するために次のコマンドを提供しています。ここで、「systemip」は、チェックするシステムの IP アドレスです。このコマンドは、チェックするシステムにアクセスできるワークステーションから発行する必要があります。

<#root>

curl -k -H "Authorization: 0ff4fbf0ecffa77ce8d3852a29263e263838e9bb" -X POST "https://

systemip

/webui/logoutconfirm.html?logon_hash=1"

要求によって 0123456789abcdef01 などの 16 進数文字列が返される場合、インプラントが存在します。

注：上記のコマンドは、単一のコマンドラインとして入力する必要があります。

注：システムが HTTP アクセス専用に設定されている場合は、コマンドの例で HTTP スキームを使用してください。

エクスプロイトを検出するために次の Snort ルール ID も使用できます。

- 3:50118：インプラントの初期挿入のアラート（CVE-2023-20273）
- 3:62527：インプラントの相互作用のアラート
- 3:62528：インプラントの相互作用のアラート
- 3:62529：インプラントの相互作用のアラート
- 3:62541：初期アクセスのエクスプロイト試行に関するアラート（CVE-2023-20198）
- 3:62542：初期アクセスのエクスプロイト試行に関するアラート（CVE-2023-20198）

回避策

これらの脆弱性に対処する回避策はありません。

HTTP サーバ機能を無効にすると、こうした脆弱性に対する攻撃ベクトルが排除されるため、対象デバイスのアップグレードが可能になるまでの適切な対応策となる可能性があります。管理者は、グローバル コンフィギュレーション モードで no ip http server または no ip http secure-

Server コマンドを使用して、HTTP サーバ機能を無効にすることができます。HTTP サーバと HTTP セキュア サーバの両方が使用されている場合、HTTP サーバ機能を無効にするには両方のコマンドが必要です。

HTTP サーバへのアクセスを信頼できるネットワークのみに制限することで、これらの脆弱性のリスクが限定的になります。次の例は、信頼できる 192.168.0.0/24 ネットワークから HTTP サーバへのリモートアクセスを許可する方法を示しています。

```
!
ip http access-class 75
ip http secure-server
!
access-list 75 permit 192.168.0.0 0.0.0.255
access-list 75 deny   any
!
```

注：Cisco IOS XE ソフトウェアの新しいバージョンでアクセスリストを適用する場合、前述の例では ip http access-class ipv4 75 コマンドを使用します。詳細情報については、「アクセスリストを使用した Cisco IOS XE デバイス WebUI 宛てのトラフィックのフィルタ処理」を参照してください。

この緩和策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

修正済みソフトウェア

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ

ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

Cisco.com の シスコサポート & ダウンロードページには、ライセンスとダウンロードに関する情報が記載されています。このページには、[マイデバイス（My Devices）] ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。

ソフトウェアのアップグレードを検討する際には、シスコ セキュリティ アドバイザリ ページで入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける可能性とアップグレード ソリューション一式を確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）に連絡してアップグレードを入手してください。

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

次の表に示すように、該当する修正済みのソフトウェア リリースにアップグレードすることをお勧めします。

Cisco IOS XE ソフトウェア リリース トレイン	First Fixed Release（修正された最初のリリース）	Available
17.9	17.9.4a	Yes
17.6	17.6.6a	Yes
17.3	17.3.8a	Yes
16.12（Catalyst 3650 および 3850 のみ）	16.12.10a	Yes

次の表の SMU は、Cisco Bug ID CSCwh87343 に対応しています。

Cisco IOS XE ソフトウェア リリース トレイン	基本リリース	SMU が利用可能
17.9	17.9.4	Yes
17.6	17.6.5	Yes

プラットフォームのリリース情報の詳細については、「Cisco IOS XE ソフトウェア Web UI 特権昇格の脆弱性に対するソフトウェア修正の提供状況 - CVE-2023-20198」を参照してください。

Cisco IOS および IOS XE ソフトウェア

お客様が Cisco IOS ソフトウェアおよび IOS XE ソフトウェアの脆弱性による侵害の可能性を判断できるように、シスコは Cisco Software Checker を提供しています。このツールを使うことで、特定のソフトウェアリリースに関連するすべてのシスコ セキュリティ アドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース（「First Fixed」）を特定できます。また、該当する場合には、Software Checker により判別されたすべてのアドバイザリに記載のすべての脆弱性が修正された最初のリリース（「Combined First Fixed」）を特定できます。

このツールを使用するには、「Cisco Software Checker」ページの手順に従います。あるいは、次のフォームを使用して、シスコ セキュリティ アドバイザリに該当するリリースであるかどうかを確認します。このフォームを使用するには、次の手順に従います。

1. ツールで検索するアドバイザリを選択します。このアドバイザリのみ、セキュリティ影響評価（SIR）が「重大」または「高」のアドバイザリのみ、すべてのアドバイザリのいずれかです。
2. リリース番号（15.9(3)M2、17.3.3 など）を入力します。
3. [チェック（Check）] をクリックします。

2 | Critical,High,Medium | このアドバイザのみ

Enter release number | Check

Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデント レスポンス チーム）は、このアドバイザリに記載されている該当するリリース情報と修正されたリリース情報のみを検証します。

推奨事項

シスコはインターネットに面したすべてのシステムで HTTP サーバー機能を無効にすること、または、信頼できる送信元アドレスへのアクセスを制限することを強く推奨しています。HTTP サーバ機能を無効にするには、グローバル コンフィギュレーション モードで no ip http server また

は no ip http secure-server コマンドを使用します。HTTP サーバーと HTTPS サーバーの両方を使用している場合、HTTP サーバー機能を無効にするには、両方のコマンドが必要です。

以下の指針が対応策適用の判断に役立ちます:

- IOS XE を実行していますか。
  - いいえ。 システムには脆弱性はありません。追加の対応は不要です。
  - はい。ip http server または ip http secure-server が設定されていますか。
    - いいえ。 これらの脆弱性をエクスプロイトできません。追加の対応は不要です。
    - はい。HTTP/HTTPS 通信を必要とするサービス (eWLC など) を実行していますか。
      - いいえ。 HTTP サーバー機能を無効にしてください。
      - はい。可能であれば、HTTP/HTTPS サービスへのアクセスを信頼できるネットワークからだけに制限してください。

シスコは HTTP/HTTPS Server 機能にアクセスリストを適用して信頼されていないホストやネットワークからのアクセスを制限することが、有効な緩和策であると評価しています。

これらのサービスに対してアクセス制御を実施する場合、HTTP/HTTPS サービスが中断される可能性があるため、必ず設定を見直してください。これらの手順が不明な場合は、サポート組織と協力して適切な制御手法を決定してください。

設定変更後には、copy running-configuration startup-configuration コマンドを使用して、変更内容を保存してください。システムの再起動後にも設定変更内容を維持できます。

HTTP サーバー機能を無効にした場合の影響の詳細については、「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 TAC テクニカル FAQ - CVE-2023-20198」を参照してください。

不正利用事例と公式発表

シスコでは、これらの脆弱性が実際にエクスプロイトされたことを認識しています。

出典

これらの脆弱性は、複数の Cisco TAC サポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

改訂履歴

バージョン	説明	セクション	ステータス	日付
2.6	脆弱性を含んでいないことが確認された製品のリストを更新。	該当製品	Final	2023 年 11 月 1 日
2.5	これらの変更を反映するために、修正済みリリースの表を更新。また、ソフトウェアチェッカーを追加し、概要を更新。	概要および修正済みソフトウェア	Final	2023 年 10 月 31 日
2.4	追加の修正済みリリースを示すために概要を更新。また、修正済みリリースの表を更新。	修正済みソフトウェアの概要	Interim	2023 年 10 月 30 日
2.3	追加の修正済みリリースを示すために概要を更新。修正済みリリースの表と SMU テーブルを更新。技術的な FAQ へのリンクを追加するために推奨事項を更新。	要約, 修正済みソフトウェア, 推奨事項	Interim	2023 年 10 月 27 日
2.2	脆弱性が含まれないことが確認された製品の変更を示すために概要を更新。脆弱性が存在しない製品のリストを更新。SMU テーブルの内容を更新。	概要、影響を受ける製品、修正済みソフトウェア	Interim	2023 年 10 月 26 日
2.1	SMU の可用性を示すために概要を更新。SMU の可用性テーブルにより修正済みソフトウェアを更新。	修正済みソフトウェアの概要	Interim	2023 年 10 月 26 日
2.0	拡張検出が利用可能であることを示すために概要を更新。拡張検出コマンドにより侵害の兆候を更新。	概要、侵害の兆候	Interim	2023 年 10 月 23 日
1.4	最初の修正が利用可能であることを示すために概要を更新。固有の修正済みリリースに関する情報を追加。	修正済みソフトウェアの概要	Interim	2023 年 10 月 22 日
1.3	CVE-2023-20273 を追加。観測された攻撃に関する情報を追加。リスク緩和に関する説明を追加。Snort ルール ID を更新。	概要、影響を受ける製品、詳細、侵害の兆候、回避策、および推奨事項	Interim	2023 年 10 月 20 日
1.2	アクセスリストによる緩和策を追加。	推奨事項	Interim	2023 年 10 月 17

バージョン	説明	セクション	ステータス	日付
				日
1.1	トリアージ意思決定ツリーを追加。	推奨事項	Interim	2023 年 10 月 16 日
1.0	初回公開リリース	—	Interim	2023 年 10 月 16 日

利用規約

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。