Cisco IOS XE ソフトウェアの Web UI で発見されたコマンド インジェクションの脆弱性

アドバイザリーID : cisco-sa-webui-cmdij-FzZAeXAy
CVE-2023-20231
初公開日 : 2023-09-27 16:00
バージョン 1.0 : Final
CVSSスコア : 8.8
回避策 : No workarounds available
Cisco バグ ID : CSCwe12578

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

Cisco IOS XEソフトウェアのWeb UIの脆弱性により、認証されたリモート攻撃者が該当デバイスに対してインジェクション攻撃を実行する可能性があります。

この脆弱性は、不十分な入力検証に起因します。攻撃者は、巧妙に細工された入力を Web UI に送信することにより、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者はレベル15の特権で任意のCisco IOS XEソフトウェアCLIコマンドを実行できる可能性があります。

注:この脆弱性は、攻撃者がLobby Ambassadorアカウントのクレデンシャルを取得した場合にのみ不正利用できます。このアカウントはデフォルトでは設定されていません。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。この脆弱性に対処する回避策はありません。

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-webui-cmdij-FzZAeXAy

このアドバイザリは、Cisco IOSおよびIOS XEソフトウェアのセキュリティアドバイザリバンドル公開の2023年9月リリースの一部です。アドバイザリとリンクの一覧については、『Cisco Event Response: September 2023 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication』を参照してください。

該当製品

脆弱性のある製品

この脆弱性は、Cisco IOS XEソフトウェアの脆弱性が存在するリリースを実行し、Lobby Ambassadorアカウントを有効にし、HTTPサーバ機能を有効にしている次のシスコ製品に影響を与えます。

- Catalyst 9300 シリーズ スイッチ
- Catalyst 9400 シリーズ スイッチ
- Catalyst 9500 シリーズ スイッチ
- クラウド向け Catalyst 9800-CL ワイヤレスコントローラ
- Catalyst 9300、9400、9500 シリーズ スイッチ用 Catalyst 9800 組み込みワイヤレスコントローラ
- Catalyst 9100Xシリーズアクセスポイントの組み込みワイヤレスコントローラ

脆弱性が存在する Cisco ソフトウェアリリースについては、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。

デバイス設定の確認

ロビーアンバサダーアカウントとHTTPサーバ機能がデバイスで設定されているかどうかを確認するには、次の手順を使用します。

ロビーアンバサダーアカウント設定の決定

デバイスで設定されているLobby Ambassadorアカウントの数を確認するには、デバイスにログインしてshow running-config | count type lobby-admin CLIコマンドを使用します。次の例は、1つのLobby Ambassadorアカウントが設定されているデバイスでのCLI出力を示しています。

<#root>

```
Router#
show running-config | count type lobby-admin

Number of lines which match regexp = 1
```

行の最後の数字は、デバイスで設定されているLobby Ambassadorアカウントの数を示します。

注：Lobby Ambassadorロールは、RADIUSまたはTACACS+を使用してユーザアカウントに関連付けることができます。Cisco Identity Services Engine(ISE)などの認証、許可、アカウンティング(AAA)サーバを使用して、デバイスにアクセスするユーザアカウントを管理しているお

客様は、cisco-av-pair=lobby-admin属性が設定されたユーザの存在を確認する必要があります。Cisco ISEでLobby Ambassadorアカウントを設定する方法の例については、「RADIUSおよびTACACS+認証での9800 WLC Lobby Ambassadorの設定」を参照してください。

HTTP サーバ設定の確認

あるデバイスで HTTP サーバが有効かどうかを判断するには、デバイスにログインし、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。 | | 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コマンドが含まれるかどうかを確認します。どちらかのコマンドが存在する場合は、そのデバイスに対してHTTPサーバ機能が有効になっています。

以下に、show running-config | include ip http server|secure|activeコマンドを実行します。

<#root>

```
Router#
show running-config | include ip http server|secure|active


ip http server
ip http secure-server
```

注：デバイス設定にコマンドまたはその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、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、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。

Cisco IOS XEソフトウェアは、デバイスにLobby Ambassadorアカウントが設定されている場合にのみ、この脆弱性の影響を受けます。これはデフォルト設定ではないため、管理者が追加する必要があります。

脆弱性を含んでいないことが確認された製品

このアドバイザリの脆弱性のある製品セクションに記載されている製品のみが、この脆弱性の影響を受けることが分かっています。

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- IOS ソフトウェア
- IOS XR ソフトウェア
- Meraki 製品
- NX-OS ソフトウェア

回避策

この脆弱性に対処する回避策はありません。

ただし、管理者はLobby Ambassadorアカウントを無効にして、この脆弱性に対する攻撃ベクトルを排除できます。

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。

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

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）は、本アドバイザリに記載されている脆弱性の不正利用事例やその公表を確認していません。

出典

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-cmdij-FzZAeXAy

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2023年9月27日

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

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。