Critical

アドバイザリーID : cisco-sa-iosxe-webui-privesc-j22SaA4z CVE-2023-20198 Download CVRF Email
初公開日 : 2023-10-16 15:00
最終更新日 : 2023-10-17 12:18
バージョン 1.2 : Interim
CVSSスコア : 10.0
回避策 : No workarounds available
Cisco バグ ID : CSCwh87343

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

シスコでは、インターネットや信頼できないネットワークに接続された場合に、Cisco IOS XEソフトウェアのWeb UI機能のこれまで知られていなかった脆弱性が積極的に悪用されることを認識しています。この脆弱性により、リモートの認証されていない攻撃者が、特権レベル15のアクセス権を持つアカウントを該当システムに作成できます。攻撃者はそのアカウントを使用して、該当システムの制御を取得できます。

この脆弱性に対する攻撃ベクトルを閉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

シスコは、この調査のステータスおよびソフトウェアパッチが入手可能になった時点でアップデートを提供します。

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

Web UI機能が有効になっている場合、この脆弱性は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**または**ip http secure-server**コマンドを使用して有効にします。

HTTP サーバ設定の確認

HTTPサーバ機能がシステムで有効になっているかどうかを確認するには、システムにログインして**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存在する場合は、HTTPサーバ機能がシステムに対して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ます。

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

注 : システム設定にコマンドまたは両方のコマンド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。

詳細

Web UIは組み込みのGUIベースのシステム管理ツールで、システムのプロビジョニング、システムの導入と管理の簡素化、およびユーザエクスペリエンスの向上を実現します。デフォルトイメージが付属しているため、システム上で何も有効にしたり、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を使用すると、CLIの専門知識がなくても、構成を構築したり、システムの監視やトラブルシューティングを行うことができます。

Web UIおよび管理サービスは、インターネットや信頼できないネットワークに公開しないでください。

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確認するには、次のチェックを実行します。

システムログを調べ、次のログメッセージのいずれかが存在するかどうかを確認します。ここで、***user***には、**cisco_tac_admin**、**cisco_support**、またはネットワーク管理者が知らない設定済みのローカルユーザを指定できます。

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

%SEC_LOGIN-5-WEBLOGIN_SUCCESS: Login Success [user: user] [Source: source_IP_address] at 03:4
```

注:%SYS-5-CONFIG_Pメッセージは、ユーザがWeb UIにアクセスしたインスタンスごとに表示されます。検索するインジケータは、メッセージに存在する新規または不明なユーザ名です。

システムログを調べて、次のメッセージを確認します。ここで、***filename***は、予想されるファイルインストールアクションと相関しない未知のファイル名です。

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

Cisco Talosは次のコマンドを提供して、インプラントの存在を確認しています。ここで、***systemip***は確認するシステムのIPアドレスです。このコマンドは、対象の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。

```
curl -k -X POST "https://systemip/webui/logoutconfirm.html?logon_hash=1"
```

要求が16進数文字列を返す場合、インプラントは存在します。

注：システムがHTTPアクセス専用に設定されている場合は、コマンド例のHTTP方式を使用します。

不正利用を検出するには、次のSnortルールIDも使用できます。

- 3:50118:2 – 最初のインプラント注射を警告できる
- 3:62527:1 – インプラントの相互作用に関するアラートを通知できる
- 3:62528:1 – インプラントの相互作用に関するアラートを通知できる
- 3:62529:1 – インプラントの相互作用に関するアラートを通知できる

回避策

この脆弱性に対処する回避策はありません。

不正利用事例と公式発表

シスコは、この脆弱性が活発に悪用されていることを認識しています。

出典

この脆弱性は、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
1.2	アクセスリストの緩和策を追加。	推奨事項	Interim	2023-OCT-17
1.1	トリアージ決定ツリーを追加。	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

クイックリンク