Cisco IOS XEソフトウェアのWebベース管理インターフェイスの脆弱性

Medium

アドバイザリーID : cisco-sa-webui-multi-ARNHM4v6
初公開日 : 2025-05-07 16:00
バージョン 1.0 : Final
CVSSスコア : 6.5
回避策 : No workarounds available
Cisco バグ ID : CSCwk16979 CSCwk23580 CSCwk25133

CVE-2025-20193
CVE-2025-20194
CVE-2025-20195

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ベースの管理インターフェイスにおける複数の脆弱性により、リモート攻撃者が基盤となるオペレーティングシステムからファイルを読み取ったり、設定ファイルの一部を読み取ったり、syslogをクリアしたり、クロスサイトリクエストフォージェリ(CSRF)攻撃を実行したりできる可能性があります。

これらの脆弱性の詳細については本アドバイザリの「詳細情報」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-webui-multi-ARNHM4v6

このアドバイザリは、2025年5月に公開されたCisco IOSソフトウェアおよび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の一部です。これらのアドバイザリとリンクの一覧については、『シスコイベントレスポンス：Cisco IOSおよびIOS XEソフトウェアに関するセキュリティアドバイザリ公開資料（半年刊、2025年5月）』を参照してください。

該当製品

脆弱性のある製品

公開時点で、Webベースの管理インターフェイスが有効になっているCisco IOS XEソフトウェアは、これらの脆弱性の影響を受けました。

注：Webベースの管理インターフェイスをイネーブルにするには、ip http serverまたはip http secure-serverコマンドを使用します。

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。

HTTP サーバ設定の確認

HTTPサーバ機能がデバイスで有効になっているかどうかを確認するには、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コマンドが存在す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です。

次の例は、HTTPサーバ機能が有効になっているデバイスでの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：デバイス設定にどちらかの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ベースの管理インターフェイス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 が含まれている場合、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も含まれている場合、この脆弱性はHTTPSでは不正利用できません。

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、これら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。

- 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

詳細

これらの脆弱性は依存関係にはなく、いずれかの脆弱性をエクスプロイトするために別の脆弱性をエクスプロイトする必要はありません。さらに、いずれかの脆弱性の影響を受けるソフトウェアリリースであっても、他の脆弱性の影響は受けない場合があります。

脆弱性の詳細は以下のとおりです。

CVE-2025-20193:Cisco IOS XEソフトウェアの情報開示の脆弱性

Cisco IOS XEソフトウェアのWebベース管理インターフェイスにおける脆弱性により、認証された低特権のリモート攻撃者が、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ベースの管理インターフェイス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、攻撃者は基盤となるオペレーティングシステムからファイルを読み取る可能性があります。

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。

バグID: CSCwk16979
CVE ID：CVE-2025-20193
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.5
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

CVE-2025-20194:Cisco IOS XEソフトウェアのコマンドインジェクションの脆弱性

Cisco IOS XEソフトウェアのWebベース管理インターフェイスにおける脆弱性により、認証された低特権のリモート攻撃者が、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ベースの管理インターフェイス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、攻撃者は基盤となるオペレーティングシステムから限定されたファイルを読み取ったり、該当デバイスのsyslogおよびライセンスログをクリアしたりできる可能性があります。

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。

バグID: CSCwk25133
CVE ID：CVE-2025-20194
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.4
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

CVE-2025-20195:Cisco IOS XEソフトウェアのWebベース管理インターフェイスにおけるCSRFの脆弱性

Cisco IOS XEソフトウェアのWebベース管理インターフェイスにおける脆弱性により、認証されていないリモートの攻撃者が、該当デバイスのCLIでCSRF攻撃を実行し、コマンドを実行する可能性があります。

この脆弱性は、該当デバイス上の Web ベース管理インターフェイスの CSRF 保護が不十分なことに起因します。攻撃者は、認証済みユーザーを、巧妙に細工されたリンクにアクセスするように誘導することで、この脆弱性をエクスプロイト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、該当デバイスのsyslog、パーサー、およびライセンスのログをクリアする権限を持つユーザにこれらのログをクリアされる可能性があります。

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。

バグID: CSCwk23580
CVE ID：CVE-2025-20195
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：4.3
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N

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。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コマンドまたは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。

信頼できるネットワークだけにHTTPサーバへのアクセスを許可すると、これらの脆弱性による影響を制限できます。次の例は、信頼できる 192.168.10.0/24 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 ipv4 restrict_ipv4_webui
!
ip access-list standard restrict_ipv4_webui
permit 192.168.10.0 0.0.0.255
!
```

詳細については、「アクセスリストを使用してCisco IOS XEデバイスWebUI宛てのトラフィックをフィルタリングする」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

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完全なアップグレード ソリューション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。

Cisco IOS および IOS XE ソフトウェア

お客様が Cisco IOS 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（例：15.9(3)M2、17.3.3）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）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例とその公表は確認しておりません。

出典

この脆弱性は、シスコ内部でのシステム 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-multi-ARNHM4v6

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	2025年5月7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。