

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-cmdinj- [CVE-2025-gVn3OKNC](#) [20186](#)

初公開日 : 2025-05-07 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 : [CSCwk27168](#)

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ソフトウェアのワイヤレスLANコントローラ(WLC)機能のWebベース管理インターフェイスにおける脆弱性により、lobby ambassadorユーザアカウントを持つ認証されたリモート攻撃者が、該当デバイスに対してコマンドインジェクション攻撃を実行でき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、攻撃者は特権レベル15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:この脆弱性を不正利用できるのは、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のみです。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。

このアドバイザリーは、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-cmdinj-gVn3OKNC>

このアドバイザリーは、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ーバンドルの一部です。これらのアドバイザリー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](#)』

[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

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アカウントとHTTPサーバ機能の両方が有効になっている次のシスコ製品に影響を与えます。

- 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 9800 シリーズ 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
- サービス統合型ルータ(ISR)1100(Wi-Fi 6)にアクセスポイント(AP)を内蔵
- Catalyst IR1800高耐久性シリーズルータ用Wi-Fi 6着脱可能モジュール

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

Cisco IOS XEソフトウェアがこの脆弱性の影響を受けるのは、該当デバイスにlobby ambassadorアカウントが設定されている場合のみです。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。Lobby AmbassadorアカウントとHTTPサーバ機能がデバイスに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 アカウント設定の確認

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コマンドを実行します。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
```

行末の数値は、デバイスで設定されているロビー アンバサダー アカウントの数を示しています。この数値がゼロで、デバイスが認証、認可、アカウントティング(AAA)を使用していない場合、この脆弱性の影響を受けません。

注：lobby ambassadorルールは、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属性が設定されている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+認証による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

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 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 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](#)にリストされている製品だけがこの脆弱性の影響を受けることが知られています。

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
- WLC AireOS 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、管理者はこの脆弱性に対する攻撃ベクトルを排除するためにlobby ambassadorアカウントを無効にすることができます。

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することになります。

<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です。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。

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 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) 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-cmdinj-gVn3OKNC>

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、単独の転載や意識を施した場合、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。