Cisco IOSおよびIOS XEソフトウェアのCLIにおけるDenial of Service(DoS)の脆弱性

Medium

アドバイザリーID : cisco-sa-ios-cli-EB7cZ6yO
初公開日 : 2025-09-24 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 : CSCwm86360

CVE-2025-20149

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ソフトウェアおよびCisco IOS XEソフトウェアのCLIの脆弱性により、認証されたローカル攻撃者が該当デバイスの予期しないリロードを引き起こし、その結果、サービス妨害(DoS)状態が発生する可能性があります。

この脆弱性は、バッファオーバーフローが原因です。権限の低いアカウントを持つ攻撃者が、CLIプロンプトで巧妙に細工されたコマンドを使用することにより、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者は該当デバイスのリロードを引き起こし、その結果 DoS 状態が発生す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。

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-ios-cli-EB7cZ6yO

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2025年9月リリースの一部です。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9月）』を参照してください。

該当製品

脆弱性のある製品

shell processing fullコマンドが設定されている場合、この脆弱性はCisco IOSソフトウェアおよびIOS XEソフトウェアに影響を与えます。このコマンドは、デフォルトで無効になっています。

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。

デバイス設定の確認

デバイスでshell processing fullコマンドが設定されているかどうかを確認するには、デバイスにログインしてCLIでshow run | include shellコマンドを使用します。このコマンドで出力が生成されない場合、デバイスは影響を受けません。

次に、shell processing fullが設定されているデバイスでのshow run | include shellコマンドの出力例を示します。

```
Switch#show run | include shell
shell processing full
```

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 XR ソフトウェア
- 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。

shell processing fullコマンドを削除することで、この脆弱性に対する攻撃ベクトルを排除できます。この脆弱性は、該当するデバイスがアップグレードされるまでの適切な緩和策となる可能性があります。shell processing fullコマンドを削除するには、グローバルコンフィギュレーションモードでno shell processing fullコマンドを使用します。

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

シスコでは、修正済みソフトウェアリリースへのアップグレードが利用可能になるまで、回避策や緩和策は一時的な解決策であると考えています。この脆弱性を完全に修復し、本アドバイザリで説明されている障害の発生を回避するために、お客様には本アドバイザリで説明されている修正済みソフトウェアにアップグレードすることを強く推奨します。

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、このアドバイザリで説明されている脆弱性に対して概念実証段階のエクスプロイトコードが入手可能であることを認識しています。

このアドバイザリで説明されている脆弱性の悪用に関する情報は Cisco PSIRT に寄せられていません。

出典

この脆弱性は、Cisco Technical Assistance Center(TAC)の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-ios-cli-EB7cZ6yO

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9月24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。