

Cisco IOS XEソフトウェアの補助非同期ポートにおけるDoS脆弱性



アドバイザリーID : cisco-sa-aux-333WBz8f [CVE-2024-](#)

初公開日 : 2024-03-27 16:00

[20309](#)

バージョン 1.0 : Final

CVSSスコア : [5.6](#)

回避策 : Yes

Cisco バグ ID : [CSCwh47363](#)

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ソフトウェアの補助非同期ポート(AUX)機能の脆弱性により、認証されたローカル攻撃者が該当デバイスのリロードまたは応答停止を引き起こす可能性があります。

この脆弱性は、フロー制御ハードウェアがAUXポートで有効になっている場合の特定の入力トラフィックの不適切な処理に起因します。攻撃者は、AUXポートにリバースTelnetし、接続後に特定のデータを送信することで、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、攻撃者はデバイスをリセットまたは応答を停止させ、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。

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。本脆弱性に対処する回避策がいくつかあります。

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-aux-333WBz8f>

このアドバイザリーは、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ーバンドル公開の2024年3月リリースの一部です。アドバイザリーとリンクの一覧については、『[Cisco Event Response: March 2024 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

公開時点では、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

するシスコプラットフォームに影響を与え、次の条件が満たされた場合に影響を与えました。

- デバイスにAUXポートがある。
- AUXポートはflowcontrol hardwareで設定されます。
- AUXポートにハードウェアが接続されていないか、接続されているモデムからフロー制御をオフにする信号が送られていて、フロー制御を再びオンにしません。

公開時点で脆弱性が確認されている Cisco ソフトウェアの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。

AUXポート設定の確認

デバイスにAUXポートがあるかどうか、およびflowcontrol hardwareが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 | section aux 0 CLIコマンドを使用して、flowcontrol hardwareコマンドとtransport input all|telnetコマンドの存在を確認します。次の例に示すように、これらが存在する場合は、ハードウェアが接続されていないか、接続されたモデムからフロー制御をオフにするように指示されてもフロー制御がオンに戻らない場合、デバイスは脆弱であると見なされます。

```
<#root>
```

```
Router#
```

```
show running-config | section line aux 0
```

```
line aux 0
  transport input all
  transport output none
```

```
flowcontrol hardware
```

```
Router#
```

次の例に示すように、出力にflowcontrol hardwareが含まれていない場合、または出力が空白の場合、そのデバイスはこの脆弱性の影響を受けません。

```
<#root>
```

```
Switch#
```

```
show running-config | section line aux 0
```

```
Switch#
```

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。

AUXポートが使用されていない場合は、次の例に示すように無効にする必要があります。

```
<#root>
Router#
show running-config | section line aux 0

line aux 0
  transport input none
  transport output none
  no exec
Router#
```

この回避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。

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	オン	

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-aux-333WBz8f>

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	2024年3月27日

利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザー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。