

Cisco IOS XEソフトウェアのアクティブデバッグコードの脆弱性

Medium	アドバイザリーID : cisco-sa-XE-BLKH-Ouvrnf2s	CVE-2021-1381
m	初公開日 : 2021-03-24 16:00	
	バージョン 1.0 : Final	
	CVSSスコア : 6.1	
	回避策 : No workarounds available	
	Cisco バグ ID : CSCvu78908	

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ソフトウェアの脆弱性により、高い権限を持つ認証されたローカルの攻撃者、またはデバイスに物理的にアクセスする認証されていない攻撃者がデバッグコンソールを開く可能性があります。

この脆弱性は、コマンド許可の制限が不十分であることに起因します。攻撃者は、ハードウェアプラットフォームでコマンドを実行してデバッグコンソールを開くことで、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、攻撃者はデバッグコンソールにアクセス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ました。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、次のリンクで確認できます。

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-XE-BLKH-Ouvrnf2s>

該当製品

脆弱性のある製品

公開時点で、この脆弱性は、Cisco IOS XEソフトウェアの脆弱性のあるリリースを実行している次のシスコデバイスに影響を与えました。

- IR1101サービス統合型ルータ

- ESR6300エンベデッドシリーズルータ

脆弱性が存在するシスコ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。

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確認されています。

シスコは、この脆弱性が次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
- 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。

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、[Cisco Security Advisories](#)ページから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、問題の有無と完全なアップグレードソリューションを確認することをお勧めします。

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搭載されていることを確認し、現在のハードウェアおよびソフトウェアの設定が新しいリリースで引き続き適切にサポートされることを確認する必要があります。情報が明確でない場合は、Cisco Technical Assistance Center(TAC)また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該当するかどうかを判断できるように、Cisco Software Checkerを使用して、特定のソフトウェアリリースに影響するCisco Security Advisoryと、各アドバイザリに記載されている脆弱性を修正した最初のリリース(「First Fixed」)をです。該当する場合、このツールは、特定されたすべてのアドバイザリに記載されているすべての脆弱性を修正した最初のリリース(「Combined First Fixed」)も返します。

お客様は、[Cisco Software Checker](#)を使用して[次の](#)方法でアドバイザリを検索できます。

- ソフトウェアと1つ以上のリリースを選択します
- 特定のリリースのリストを含む.txtファイルをアップロードします
- `show version`コマンドの出力を入力します

検索を開始した後、すべてのCisco Security Advisories、特定のアドバイザリ、または最新のバンドル公開のすべてのアドバイザリを含むように検索をカスタマイズできます。

また、次のフォームを使用して、Cisco IOSまたはIOS XEソフトウェアリリース(15.1(4)M2や3.13.8Sなど)を入力して、リリースがCisco Security Advisoryの影響を受けるかどうかを確認できます。

デフォルトでは、[Cisco Software Checker](#)には、CriticalまたはHigh Security Impact Rating(SIR)を持つ脆弱性の結果のみが含まれます。Medium SIRの脆弱性の結果を含めるには、Cisco.comのCisco Software Checkerを使用し、検索をカスタマイズするときにImpact RatingのドロップダウンリストのMediumチェックボックスをオンにします。

Cisco IOS XEソフトウェアリリースとCisco IOSソフトウェアリリースのマッピングについては、Cisco IOS IOSに応じて、[Cisco IOS XE 2リリースノート](#)、[Cisco IOS XE 3Sリリースノート](#)、または[Cisco IOS XE 3SGリリースノート](#)を参照してくださいXEソフトウェアリリース

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不正利用事例や公表は確認しておりません。

出典

この脆弱性は、Cisco Advanced Security Initiative Group(ASIG)のX.B.による内部セキュリティテストで発見されました。

URL

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-XE-BLKH-Ouvrnf2s>

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	最初のパブリックリリース。	—	最終	2021年3月24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。