Cisco IOS XE SD-WANソフトウェアにおける任意のファイル破損の脆弱性

Medium

アドバイザリーID : cisco-sa-iosxe-arbfile-FUxskKDE
CVE-2021-1434
初公開日 : 2021-03-24 16:00
バージョン 1.0 : Final
CVSSスコア : 4.4
回避策 : No workarounds available
Cisco バグ ID : CSCvu39228

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 SD-WANソフトウェアのCLIの脆弱性により、認証されたローカルの攻撃者が基盤となるファイルシステム内の任意のファイルを上書きする可能性があります。

この脆弱性は、特定のCLIコマンドのパラメータの検証が不十分であることに起因します。攻撃者は、特定のパラメータを指定してこのコマンドを発行することにより、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ホストファイルシステムに存在する任意のファイルの内容を上書き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。

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-iosxe-arbfile-FUxskKDE

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 SD-WANソフトウェアの脆弱性が存在するリリースを実行し、SD-WAN機能が有効になっている次のシスコ製品に影響を与えました。SD-WAN 機能は、デフォルトでは有効になっています。

- 1000 シリーズ サービス統合型ルータ（ISR）
- 4000 シリーズ ISR

- ASR 1000 シリーズ アグリゲーション サービス ルータ
- Cloud Services Router 1000V シリーズ

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。

デバイス設定の確認

SD-WAN 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方法は 2 つあります。

オプション 1：show running-config | include sdwan コマンド

sdwan モード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、show running-config | include sdwan コマンドを使用して、出力でトンネルモードを確認します。コマンドから tunnel mode sdwan が返される場合、sdwan 機能は有効になっており、そのデバイスには脆弱性が存在します。コマンドから出力が返されない、またはコマンドが存在しない場合、SD-WAN 機能は有効になっていないため、そのデバイスには脆弱性は存在しません。

以下に、show running-config | include sdwan コマンドを SD-WAN 機能が有効になっているデバイスで実行した場合の出力例を示します。

```
<#root>

Router#

show running-config | include sdwan


tunnel mode sdwan
Router#
```

オプション 2：show version コマンドを使用します。

または、show version コマンドを使用して、Cisco IOS XE デバイスがコントローラモードであるかどうかを確認します。出力の最後には、デバイスがコントローラモードであるかどうかを示すルータの動作モードが含まれます。

次に、SD-WAN 機能が有効になっているデバイスに対する show version コマンドの出力例の一部を示します。

```
<#root>

Router#

show version
```

```
.
.
.
Router operating mode: Controller-Managed
.
.
.
```

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
- 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、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

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、シスコでは Cisco Software Checker を提供しています。このツールにより、特定のソフトウェアリリースに該当するシスコ セキュリティ アドバイザリ、および各アドバイザリで説明されている脆弱性が修正された最初のリリース（「First Fixed」）を特定できます。また該当する場合、そのリリースに関するすべてのアドバイザリ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。

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する
- show version コマンドの出力を入力する

検索を開始した後で、すべてのシスコ セキュリティ アドバイザリ、特定のアドバイザリ、または最新の公開資料に記載されているすべてのアドバイザリが含まれるように検索をカスタマイズできます。

また、次の形式を使用して、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）を入力することで、そのリリースがシスコ セキュリティ アドバイザリの影響を受けているかどうかを判断できます。

Check

デフォルトでは、Cisco Software Checker の結果には、Security Impact Rating（SIR）が「重大」または「高」の脆弱性だけが含まれます。「中間」の SIR 脆弱性の結果を含めるには、Cisco.com にある Cisco Software Checker を使用して、検索をカスタマイズするときに [影響の評価（Impact Rating）] の下にあるドロップダウンリストの [中間（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 XE ソフトウェアのリリースに応じて「Cisco IOS XE 2 Release Notes」、「Cisco IOS XE 3S Release Notes」、または「Cisco IOS XE 3SG Release Notes」を参照してください。

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

この脆弱性は Cisco TAC 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-iosxe-arbfile-FUxskKDE

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	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。