Cisco IOS XE SD-WANソフトウェアのパストラバーサルの脆弱性

Medium	**アドバイザリーID :** cisco-sa-iosxe-sdwpathtrav-nsrue2Mt **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 :** CSCvu28373	CVE-2021-1436

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における脆弱性により、認証されたローカルの攻撃者がパストラバーサル攻撃を実行し、該当システムの機密ファイルへの読み取りアクセスを取得できる可能性があります。

この脆弱性は、ユーザが入力した検証が不十分であることに起因します。攻撃者は、巧妙に細工された要求を該当システム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、攻撃者は該当システム上の任意のファイルを表示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。

このアドバイザリは、次のリンクで確認できます。
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-sdwpathtrav-nsrue2Mt

該当製品

脆弱性のある製品

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機能を有効にしている場合、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せん。

- 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

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、この公開時点で脆弱性が存在していたシスコソフトウェアリリースに関する情報を確認してください。

デバイス設定の確認

デバイスでSD-WAN機能が有効になっているかどうかを確認するには、次の2つの方法があります。

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コマンドを発行し、出力のトンネルモードを確認します。このコマンドがtunnel mode sdwanを返すと、sdwan機能が有効になり、デバイスが脆弱になります。コマンドが出力を返さない場合、またはコマンドが存在しない場合は、SD-WAN機能が有効になっていないため、デバイスはこの脆弱性の影響を受けません。

show running-config | include sdwanコマンドを使用します。

```
Router# show running-config | include sdwan
tunnel mode sdwan
Router#
```

オプション2:show versionコマンドの使用

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判別します。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動作モードが含まれます。

次の例は、SD-WAN機能が有効になっているデバイスでのshow versionコマンド出力の一部を示しています。

```
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、シスコのJames Spadaro IIIの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-iosxe-sdwpathtrav-nsrue2Mt

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