Cisco SD-WAN ソリューションの不適切なアクセス制御の脆弱性

High

アドバイザリーID : cisco-sa-sd-wan-file-access-VW36d28P
初公開日 : 2022-04-13 16:00
最終更新日 : 2024-01-23 21:31
バージョン 1.1 : Final
CVSSスコア : 7.8
回避策 : No workarounds available
Cisco バグ ID : CSCvy11382

CVE-2022-20716

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 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昇格した権限を取得する可能性があります。

この脆弱性は、影響を受けるシステム内のファイルのアクセス制御が不適切であることに起因します。ローカルの攻撃者は、脆弱性のあるデバイス上のファイルを変更することで、この脆弱性をエクスプロイトする可能性があります。エクスプロイトに成功した場合、攻撃者は昇格した権限を取得し、root ユーザーの権限でシステム上でアクションを実行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-sd-wan-file-access-VW36d28P

該当製品

脆弱性のある製品

本脆弱性は、以下のシスコ製品に影響します。

- SD-WAN vBond Orchestrator ソフトウェア
- SD-WAN vEdge クラウドルータ
- SD-WAN vEdge ルータ

- SD-WAN vManage ソフトウェア
- SD-WAN vSmart コントローラソフトウェア

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。

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。

シスコでは、この脆弱性が Cisco IOS XE SD-WAN ソフトウェアには影響を与えないことを確認しています。

セキュリティ侵害の痕跡

「Cisco Security Indicators of Compromise Reference Guide」にはよく見られる侵害の兆候（IoC）が記載されており、このシスコ セキュリティ アドバイザリで公開されている脆弱性の影響を受ける可能性のあるデバイスを特定するのに役立ちます。

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

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

Cisco.com の Cisco Support and Downloads ページには、ライセンスとダウンロードに関する情報が記載されています。このページには、[マイデバイス（My Devices）] ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。

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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）に連絡してアップグレードを入手してください。

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

次の表では、左の列にシスコソフトウェアのリリースを記載しています。中央の列は、リリースがこのアドバイザリに記載されている脆弱性に該当するかどうか、および、この脆弱性に対する修正を含む最初のリリースを示しています。右の列は、リリースがアドバイザリ集に記載された「重大」または「高」SIR の脆弱性の影響を受けるかどうかと、それらの脆弱性に対する修正を含むリリースを示しています。

次の表に示す適切な修正済みのソフトウェアリリースにアップグレードすることをお勧めします。本アドバイザリは以下のアドバイザリを含むコレクションの一部です。お客様におかれましては、これらも考慮したうえでアップグレード ソリューション全体をご確認ください。

- cisco-sa-sd-wan-file-access-VW36d28P Cisco SD-WAN ソリューションの不適切なアクセス制御の脆弱性
- cisco-sa-sdwan-privesc-vman-tEJFpBSL Cisco SD-WAN vManage における特権昇格の脆弱性

Cisco SD-WAN ソフトウェアリリース	この脆弱性に対する最初の修正リリース	First Fixed Release for All Vulnerabilities Described in the Collection of Advisories
18.4	修正済みリリースに移行。	修正済みリリースに移行。

Cisco SD-WAN ソフトウェアリリース	この脆弱性に対する最初の修正リリース	First Fixed Release for All Vulnerabilities Described in the Collection of Advisories
19.2	修正済みリリースに移行。	修正済みリリースに移行。
20.3	20.3.6	20.3.6
20.4	修正済みリリースに移行。	修正済みリリースに移行。
20.5	修正済みリリースに移行。	修正済みリリースに移行。
20.6	20.6.1	20.6.1
20.7	20.7.1	20.7.1

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

この脆弱性を報告してくださった Joris Oversteyns 氏に感謝の意を表します。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-file-access-VW36d28P

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	修正済みソフトウェアの情報を更新。	修正済みリリース	Final	2024 年 1 月 23 日
1.0	初回公開リリース	—	Final	2024 年 1 月 23 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。