Cisco Catalyst SD-WAN Managerの特権昇格の脆弱性

アドバイザリーID : cisco-sa-sdwan-priviesc-WCk7bmmt
初公開日 : 2025-05-07 16:00
バージョン 1.0 : Final
CVSSスコア : 7.8
回避策 : No workarounds available
Cisco バグ ID : CSCwk92200

CVE-2025-20122

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 Catalyst SD-WAN Manager（旧称Cisco SD-WAN vManage）のCLIの脆弱性により、認証されたローカルの攻撃者が、基盤となるオペレーティングシステムのルートユーザの権限を取得する可能性があります。

この脆弱性は、不十分な入力検証に起因します。SD-WAN Managerシステムに対する読み取り専用権限を持つ認証された攻撃者が、巧妙に細工された要求をSD-WAN ManagerのCLI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、攻撃者は基盤となるオペレーティングシステムのルート権限を取得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-sdwan-priviesc-WCk7bmmt

該当製品

脆弱性のある製品

この脆弱性は、Cisco Catalyst SD-WAN Managerに影響を与えます。

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リストされている製品だけがこの脆弱性の影響を受けることが知られています。

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 XE ソフトウェア
- Meraki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

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 シスコサポート & ダウンロードページには、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完全なアップグレード ソリューション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

このアドバイザリは、Cisco Catalyst SD-WAN Managerの脆弱性に関する一連のアドバイザリの一部です。このコレクションには、次のアドバイザリが含まれます。

- Cisco Catalyst SD-WAN Managerの特権昇格の脆弱性
- Cisco Catalyst SD-WAN Managerの任意のファイル作成の脆弱性
- Cisco Catalyst SD-WAN Managerの証明書検証の脆弱性
- Cisco Catalyst SD-WAN Managerの任意のファイルを上書きする脆弱性
- Cisco Catalyst SD-WAN Managerストアドのクロスサイトスクリプティングの脆弱性
- Cisco Catalyst SD-WAN Managerの反映HTMLインジェクションの脆弱性

次の表では、左の列にシスコ ソフトウェア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、リリースがこのアドバイザリ集の一部である脆弱性の影響を受けるかどうか、およびこのコレクションのすべての脆弱性に対する修正を含むリリースを示しています。

該当する修正済み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。

Cisco Catalyst SD-WAN Managerリリース	この脆弱性に対する最初の修正リリース	このコレクションに含まれるすべての脆弱性に対する最初の修正リリース
20.8以前[1]	修正済みリリースに移行。	修正済みリリースに移行。
20.92	20.9.7	修正済みリリースに移行。
20.101	修正済みリリースに移行。	修正済みリリースに移行。
20.111	修正済みリリースに移行	修正済みリリースに移行。

Cisco Catalyst SD-WAN Managerリリース	この脆弱性に対する最初の修正リリース	このコレクションに含まれるすべての脆弱性に対する最初の修正リリース
	。	
20.12	20.12.5	修正済みリリースに移行。
20.131	修正済みリリースに移行。	修正済みリリースに移行。
20.142	修正済みリリースに移行。	修正済みリリースに移行。
20.15	20.15.2	修正済みリリースに移行。
20.16	20.16.1	20.16.1

1. これらのリリースは ソフトウェアメンテナンスが終了しています。シスコでは、お客様が サポートされているリリースにアップグレードすることを強く推奨します。
2. これらのリリースは、サポート終了プロセスに入っています。特定のリリースのマイルストーン日付については、そのリリースの『 販売終了およびサポート終了のお知らせ』を参照してください。

ソフトウェアの移行を検討する際は、[シスコ セキュリティ アドバイザリ（Cisco Security Advisories）] 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の有無と完全なアップグレード ソリューションを確認してください。

いずれの場合も、新しいソフトウェアがお客様のネットワークニーズに十分に対応し、現在のハードウェアおよびソフトウェア構成が新しい製品で適切にサポートされ続けることを確認する必要があります。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。

シスコの Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデント レスポンス チーム）は、このアドバイザリに記載されている該当するリリース情報と修正済みリリース情報のみを検証します。

不正利用事例と公式発表

Cisco 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その公表は確認しておりません。

出典

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

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-

priviesc-WCk7bmmt

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	2025年5月7日

利用規約

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。