Cisco Catalyst SD-WAN Managerの認証済み特権昇格の脆弱性

High

アドバイザリーID : cisco-sa-sdwan-privesc-4uxFrdzx
CVE-2026-20245
初公開日 : 2026-06-04 22:27
最終更新日 : 2026-06-05 14:38
バージョン 1.1 : Interim
CVSSスコア : 7.8
回避策 : No workarounds available
Cisco バグ ID : CSCwu18563

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（以前の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、該当システムに巧妙に細工されたファイルを提供し、rootとして任意のコマンドを実行する可能性があります。

この脆弱性は、ユーザ指定の入力の検証が不十分であることに起因します。攻撃者は、巧妙に細工されたファイルを該当システムにアップロードすることにより、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にコマンドインジェクション攻撃を仕掛け、rootユーザとして権限を昇格させる可能性があります。

この脆弱性を不正利用するには、攻撃者は該当システムでnetadmin権限を持っている必要があります。これには、CVE-2026-20182またはCVE-2026-20127の有効なクレデンシャルの取得または不正利用が必要になります。シスコでは、他の方法による不正利用の成功を認識していません。シスコでは、この不具合の不正利用によってエッジデバイスにプッシュされる設定変更が発生した限られた事例を確認しています。

2026年5月14日に公開された『Catalyst SD-WAN Security Advisory』に記載されている修正済みソフトウェアにアップグレードして、エッジデバイスの設定を確認することをお勧めします。

シスコでは、本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せん。この脆弱性に対処する回避策はありません。

重要：侵害の兆候の可能性に関する情報を保存しておくため、お客様はアップグレードを行う前に、SD-WAN 環境内の各制御コンポーネントから request admin-tech コマンドを発行する必要があります。admin-tech ファイルが収集された後、できるだけ早くソフトウェアをアップグレード

する必要があります。

SD-WAN展開を修正済みリリースにアップグレードする前に、関連するログを保持しておいてください。アップグレード後、このアドバイザリに記載されているセキュリティ侵害のインジケータのログをチェックして、システムが侵害されていないことを確認します。ログに侵害のインジケータが示され、システムが侵害されていることが確認された場合は、ソフトウェアアップデートを適用するだけでは脆弱性は解決されません。このような場合は、Cisco Technical Assistance Center(TAC)が提供する具体的な修復手順に従って、システムを保護してください。この項は情報が入手可能になった時点で更新されます。

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-privesc-4uxFrdzx

該当製品

脆弱性のある製品

この脆弱性は、デバイスの設定に関係なく、Cisco Catalyst SD-WAN Managerに影響を与えます。

この脆弱性は、以下を含むすべての展開タイプに影響します。

- オンプレミス展開
- Cisco SD-WAN Cloud-Pro
- Cisco SD-WAN Cloud（Cisco Managed）
- 政府/自治体向け Cisco SD-WAN（FedRAMP）

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。

セキュリティ侵害の痕跡

インターネットに公開されているCisco Catalyst SD-WAN Managerシステムで、ポートがインターネットに公開されているものは、セキュリティ侵害を受けるリスクがあります。場合によっては、標準的な運用中にセキュリティ侵害の兆候が発生することがあります。したがって、誤検出を特定して回避するために、通常のネットワークポスチャに対して評価を行う必要があります。

次の例に示すエントリがないか、/var/log/にあるscripts.logファイルを監査することをお勧めしま

す。

```
Apr 15 09:44:57 vmanage vScript: Tenant list upload per vsmart serial number: /usr/bin/vconfd_script_up
```

注：これらは正当なコマンドであり、ログでは正当な使用と悪意のある使用は区別されません。

Cisco Catalyst SD-WAN Managerが侵害されたかどうかを判断するために、お客様はCisco TACでサービスリクエストをオープンできます。Cisco TACの新しいケースをオープンする前に、SD-WANの展開に含まれる各制御コンポーネントからrequest admin-techコマンドを発行することをお勧めします。これにより、admin-techファイルをCisco TACに提供して確認できます。これには、設定に対して最近行われた不正な変更を示す可能性のあるエッジデバイスも含める必要があります。

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

シスコでは、今後のリリースでCisco Catalyst SD-WAN Managerでこの脆弱性に対処する予定です。この項は情報が入手可能になった時点で更新されます。

その他の情報が必要な場合は、Cisco 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。

不正利用事例と公式発表

2026年6月、Cisco Product Security Incident Response Team(PSIRT)はこの脆弱性の不正利用を認識しました。

この脆弱性を不正利用するには、攻撃者は該当システムでnetadmin権限を持っている必要があります。これには、CVE-2026-20182またはCVE-2026-20127の有効なクレデンシャルの取得または不正利用が必要になります。シスコでは、他の方法による不正利用の成功を認識していません。

出典

シスコは、この脆弱性を報告していただいたMandiant社のChester Sng氏、Pete Boonyakarn氏、およびLogeswaran Nadarajan氏に感謝いたします。

URL

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

privesc-4uxFrdzx

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	研究者を含むようにソースを更新。	出典	Interim	2026年6月5日
1.0	初回公開リリース	—	Interim	2026年6月4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。