Cisco Catalyst SD-WAN Managerの任意のファイルへの書き込みの脆弱性

Medium

アドバイザリーID : cisco-sa-sdwan-arbfw-c2rZvQ
CVE-2026-20262
初公開日 : 2026-06-15 16:00
最終更新日 : 2026-06-15 22:00
バージョン 1.1 : Final
CVSSスコア : 6.5
回避策 : No workarounds available
Cisco バグ ID : CSCwu18441

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Web UIにおける脆弱性により、認証されたリモートの攻撃者が、該当システムのファイルシステム上でファイルの作成や任意のファイルの上書きを行う可能性があります。

この脆弱性は、該当ソフトウェアがファイルのアップロードプロセス中にユーザ入力を適切に検証しないことに起因しています。攻撃者は、該当システムの該当APIエンドポイントに巧妙に細工されたHTTP要求を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上で任意のファイルを作成または上書きできるようになります。このファイルは、後でルートに昇格するために使用できます。この脆弱性を不正利用するには、攻撃者は少なくとも書き込みアクセス権を持つ有効なクレデンシャルを持っている必要があります。

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-arbfw-c2rZvQ

該当製品

脆弱性のある製品

公開時点では、デバイスの設定にかかわらず、この脆弱性はCisco Catalyst SD-WAN Managerに影響を与えていました。

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）

このアドバイザリの公開時点で脆弱性が存在するシスコ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。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

シスコでは、本アドバイザリ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することを強くお勧めします。

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。

お客様には、それぞれのログファイルから次のエントリを監査することを推奨します。

/var/log/nmsにあるvmanage-server.logファイルの次のエントリは、疑わしいWARファイルのアップロードを示しています。このファイルは最初のセキュリティ侵害ベクトルである可能性があります。

```
11-June-2026 03:53:37,310 EDT INFO  [a66cdc5f-807d-4c23-944e-5c809a2ece6b] [server] [SdraAnyConnectFileU
```

次の2つのログは、この脆弱性に関連する追加のアクティビティを示します。これらのアクティビティはログに表示されることがありますが、常に表示されるわけではありません。悪意のあるコードの展開や操作など、最初のセキュリティ侵害の後に攻撃者が何を実行できるかを把握できます。ただし、これらのアクティビティはすべてのインシデントログに一貫して表示されるとは限

りません。この理解の組み合わせは、お客様が環境を監査する際にエクスプロイト後の動作の可能性を認識するのに役立ちます。

/var/log/nms/にあるvmanage-appserver.logファイルから、

```
11-June-2026 07:52:55,275 UTC INFO  [server] (DeploymentScanner-threads - 2) WFLYSRV0010: Deployed "s
```

/var/log/nms/containers/service-proxy/にあるserviceproxy-access.logファイルから、

```
[2026-06-11T07:57:33.635Z] "POST /suspicious/index.jsp HTTP/1.1" 200 - 267 76 17 - "1.1.1.54" "Mozilla/
```

注：このアクティビティは、vManage(Catalyst SD-WAN Manager)環境内の内部システムファイル管理に制限されています。これは、SD-WANリモートアクセス(SDRA)機能の動作状態、設定、または接続とは相関せず、影響を与えません。これらのログを確認し、ログの出所や目的が不明なお客様は、Cisco Technical Assistance Center(TAC)にサポートを要請してください。

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展開の各制御コンポーネントからrequest admin-techコマンドを使用することを推奨します。これにより、admin-techファイルがCisco TACに提供されて、確認を受けることができます。

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、回避策や緩和策（該当する場合）は、修正済みソフトウェアリリースへのアップグレードが利用可能になるまでの一時的な解決策であると考えています。この脆弱性を完全に修正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリ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することを強く推奨します。

修正済みリリース

発行時点では、次の表に示すリリース情報は正確でした。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

左側の列にはシスコソフトウェアリリース、右側の列に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の影響を受けるかどうか、およびこの脆弱性に対する修正を含むリリースが示されています。

Cisco Catalyst SD-WAN リリース	First Fixed Release（修正された最初のリリース）
20.9.9.1 以前	20.9.9.2
20.12.7.1 以前	20.12.7.2
20.15.4.4 以前	20.15.4.5
20.15.5.2 以前	20.15.5.3
20.18.3	20.18.3.1
26.1.1.1 以前	26.1.1.2

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

2026年6月、Cisco PSIRTはこの脆弱性の限定的なエクスプロイトに気づきました。これらの脆弱性が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、引き続き強くお勧めします。

出典

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfw-c2rZvQ

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	概要で指定された書き込みアクセス権限。Indicators of Compromiseにコンテキストを追加	セキュリティ侵害の概要と指標	Final	2026年6月15日
1.0	初回公開リリース	—	Final	2026年6月15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。