

Catalyst SD-WANセキュリティアドバイザリの修正 – 2026年9月

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[是正ワークフローの概要](#)

[ステップ1: すべてのマネージャからのAdmin-Techファイルの収集](#)

[代替: 手動検証 \(Admin-Techを収集できない場合のみ\)](#)

[ステップ2: 修正済みソフトウェアバージョンへのアップグレード](#)

[ステップ3:TACケースを開き、スキャン用のAdmin-Techファイルをアップロードする](#)

[ステップ4: セキュリティ侵害が特定された場合 – TACガイダンス](#)

[修正済みソフトウェアバージョン](#)

[付録: 手動による検証手順 \(Admin-Tech収集ができない場合のみ\)](#)

[セキュリティ侵害の指標を特定する方法](#)

[検証1: サービスプロキシアクセスログの監査](#)

[検証2: Manager Serverログの監査](#)

[よく寄せられる質問 \(FAQ\)](#)

概要

このドキュメントでは、2026年9月30日のPSIRTアドバイザリに記載されている日付に従って、重要なSD-WANセキュリティの脆弱性を特定して修正する手順について説明します。シスコでは、この問題を修正するために、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強く推奨します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Catalyst SD-WANアーキテクチャおよび制御コンポーネント(Manager、Controller、Validator)
- Cisco Catalyst SD-WANのアップグレード手順

- Cisco TAC Case ManagementおよびAdmin-Tech収集手順

使用するコンポーネント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

詳細な背景情報と最新のアップデートについては、PSIRTの公式アドバイザリページを参照してください。

このアドバイザリは、次のリンク先で確認できます。

- [Cisco Catalyst SD-WAN ManagerのAPI認証バイパスに関する脆弱性](#)(CVE-2026-76504、CWE-177) セキュリティ影響評価：重要（CVSS基本スコア9.8）。

この不具合は、次のPSIRTアドバイザリで説明されています。

- Cisco Bug ID CSCww79570

このアドバイザリは、Cisco Catalyst SD-WAN Manager(vManage)に影響を与えます。

是正ワークフローの概要



注：最初の修正済みリリースより前のリリースが稼働しているすべてのSD-WAN Manager(vManage)に脆弱性が存在するため、すぐにアップグレードする必要があります。ただし、すべてのCatalystマネージャがセキュリティ侵害の証拠を示しているわけではありません。

必要な処置：すべてのCatalyst SD-WAN Managerからadmin-techsを収集し、すべてを修正済みリリースにアップグレードし、Cisco TACでケースをオープンして、admin-techsでセキュリティ侵害のインジケータをスキャンできるようにします。

TACは次のユーザが利用できます。

- セキュリティ侵害の指標に関して提供した管理テクノロジーをスキャンする
- アップグレード中に問題が発生した場合は、アップグレードサポートを提供します
- セキュリティ侵害の指標が特定された場合は、追加の修復方法を案内します。

1. Admin-Techの収集:診断データが失われないように、アップグレードの前に、クラスタおよ

びディザスタリカバリ(DR)導入のすべてのノードを含むすべてのCatalyst SD-WAN Managerでadmin-techを実行します。Log and Tech optionsを選択します。コアは必要ありません。

- 修正済みリリースへのアップグレード：すべてのManager(vManage)を、「[修正済みソフトウェアバージョン](#)」表に記載されている修正済みソフトウェアバージョンにアップグレードします。



注:TACスキャン結果を待たずにアップグレードを実行してください。修正済みリリースへのアップグレードは最も優先度が高く、この脆弱性を解消します。ステップ3のTACスキャンで、アップグレード後にさらなるアクションが必要かどうか判断されます。

- TACケースを開き、セキュリティ侵害の指標をスキャンするAdmin-Techをアップロードする:Cisco TACケースを開き、ステップ1で収集したすべてのAdmin-Techログバンドルをアップロードします。TACは管理テクノロジーをスキャンして、セキュリティ侵害の痕跡を検出します。
- セキュリティ侵害が特定された場合は、TACガイダンスを使用します。TACがお客様の環境でセキュリティ侵害の指標を特定した場合は、TACが提供するすべての修復ガイダンスに従います。セキュリティ侵害の兆候が見つからない場合は、アップグレード以外のアクションは必要ありません。

ステップ1：すべてのマネージャからのAdmin-Techファイルの収集

必須：診断データが失われないように、アップグレードの前にすべてのマネージャ(vManage)からadmin-techファイルを収集します。これらのファイルは、TACがステップ3で環境をスキャンして侵害の痕跡を検出するために使用されます。

コレクション：



注:admin-tech生成の場合は、LogおよびTechオプションを選択します。コアは必要ありません。

- ALL Managers(vManage)でadmin-techを実行します。
- マネージャがクラスタとして実行されている場合は、すべてのクラスタメンバーでadmin-techを実行します。
- ディザスタリカバリ(DR)を導入している場合は、プライマリとDRサイトの両方のすべてのマネージャでadmin-techを実行します。

[SD-WAN環境でのAdmin-Techの収集とTACケースへのアップロード](#)



注:TACはこれらのファイルを分析して、お客様の環境に侵入の痕跡がないか評価し、適切な修復パスを指示します。

代替：手動検証（Admin-Techを収集できない場合のみ）

admin-techファイルを共有できない場合は、手動の検証手順を使用できます。これらの手順は、文書化してTACと共有する必要がある暫定的な指標を提供します。

詳細な手順については、このドキュメントの最後にある「[手動による確認手順](#)」のセクションを参照してください。調査結果をすべて文書化し、サポート案件でTACに提供します。

ステップ2：修正済みソフトウェアバージョンへのアップグレード

ステップ1で管理テクニックを収集した後、すべてのマネージャ(vManage)を修正済みソフトウェアバージョンにアップグレードします。



重要:TACスキャン結果を待たずにアップグレードを実行してください。修正済みリリースへのアップグレードは最も優先度が高く、この脆弱性を解消します。ステップ3のTACスキャンで、アップグレード後にさらにアクションが必要かどうか判断されます。

このドキュメントの「[修正済みソフトウェアバージョン](#)」の表から適切なバージョンを選択します。



警告：アップグレードは現在のメジャーリリース内に留まる必要があります。TACのガイドランスがない場合は、上位のメジャーリリースにアップグレードしないでください。

[vManage GUIまたはCLIを使用したSD-WANコントローラのアップグレード](#)



注：アップグレード中に問題が発生した場合は、TACサービスリクエストをオープンしてアップグレードサポートを受けてください。

ステップ3:TACケースを開き、スキャン用のAdmin-Techファイ

ルをアップロードする

ステップ2でアップグレードを行った後、Cisco TACサポートケースをオープンし、ステップ1で収集したadmin-techファイルをアップロードします。TACは管理テクノロジーをスキャンして、セキュリティ侵害の痕跡を検出します。

必要なアクション：

1. タイトルに「CVE-2026-76504」というCVE-IDを使用して重大度3 TACのケースをオープンし、スキャンングプロセスを開始します。
2. ステップ1で収集したすべてのadmin-techログバンドル（クラスタおよびDRノードを含むすべてのマネージャ）をアップロードします。
3. TACがスキャンを完了し、結果を通知するまで待ちます。



注:TACはadmin-techファイルを分析し、スキャンの結果を通知します。セキュリティ侵害の兆候が見つからない場合は、アップグレード以外のアクションは必要ありません。

ステップ4：セキュリティ侵害が特定された場合 – TACガイダンス

お客様の環境におけるセキュリティ侵害の痕跡がTACによって特定されると、TACから具体的な修復ガイダンスが提供されます。TACが提供するすべての指示に従ってください。

侵害の兆候が見られない場合は、ステップ2で完了したアップグレードで十分であり、それ以上の修復は必要ありません。

修正済みソフトウェアバージョン

これらのソフトウェアリリースには、この脆弱性に対する修正が含まれています。現在のリリーストレインの最初の修正済みリリースにアップグレードします。

Cisco Catalyst SD-WANソフトウェアリリース	第 1 修正済みリリース	利用可能なソフトウェア
20.91 よりも前	修正済みリリースに移行。	
20.9	20.9.10.1	20.9.10.1 vManage用アップグレードイメージ
20.12	20.12.8.2	20.12.8.2 vManage用アップグレ

Cisco Catalyst SD-WANソフトウェアリリース	第 1 修正済みリリース	利用可能なソフトウェア
		ードイメー
20.15	20.15.6.1	20.15.6.1 vManage用アップグレードイメー
20.18	20.18.4.1	20.18.4.1 vManage用アップグレードイメー
26.1	26.1.2.1	26.1.2.1 vManageのアップグレードイメー
26.2	26.2.1	26.2.1 vManageのアップグレードイメー

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、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。

Cisco Product Security Incident Response Team(PSIRT)は、このアドバイザリに記載されている該当リリースと修正済みリリースの情報のみを検証します。



注：シスコは、クラウドベースのCisco SD-WAN Cloud(Cisco Managed)リリース 20.15.605でも、この脆弱性に対処しています。ユーザ操作は不要です。お客様は、サービスGUIのヘルプ機能を使用して、現在の修復ステータスまたはソフトウェアバージョンを確認できます。

重要な参考資料

- [アップグレードマトリックス](#)
- [コントローラ互換性マトリックス](#)

付録：手動による検証手順（Admin-Tech収集ができない場合のみ）



注:Admin-tech収集が推奨される方法です。admin-techファイルの収集と共有が絶対に不可能な場合は、手動検証のみを使用してください。admin-techファイルを収集できない場合は、次の手動の手順を使用してTACの暫定的なインジケータを収集します。



注：

- これらの手順では、暫定データのみが提供されます
- 正確な評価には、admin-techの収集を強く推奨
- 結果を文書化し、サポートケースでTACと共有します。
- TACが正式な評価を決定

要件：これらの手順は、すべてのManager(vManage)で実行する必要があります。これには、ディザスタリカバリ(DR)サイトのすべてのクラスタメンバーとManagerが含まれます。vshellからログファイル (Manager CLIからvshell) にアクセスし、現在のログファイルとローテーションされたログファイルの両方を確認します。

セキュリティ侵害の指標を特定する方法

このアドバイザリには、侵害の痕跡が2つあります。両方とも、不明または不正なIPアドレスからの、要求の文字がエンコードされたj_security_checkのエントリに関連します (例：
： /%6a_security_check) 。



重要：このセクションの例では、要求でのエンコードされた文字jとしての%6aの使用を示しています。これは一例に過ぎず、この脆弱性では要求でエンコードされた1文字のみを使用できます。



注：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危険性があります。場合によっては、標準的な運用中に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。

指標	ログファイル	意味	確認
エンコードされたj_security_check要求を受信しました	/var/log/nms/containers/service_proxy/serviceproxy-access.log*	クライアントがこのタイプの要求をマネージャに送信しました。	検証 1
エンコードされたj_security_check要	/var/log/nms/vmanage-server.log*	マネージャは、	検証

指標	ログファイル	意味	確認
求がviptela-reserved-*ユーザに対して処理されました		viptela-reserved-*ユーザ (予約済みのシステムサービスアカウント) に対してこのタイプの要求を処理しました。	2

検証1：サービスプロキシアクセスログの監査

次の例に示すように、不明または不正なIPアドレスからのj_security_checkに関連するエントリについて、/var/log/nms/containers/service_proxy/serviceproxy-access.logにあるserviceproxy-access.logファイルを監査します。

```
[2026-09-29T23:11:13.948-05:00] "POST /%6a_security_check HTTP/1.1" 200 - 48 0 4 - "10.10.10.47,192.168
```

vManageシステムの一部のログファイルは、ルートアクセスの背後で制限され、お客様が直接アクセスすることはできません。これらのログを確認するには、admin-techファイルを生成する必要があります。

TACの結果とドキュメントの解釈

該当するエントリが見つからない場合：

- このマネージャのこのログにはセキュリティ侵害のインジケータは検出されませんでした
- この結果をTACケースに文書化します。
- 検証2を続行し、残りのマネージャで両方の検証を繰り返します

このようなエントリが見つかった場合：

- 示されている各送信元IPアドレスを注意深く調べます
- 不明または不正なIPアドレスからのエントリを探します。送信元IPが環境内の許可されたアクティビティに属しているかどうかを確認する（たとえば、実行する脆弱性スキャンまたは侵入テスト）
- 送信元IPが正当なものであると特定できない場合、侵害の潜在的なインジケータを示している可能性があります
- すべての調査結果を文書化し、TACサービスリクエストを直ちにオープンする

- ログエントリ、タイムスタンプ、送信元IP、およびHTTPステータスコードをケースに含めます
- TACが公式評価の決定を行う

検証2:Manager Serverログの監査

不明または不正なIPアドレスからのj_security_checkに関連するエントリ、特に次の例に示すようにviptela-reserved-で始まる名前を持つユーザに対して呼び出されるエントリについて、`/var/log/nms/vmanage-server.log`にあるvmanage-server.logファイルを監査します。

```
29-Sep-2026 23:11:13,952 CDT [] [vManage-new] [UserUtils] (default task-127462) [default] Request Store
```



注:viptela-reservedシステムサービスアカウントについては、『Cisco Catalyst SD-WANシステムおよびインターフェイス構成ガイド』の「認証、認可、アカウントティング」セクションに記載されています。

TACの結果とドキュメントの解釈

該当するエントリが見つからない場合：

- このマネージャのこのログにはセキュリティ侵害のインジケータは検出されませんでした
- この結果をTACケースに文書化します。
- 残りのマネージャに対して両方の検証を繰り返します。

このようなエントリが見つかった場合：

- これは、セキュリティ侵害の潜在的な兆候を示している可能性があります
- すべての調査結果を文書化し、TACサービスリクエストを直ちにオープンする
- ケースにログエントリとタイムスタンプを、同じ期間の検証1の結果とともに含めます
- TACが公式評価の決定を行う

よく寄せられる質問 (FAQ)

Q：このセキュリティアドバイザリに対処するための最初のステップは何ですか。

A：すべてのマネージャ(vManage)からadmin-techファイルを収集し、すべてのマネージャを修正済みのソフトウェアバージョンにアップグレードします。アップグレードが完了したら、TACケースを開き、管理手順をアップロードします。これにより、TACが環境をスキャンして侵害の痕跡を検出できます。

Q：このアドバイザリの影響を受けるコンポーネントは何ですか。

A：この脆弱性の影響を受けるのは、Cisco Catalyst SD-WAN Manager(vManage)だけです。

Q：コントローラ、バリデータ、またはエッジルータもアップグレードする必要がありますか。

A：いいえ。このアドバイザリには対応していません。すべてのManager(vManage)を修正済みのリリースにアップグレードし、[コントローラ互換性マトリクス](#)を使用して、新しいManagerリリースと他のコンポーネントとの互換性を確認します。

Q：回避策はありますか。

A：いいえ。この脆弱性に対処する回避策はありません。修正済みリリースにアップグレード。

Q：どのバージョンにアップグレードする必要がありますか。

A：現在のリリーストレインの最初の修正済みリリースにできるだけ早くアップグレードしてください。このドキュメントの「[修正済みソフトウェアバージョン](#)」の表を参照してください。ご使用の環境に適したバージョンのTACの確認

Q：以前のSD-WANセキュリティアドバイザリの修正済みリリースにすでにアップグレードされています。もう一度アップグレードする必要がありますか。

A：はい。ただし、現在のリリースが「[修正済みソフトウェアバージョン](#)」表に記載されたトレインの最初の修正済みリリース以降でない場合は除きます。以前のアドバイザリの修正済みリリースには、必ずしもこの脆弱性の修正が含まれているわけではありません。

Q：すべてのマネージャからadmin-techsを収集する必要がありますか。

A：はい。TACでは、お客様の環境を適切に評価するために、すべてのManager(vManage)のすべてのクラスタメンバーおよびDisaster Recovery(DR)サイトのすべてのManagerからのadmin-techファイルを必要とします。

Q：自分で侵入の痕跡を確認できますか。

A：はい。admin-techファイルを収集できない場合は、各マネージャで「[手動確認手順](#)」を使用して、その結果をTACと共有してください。Admin-tech収集が推奨される方法であり、TACが公式アセスメントを決定します。

Q:TACはシステムが侵害されたかどうかを判断する方法を教えてください。

A:TACは、専用ツールを使用してアドミンテクノロジファイル进行分析し、侵害の痕跡がないか環境を評価します。

Q：セキュリティ侵害の兆候が見つかった場合、どうなりますか。

A:TACから連絡があり、お客様の環境に固有の次のステップとガイダンスについて話し合います。シスコがユーザに代わって修復を実行することはありません。TACは、ユーザが作業を進めるために必要なガイダンスを提供します。

Q:TACが管理技術者を分析する前に、アップグレードを開始できますか。

A：はい。管理手順を収集し、修正済みリリースにアップグレードしてからTACケースをオープン

ンします。これにより、TACは管理手順をスキャンして侵害の痕跡を検出できます。

Q：修復中にダウンタイムが発生する可能性がありますか。

A：影響は、導入アーキテクチャと修復パスによって異なります。TACは、プロセス中のサービスへの影響を最小限に抑えるためのガイダンスを提供します。

Q：クラウドホスト型のSD-WANオーバーレイを所有しています。アップグレードにはどのようなオプションがありますか。

A：クラウドホステッドオーバーレイでは、次の2つのオプションがあります。

1. SSP > Overlay Details > Change Windowsの順に選択して、環境の自動アップグレードがスケジュールされているかどうかを確認します。
2. スケジュールされたアップグレードを待機しない場合は、次の2つのオプションがあります。
 - このドキュメントで入手できるアップグレードガイドを使用して、自分でアップグレードしてください。
 - 希望するメンテナンスウィンドウでスタンバイTACケースをオープンします。アップグレードで問題が発生した場合は、TACを利用できます。

Q：シスコがホストするオーバーレイです。SSPのアクセスルールを確認する必要がありますか。

A：シスコがホストするすべてのカスタマーは、SSP > Overlay Details > Allow Inboundルールで各自のAllowed Inboundルールを確認し、各自の側から必要なプレフィックスのみが許可されていることを確認することをお勧めします。これらのルールは管理アクセス専用であり、エッジルータには適用されません。

Q: Cisco TACでは、この脆弱性に対するフォレンジック分析や調査サービスを提供していますか。

A: Cisco TACでは、この脆弱性に関連するIndicators of Compromise(IoC)をスキャンすることでお客様を支援できます。ただし、TACは詳細なフォレンジック分析やインシデント調査を実行しません。包括的なフォレンジック調査や詳細なセキュリティ調査を行うには、お客様が希望するサードパーティのインシデント対応(IR)会社に協力を依頼することをお勧めします。

Q: SD-WANオーバーレイの脆弱性を軽減するための一般的なベストプラクティスまたは方法を教えてください。

A: SD-WANオーバーレイの脆弱性を軽減するためのベストプラクティスと推奨事項については、『[Cisco Catalyst SD-WAN強化ガイド](#)』を参照してください。

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。