Catalyst SD-WANセキュリティアドバイザリの修正 – 2026年6月

内容

はじめに

このドキュメントでは、2026年6月4日付けのPSIRTアドバイザリに基づいて、SD-WANの重大なセキュリティ脆弱性を特定して対処する手順について説明します。

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(vManage、vSmart、vBond)
- 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たものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。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。

バックグラウンド情報

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。

これらのアドバイザリは、次のリンクから入手できます。

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

これらの不具合は、次のPSIRTアドバイザリで対処されています。

- Cisco Bug ID CSCwu18563

是正ワークフローの概要

このアドバイザリでは、不正利用にnetadmin権限を必要とするSD-WAN Managerの権限昇格の脆弱性について説明します。

アドバイザリによると、認証されていないリモート攻撃者がこれらの特権を取得する既知のパスは、CVE-2026-20182(cisco-sa-sdwan-rpa2-v69WY2SW)またはCVE-2026-20127(cisco-sa-sdwan-rpa-EHchtZk)の不正利用です。

コントロールコンポーネントがこれら両方のアドバイザリの修正済みリリースにアップグレードされ、以前のイベントで提供されたadmin-techファイルで潜在的なIndicators of Compromise(IoC)が特定されなかった場合、確認されたファイルに基づいて、この新しい脆弱性の既知の認証されていないエクスプロイトパスがこれらの特定のデバイスで緩和されます。

これは、攻撃者が有効なnetadminクレデンシャルを保持している場合の脆弱性を排除するものではありません。シスコはこの脆弱性に対するソフトウェア修正をまだリリースしておらず、回避策はありません。利用可能になった時点で、詳細なガイダンスが提供されます。

必要な処置：このセキュリティアドバイザリに対処するには、Cisco TACでサービスリクエストをオープンしてください。

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する環境の評価

- 評価に基づく適切な修復パスの案内
- セキュリティ侵害の指標が特定された場合に実行する必要がある次のステップに関するガイダンスを提供する

1. Admin-Techsの収集：すべての制御コンポーネント(vSmart、vManage、vBond)でadmin-techを実行します。vSmart admin-techsは同時に実行しないでください。一度に1つずつ実行してください。その他の情報は、任意の順序で収集できます。Log and Tech optionsを選択します。 コアは必要ありません。
2. TACサービスリクエストをオープンする:Cisco TACに連絡して、すべての制御コンポーネントのAdmin-techログバンドルを提供してください。
3. TACアセスメント：環境内のセキュリティ侵害の指標の事前評価を実行します。TACは環境内のセキュリティ侵害の指標の事前評価を実行します。
4. 修復の実行：必要に応じて、TACが提供する特定のプロセスを実行します。

ステップ1：すべての制御コンポーネントからAdmin-Techファイルを収集します

必須：診断データと潜在的なIndicators of Compromise(IoC)が保持されるように、アップグレードや設定の変更を行う前にすべての制御コンポーネントからアドミニストリックファイルを収集します。これらのファイルは、ステップ3でTACが環境を分析するために使用します。

Collection: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。

1. すべてのコントローラ(vSmarts)でadmin-techを実行：これらを同時に実行しないでください。1つずつ収集します
2. すべてのマネージャ(vManages)でadmin-techを実行します。
3. すべてのバリデータ(vBond)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、お客様の環境にこのアドバイザリに関連する侵害の指標がないかどうかを評価します。このアドバイザリの分析は、正規の使用と悪意のある使用を区別しない特定のログエントリに重点を置いています。TACによる手動レビューが必要です。

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お客様は、手動の検証ステップを使用できます。このステップは、文書化してTACと共有する必要がある事前指標を提供します。

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:TACケースをオープンし、Admin-Techファイルをアップロードする

ステップ1でadmin-techを収集した後、Cisco TACサポートケースをオープンし、収集したadmin-techファイルをアップロードします。TACでは、このアドバイザリに関連するセキュリティ侵害のインジケータについて、管理者の技術者を分析します。

必要なアクション：

1. 分析を開始するには、「CVE-2026-20245」とタイトルにアドバイザリID `cisco-sa-sdwan-privesc-4uxFrdzx`を指定して重大度3 TACのケースをオープンします。
2. ステップ1で収集したすべてのadmin-techログバンドル（コントローラ、マネージャ、およびバリデータ）をアップロードします。
3. TACによる分析が完了し、結果が通知されるのを待ちます。

注：シスコはこの脆弱性に対するソフトウェア修正をリリースしておらず、回避策はありません。ステップ3のTAC分析は、指定したadmin-techファイルにセキュリティ侵害のインジケータが存在するかどうかを判断するのに役立ちます。エンジニアリング部門から入手可能になり次第、詳細なガイダンスが提供されます。

ステップ3:TACアセスメント

TACは、ステップ2でアップロードしたadmin-techファイルの予備分析を実行し、このアドバイザリに関連する侵害のインジケータについてファイルを評価します。

このアドバイザリでの分析は、各Manager(vManage)の`/var/log/scripts.log`にある特定のログエントリに重点を置いています。 基盤となるコマンドは正規のものであり、ログでは正規の使用と悪意のある使用が区別されないため、確認されたインジケータとして扱われる前に、一致するエントリに対してTACがお客様の通常の動作ポスチャに照らして手動でレビューする必要があります。

TACによる分析の結果：

- 一致するログエントリが見つかりませんでした – 確認したadmin-techファイルによると、このアドバイザリに関連するインジケータは確認されていません。現時点では、このアドバイザリに固有のアクションは不要です。結果は受信したadmin-techファイルに制限され、各デバイスのログ保持期間によって制限される可能性があります。
- 一致するログエントリの特定:TACは、お客様に追加のレビューステップを依頼します。シスコはこのアドバイザリに対するソフトウェア修正をリリースしていないため、アップグレードのみではこの脆弱性を解決できません。妥協が確認されたシナリオに関するTACのガイダンスは、ステップ4で参照される関連するTechZoneの記事に記載されています。

注：この脆弱性のエクスプロイトにはアドバイザリで説明されているように、netadmin権限が必要です。認証されていない攻撃者は、有効なクレデンシャルを使用するか、CVE-2026-20182またはCVE-2026-20127をエクスプロイトすることによってのみ、この権限を取得できます。コントロールコンポーネントをこれらのアドバイザリの両方の修正済みリリースにアップグレードし、以前のイベントに対して侵害の兆候が確認されていない場合、確認されたファイルに基づいて、この新しい脆弱性の既知の非認証のエクスプロイトパスがそれらの特定のデバイスで緩和されます。

ステップ4：セキュリティ侵害の指標が特定されたら、TACのガイダンスに従います。

お客様の環境でこのアドバイザリに関連するセキュリティ侵害の兆候が見つかった場合、TACから具体的なガイダンスをお送りします。TACが提供するすべての指示に従ってください。

このアドバイザリでセキュリティ侵害の兆候が見られない場合、確認されたadmin-techファイルに基づいて、現時点でこのアドバイザリに固有のアクションを実行する必要はありません。

⚠ 重要：シスコはこのアドバイザリに対するソフトウェア修正をリリースしておらず、回避策はありません。この脆弱性のエクスプロイトにはCVE-2026-20182またはCVE-2026-20127で取得したnetadmin権限が必要であるため、お客様はこれらの事前アドバイザリの修正が完了していることを確認する必要があります。確立された修復フローの対応するドキュメントを参照してください。

考慮事項

適切な修復を完了した後、お客様固有のセキュリティ保証要件に基づいて、次の衛生活動を評価して実施することを希望する場合があります。これらのアクティビティは、選択した修復オプションに関係なく適用されます。これらのサービスはお客様による管理が必要です。シスコはお客様に代わってサービスを指導または実行することはありません。

- すべてのローカルユーザアカウントの確認
- 資格情報の循環
- デバイス設定に含まれる秘密のローテーション（完全ではないリストなど）：
  - ローカルユーザーアカウントの資格情報
  - SNMP コミュニティ ストリング
  - TACACS秘密鍵
  - VPN事前共有キーと証明書
  - 信頼できるSSHキー
- 設定テンプレートのレビュー

エッジデバイス：セキュリティ侵害の疑い

シスコは特定の修復パスを推奨しません。修復オプションの選択はお客様に委ねられます。環境を評価するお客様への情報としての注意事項：お客様によってエッジデバイスの侵害が疑われる場合、影響を受けるエッジデバイスの工場出荷時設定へのリセットと再オンボーディングは、お客様が選択を行う際に考慮する必要がある、お客様管理によるアクションです。このアプローチを実施するかどうか、また、どのオプションを選択するかは、お客様の判断に基づきます。

安全な工場出荷時設定へのリセットを実行するための適切なコマンドは次のとおりです。

```
factory-reset all secure 3-pass
```

修正済みソフトウェアバージョン

⚠ 重要：このドキュメントの発行時点で、シスコはCVE-2026-20245に対処するソフトウェア修正をリリースしていません。アドバイザリによると、シスコは今後のリリースでCisco Catalyst SD-WAN Managerのこの脆弱性に対処する予定です。回避策はありません。このセクションは、修正済みソフトウェアが入手可能になった時点で更新されます。

この脆弱性のエクスプロイトには、認証されていない攻撃者がCVE-2026-20182またはCVE-2026-20127を通じてのみ取得できるnetadmin権限が必要であるため、お客様には、制御コンポーネントでこれらの事前アドバイザリの修正済みリリースが実行されていることを確認することをお勧めします。これらのアドバイザリの修正済みリリースは、2026年5月14日のSD-WANセキュリティアドバイザリと、対応するTechZoneドキュメントに記載されています。

- Cisco Catalyst SD-WANコントローラの認証バイパスの脆弱性（2026年5月14日）
- （修正済みソフトウェアバージョンの表）

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：推奨される方法はAdmin-tech収集です。admin-techファイルを収集してTACと共有できない場合は、次の手動確認手順のみを使用してください。この手動ステップの結果は事前に文書化されます。結果を文書化し、公式評価を実行するTACと共有します。

注：このアドバイザリでの手動検証は、1つの対象ログチェックで構成されています。検索されるログエントリは正規のコマンドによって生成され、ログだけでは正規の使用と悪意のある使用は区別されません。一致するエントリはすべて、潜在的なインジケータとして扱われる前に、顧客の通常の運用状態に照らして確認する必要があります。一致するエントリを通常の動作と照合できない場合は、結果を文書化し、TACと共有します。

検証：各マネージャ(vManage)のscripts.logでテナントリストのアップロードエントリを確認します

PSIRT忠告に従い、/var/log/にあるscripts.logファイルで、次の例のようなエントリ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
```

手順1：各マネージャ(vManage)のvshellにアクセスし、ログファイルを検索します

vManage CLIからvshellにドロップし、次のコマンドを実行します。

```
vs
zgrep "vconfd_script_upload_tenant_list.sh" /var/log/scripts.log*
```

導入環境内のすべてのvManage（すべてのクラスタメンバーとDRペアのvManageを含む）でチェックを繰り返します。

ステップ2：結果の解釈とTACへのドキュメントの提出

一致するエントリが返されない場合：

- このアドバイザリに関連する侵害の兆候は、このデバイスのログファイルには見つかりませんでした。
- この結果をTACケースに記録します（デバイスのホスト名と、検索したログファイルの日付/範囲を含めます）。
- 残りのマネージャのチェックを続行します。

一致するエントリが返された場合：

- 一致するエントリごとに、お客様の通常の運用状態を確認する必要があります。基盤となるコマンド（テナントリストのアップロード）は正当なものであり、通常の操作中に表示される可能性があります。

- 一致するエントリごとに、タイムスタンプ、完全なログ行、および`-cli path`の後で参照されるファイルパスをキャプチャします。
- 一致するエントリを既知の正当な操作と照合できない場合は、侵害の兆候である可能性があります。調査結果を文書化し、レビューのためにTACに提出します。
- 調査結果をすべて文書化し、TACサービスリクエストをオープンします。一致するログエントリとsourceコマンドの出力をケースに含めます。
- TACが正式な評価を行います。アセスメントで侵害の指標が特定されたら、関連するTechZoneドキュメントおよび修復ガイドに記載されているフローに従ってください。

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：アップグレードや設定の変更を行う前に、すべての制御コンポーネント(vSmart、vManage、vBond)からadmin-techファイルを収集し、診断データと潜在的なセキュリティ侵害のインジケータを保持します。次に、Cisco TACケースを開き、TACが分析できるようにadmin-techsをアップロードします。

Q：シスコはこの脆弱性に対するソフトウェア修正をリリースしていますか。

A：この文書の発行時点では未対応です。アドバイザリによると、シスコは今後のリリースでCisco Catalyst SD-WAN Managerのこの脆弱性に対処する予定です。回避策はありません。このドキュメントは、修正済みリリースが利用可能になった時点で更新されます。

Q：修正プログラムがない場合、シスコが推奨する処置を行う理由は何ですか。

A：この脆弱性をエクスプロイトするには、netadmin権限が必要です。アドバイザリによると、認証されていない攻撃者は、有効なクレデンシャル、またはCVE-2026-20182やCVE-2026-20127の不正利用によってのみ、これらの特権を取得できます。制御コンポーネントをこれらの前のアドバイザリの修正済みリリースにアップグレードすることにより、この脆弱性の不正利用に必要な特権を取得するための既知の非認証パスに対処できます。ステップ3のadmin-tech分析は、確認したファイルに侵害のインジケータが存在するかどうかを判断するのに役立ちます。

Q：すべての制御コンポーネントからadmin-techsを収集する必要がありますか。

A：はい。TACでは、分析を実行するために、すべてのコントローラ（vSmart、1つずつ収集）、すべてのマネージャ(vManage)、およびすべてのバリデータ(vBond)のadmin-techファイルを必要とします。

Q：このアドバイザリに関連するセキュリティ侵害の兆候がシステムにあるかどうかをTACが判断する方法を教えてください。

A: TACではadmin-techファイルを確認し、各マネージャの`/var/log/scripts.log`にあるPSIRTアドバイザリに記載されている特定のログエントリを探します。基盤となるコマンドは正当です。一致するすべてのエントリは、潜在的なインジケータとして扱われる前に、通常の動作ポスチャと照合して確認する必要があります。TACがそのレビューを行います。

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から個別のガイダンスが提供されます。現在、このアドバイザリで使用できるソフトウェア修正はないため、このアップグレードだけでは確認された侵害は解決されません。TACのガイダンスは、2026年5月と2026年2月のアドバイザリに関するTechZoneの関連記事に記載されているフローに従っています。

Q：エッジルータ(Cisco IOS XE)はこのアドバイザリの影響を受けますか。

A：このアドバイザリは、Cisco Catalyst SD-WAN Managerに影響を与えます。このアドバイザリに従い、シスコでは、この脆弱性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。お客様には、エッジデバイスの設定を確認することをお勧めします。

Q：影響を受ける導入タイプは何ですか。

A：この脆弱性は、オンプレミス導入、Cisco SD-WAN Cloud-Pro、Cisco SD-WAN Cloud(Cisco Managed)、Cisco SD-WAN for Government(FedRAMP)など、デバイスの設定に関係なく、すべてのCisco Catalyst SD-WAN Manager導入タイプに影響を与えます。

Q:2026年5月と2026年2月のアドバイザリはすでにアップグレード済みですが、これらのイベントに関するセキュリティ侵害の兆候は見つかっていません。私はこの新しい脆弱性にさらされていますか。

A：コントロールコンポーネントでCVE-2026-20182とCVE-2026-20127の両方の修正済みリリースが実行されていて、確認されたadmin-techファイル内で以前のイベントに対する侵害の兆候が確認されていない場合、確認されたファイルに基づいて、この新しい脆弱性の既知の認証されていないエクスプロイトパスが特定のデバイスで軽減されます。ただし、攻撃者が有効なnetadminクレデンシャルを保持している場合に起こりうる危険を排除することはできません。

Q:TACを待つ代わりに、自分で検証を行うことはできますか。

A: admin-techsを共有できないお客様は、付録に記載されている手動の確認ステップを実行できます。結果は暫定的なものです。結果を文書化し、公式評価を実施するTACと共有します。

Q: SD-WANオーバーレイを強化するための一般的なベストプラクティスは何ですか。

A：ベストプラクティスについては、『Cisco Catalyst SD-WAN強化ガイド』を参照してください。

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、PSIRTアドバイザリに記載されているセキュリティ侵害の指標に関するadmin-techファイルを確認することで、お客様を支援できます。Cisco TACは、詳細なフォレンジック分析やインシデント調査を行いません。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)会社に協力することをお勧めします。

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。