

既に存在する記事の太字を確認する

内容

[はじめに](#)

[参考資料：Cisco SD-WAN CVE-2026-20182に関するドキュメント](#)

[電子メール](#)

[Sherlock 1 – インテーク – アップグレードとAdmin-Techファイルの要求](#)

[Sherlock 2 – 結果 – IoCが観察されない（ファイルごと）](#)

[Sherlock 3 – リマインダー – 不足しているAdmin-Techファイル](#)

[TAC 1 – 調査 – さらなるレビューが必要（IoCの疑い）](#)

[TAC 2 – 結果 – IoCが見つかりません（エンジニア確認）](#)

[TAC 3 – 検証 – オーバーレイでのIP所有権の確認](#)

[TAC 4 – 結果 – 誤検出のクリア](#)

[TAC 5 – 重要 – IoCが特定されました、スケジュール確認コール](#)

[TAC 6 – 結果 – IoCの重複（終了およびリダイレクト）](#)

[TAC 7 – 修復 – オプションのフォローアップ（ポストコール）](#)

[TAC 8 – 修復 – 侵害されたファブリックの更新されたオプション（オプション2のフォローアップ）](#)

[TAC 17 – リバース検索 – 以前はIoCを使用していなかったが、現在はIoCを使用している\(CVE-2026-20182\)](#)

[CloudOps 1 – プロアクティブ – クラウドスキャンでIoCが検出され、Admin-Techによる検証が必要](#)

[以前に影響を受けたことがあり、オプションA、B、またはCを完了していないお客様へのWAVE 2Aの電子メール（オプション1と2を再実行する必要があります）](#)

[PSIRT2aのNo IOCに対するTAC 9テンプレート/それらが再構築を行った（以前に影響を受けた）](#)

[PSIRT2aのIOCがyesの場合にTAC 10テンプレートを作成/再構築した（以前に影響を受けた）](#)

[PSIRT2aのIOCがない場合のTAC 11テンプレート/それらが再構築されなかった（以前に影響を受けた）](#)

[PSIRT2aのIOCがyesの場合にTAC 12テンプレートが再構築されなかった（以前に影響があった）](#)

[新規のお客様向けWAVE 2A用Eメール（以前に影響を受けていません）](#)

[TAC 13 Template for no IOC / No Fixed Release Available\(WAVE 2a – Await Fix\)](#)

[TAC 14 IOCなし/修正済みリリースで利用可能なテンプレート（WAVE 2a – 今すぐアップグレード）](#)

[IOCに関するTAC 15テンプレートが特定/修正済みリリースあり（WAVE 2a：緊急アップグレード）](#)

[TAC 16 IOC用テンプレートが特定されました/修正済みリリースはありません（WAVE 2a – 強化および待機の修正）](#)

はじめに

このドキュメントでは、Cisco Catalyst SD-WANコントローラ認証バイパスの脆弱性に関連するケースのトリアーजおよび修復で使用される、承認済みのカスタマー電子メールテンプレートを

一元化します。テンプレートは送信者（管理技術データを収集してIoCの暫定的な結果を返す自動化されたケース交換）とTACエンジニア（調査、検証、修復ガイダンスのための人手によるフォローアップ）に分かれています。

参考資料：Cisco SD-WAN CVE-2026-20182に関するドキュメント

上記の電子メールテンプレートで参照されるすべてのシスコ文書のマスターリスト。番号付けは統一され、スーパースクリプトは電子メール単位で(例：^[2])このリストの項目にポインタを合わせます。

1. Cisco SD-WAN強化ガイド:<https://sec.cloudapps.cisco.com/security/center/resources/Cisco-Catalyst-SD-WAN-HardeningGuide>
2. 公式セキュリティアドバイザリ(cisco-sa-sdwan-mltnps2-JxpWm7R):<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-mltnps2-JxpWm7R>
3. TAC修復ガイド:<https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/225842-remediate-catalyst-sd-wan-security.html#toc-h1d--1516256622>
4. Cisco SD-WANアップグレードガイド:<https://www.cisco.com/c/en/us/support/docs/wan/dpt/220424-upgrade-sd-wan-controllers-with-the-use.html>
5. Cisco SD-WAN Admin-Tech Collection Guide:<https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/216954-how-to-collect-an-admin-tech-in-an-sd-wa.html>
6. 第2セキュリティアドバイザリ(cisco-sa-sdwan-rpa2-v69WY2SW):<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW>
7. Catalyst SD-WANアップグレードの開始:<https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/225515-start-your-catalyst-sd-wan-upgrade.html>

電子メール

Sherlock 1 – インテーク – アップグレードとAdmin-Techファイルの要求

使用例

TACケースがCVE-2026-20182向けにオープンされた場合の最初のアウトリーチ。admin-techデータの収集方法と、すべてのSD-WAN制御コンポーネントのアップグレード方法がアドバイスされます。

Subject

重要：CVE-2026-20182に必要なアクション：アップグレード計画とIoC評価

メッセージ

お客様各位

Cisco Technical Assistance Center(TAC)にご連絡いただきありがとうございます。

CVE-2026-20182に関連する脆弱性については、[公式のセキュリティアドバイザリ^{\[1\]}](#)で詳細を確認するとともに、[TAC Remediation Guide^{\[2\]}](#)も参照してください。

シスコの主な目的は、お客様の環境を保護することです。このリスクを軽減する上で最も重要なステップとして、アップグレードの計画と実行に優先順位を付けてください。このアップグレードをまだスケジュールしていない場合は、すぐにスケジュールしてください。

アップグレードリソース：アップグレードの実行方法の詳細については、次のシスコの公式ドキュメントを参照してください。[Cisco SD-WANアップグレードガイド^{\[3\]}](#)

CVE-2026-20182に関連する潜在的なIndicators of Compromise(IoC)について環境の初期評価を有効にするには、アップグレードの前にadmin-techコレクションを実行する必要があります。次の操作手順に従ってください。

1. **Admin-Techファイルの収集**：診断データが失われないように、アップグレードの前にすべてのSD-WAN制御コンポーネントからAdmin-Techログを生成します。これらのファイルを生成するときは、必ず「**Logs**」と「**Tech**」の両方を選択してください。
 - **vSmarts (コントローラ)**：同時に収集するのではなく、一度に1つずつ収集します。
 - **vBonds (バリデータ)**：すべてのノードから収集します。
 - **マネージャ(vManage)**：クラスタ内のすべてのノード（アクティブおよびスタンバイDR）から収集します。
2. **アップグレードの実行**：すべてのSD-WANコントロールコンポーネント(vManage、vSmart、vBond)を、アドバイザリ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。アップグレードを開始する前にadmin-techログ分析を待たないでください。アップグレードするとすぐに脆弱性が解消されます。
3. **TACケースへのアップロード**：アップグレードが完了したら、可能であれば、以前に収集したファイルを既存のTACケースに同時にアップロードします。その後、シスコのチームがこれら

のログのスキャンを実行し、お客様の環境のIndicators of Compromise(IoC)を評価します。

リソースとサポート：

admin-techファイルを安全に送信するだけでなく、ファイルを生成する手順の詳細については、『[Cisco SD-WAN Admin-Tech Collection Guide](#)^[4]』を参照してください。

BCS/LCSサブスクリプションをお持ちの場合は、Cisco NCEまたはデリバリマネージャに連絡して、アップグレードプロセスまたは次のステップに関する追加ガイダンスを受けてください。

お客様のデータのプライバシーとセキュリティは、引き続きシスコの最優先事項です。提供される情報はすべて、シスコのプライバシーおよびセキュリティポリシーに従って処理されます。

ケースにアップロードされた各ファイルについて、確認の電子メールが自動的に送信されます。これらの通知を必ず確認してください。

インフラストラクチャの保護に迅速にご協力いただき、ありがとうございます。

リンク：

[1] [公式セキュリティアドバイザリ](#)

[2] [TAC修復ガイド](#)

[3] [Cisco SD-WANアップグレードガイド](#)

[4] [Cisco SD-WAN Admin-Tech Collectionガイド](#)

よろしくお願いします。

Outlookで開く

①次の.emlダウンロードを使用します。送信する前に、すべての[カッコ付きプレースホルダ]を置き換えてください。

✉ Outlookを開く（件名のみ）

↓ .emlテンプレートのダウンロード

Sherlock 2 – 結果 – IoCが観察されない（ファイルごと）

使用例

admin-tech分析の後に送信され、アップロードされた特定のファイルについて確認された侵害のインジケータは示されません。ファイルごとに1回送信されます。

Subject

アップデート：SD-WANコンポーネントの解析結果[ファイル名を挿入] - CVE-2026-20182

お客様各位

お待ちいただきありがとうございました。

admin-techファイル[ファイル名を挿入]の解析が完了しました。このファイルでは、この特定のデバイスのCVE-2026-20182に関連する侵害の指標は特定されませんでした。

このレビューのために取得してシスコに提供したログデータの量は、シスコSD-WAN強化ガイド^[1]に従って設定したログ保持期間により制限されている場合があります。

重要：次のステップとサポート・リクエストの終了：

1. **すべての結果を待つ：**この電子メールの結果は部分的な結果である可能性があることに注意してください。提供された各ファイルを分析します。アップロードしたすべてのファイルの確認を受け取るまで待つから、アセスメントの完了を検討してください。
2. **アップグレードの優先度：**アドミンテクニカルログの事前スキャンでは侵害の痕跡(loC)が特定されていませんが、根本的な脆弱性が残っている可能性があります。Cisco Cloud-ProおよびCisco On-Premの導入については、SD-WANコントロールコンポーネントのフルアップグレードを可能な限り早く優先して行ってください。
 - ・ シスコクラウド(fka:SaaS)カスタマーファブリックは、マネージドサービスの一部として、シスコによって自動的にアップグレードされます。 操作は不要です。
3. **ケースの終了：**アップロードしたすべてのファイルについて「確認されたloCがない」という結果を受け取り、環境全体でソフトウェアのアップグレードが正常に完了した場合は、このケースを解決したと見なして、標準的な終了手順に進むことができます。

アップグレードリソース（該当する場合）：Cisco Cloud-ProおよびCisco On-Premのアップグレード方法の詳細については、シスコの次の公式ドキュメント「Cisco SD-WAN Upgrade Guide」を参照してください。

アップグレードプロセスの概要は次のとおりです。

1. Manager(vManage)リポジトリへの適切なソフトウェアイメージのアップロード
2. Manager(vManage)から始まり、Validator(vBond)とController(vSmart)に続いて、コントローラを順次アップグレードします。
3. 新しいソフトウェアバージョンのアクティブ化とシステム機能の検証

引き続きケースをモニタリングします。お客様から受け取ったファイルに基づいてすべての結果を提供した後、10営業日以内に回答がない場合、シスコはサポートの必要はないと見なして、通常のTACケース終了手順に進みます。もしご不明な点がございましたら、お知らせください。

よろしくお願いします。

Outlookで開く

①送信前に[カッコ付きのプレースホルダ]をすべて置き換えてください。

✉ Outlookを開く（件名のみ）

↓ .emlテンプレートのダウンロード

Sherlock 3 – リマインダ – 不足しているAdmin-Techファイル

使用例

送信されたadmin-techファイルがログ内のSD-WAN制御コンポーネントの数と一致しない場合の自動フォローアップ。

Subject

リマインダ：CVE-2026-20182アセスメントに必要なAdmin-Techファイルが見つかりません

メッセージ

お客様各位

SD-WAN制御コンポーネントの管理者テクノロジーが引き続き不足しているため、管理者テクノロジーログからセキュリティ侵害の指標を評価できません。 CVE-2026-20182評価を開始するには、クラスタ化されているすべてのManager(vManage)ノードを含むすべてのコントローラ(vSmarts)、バリデータ(vBond)、およびマネージャ(vManage)からAdmin-techファイルを受信する必要があります。

次のステップ：

残りのadmin-techファイルは、できるだけ早い時期にアップロードしてください。

よろしくお願いします。

Outlookで開く

①送信前に[カッコ付きのプレースホルダ]をすべて置き換えてください。

✉ Outlook（本文付き）を開く

📎 .emlテンプレートのダウンロード

TAC 1 – 調査 – さらなるレビューが必要（IoCの疑い）

使用例

セキュリティ侵害の可能性を示すログが自動処理によって見つかったと、TACエンジニアが送信し、人間による調査が必要になります。

Subject

SR番号：さらなる調査が必要

メッセージ

お客様各位

私の名前は{your_name}です。あなたの申し立てを承諾しました。引き続きCisco Technical Assistance Center(TAC)にご協力いただき、ありがとうございます。

SD-WAN制御コンポーネントから提供されたadmin-techファイルの予備分析の後、分析を完了するにはさらにTACによる調査が必要であることがわかりました。よりの確で徹底した解決を図るため、次のステップでは皆さんと緊密に連携していきます。

シスコは次のステップを通じてお客様をサポートすることに尽力しており、状況に効果的に対処するための明確なガイダンスを提供します。

このリスクを軽減する上で最も重要なステップとして、アップグレードの計画と実行に優先順位を付けてください。このアップグレードをまだスケジュールしていない場合は、すぐにスケジュールしてください。

ご不明な点やご不明な点がございましたら、お気軽にTACエンジニアまでお問い合わせください。

ご協力ありがとうございます。

よろしくお願いします。

Outlookで開く

①送信前に[かっこ付きのプレースホルダ]をすべて置き換えてください。

✉ Outlook（本文付き）を開く

↓ .emlテンプレートのダウンロード

TAC 2 – 結果 – IoCが見つかりません（エンジニア確認）

使用例

自動化によってセキュリティ侵害の指標が見つからず、エンジニアが結果を確認した後に、TACエンジニアから送信されます。

Subject

更新：TACレビュー完了 – CVE-2026-20182のIoCが見つかりません – ケース[SR #]

メッセージ

[顧客名]様

担当のCisco TACエンジニア[SR Number]と申します。

SD-WAN制御コンポーネントから提供されたadmin-techファイルの予備スキャンを実行した後、『Cisco SD-WANセキュリティアドバイザリ：

- Cisco Catalyst SD-WANコントローラにおける認証バイパスの脆弱性[1]
- Cisco Catalyst SD-WAN Managerの脆弱性[2]

ただし、すべてのSD-WAN制御コンポーネントを<insert version>にアップグレードする必要があります。アップグレードを続行する手順を次に示します。

- Catalyst SD-WANアップグレードの開始[3]
- Cisco SD-WANアップグレードガイド[4]

インターネット上でのIPアドレッシングは動的に行われる性質を持ち、お客様のネットワーク内のエッジデバイスに必要なIPアドレスを把握していないため、シスコではエッジデバイスからのログを評価できないことに注意してください。この手順を手動で完了するには、『Cisco Catalyst SD-WANコントローラ認証バイパスの脆弱性セキュリティアドバイザリ』に記載されているピアリングイベント検証ガイダンスに従うことをお勧めします。また、『Security Advisory for CVE-2026-20182』で説明されている、ピアリングイベントの検証に関連する追加の検出手順を実行することも推奨されます。

リンク

[1] Cisco Catalyst SD-WANコントローラの認証バイパスの脆弱性 –

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW>

[2] Cisco Catalyst SD-WAN Managerの脆弱性 –

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-mltnps2-JxpWm7R>

[3] Catalyst SD-WANアップグレードの開始 : <https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/225515-start-your-catalyst-sd-wan-upgrade.html>

[4] Cisco SD-WANアップグレードガイド – <https://www.cisco.com/c/en/us/support/docs/wan/dpt/220424-upgrade-sd-wan-controllers-with-the-use.html>

敬具

Outlookで開く

①送信前に[カッコ付きのプレースホルダ]をすべて置き換えてください。

✉ Outlookを開く (件名のみ)

↓ .emlテンプレートのダウンロード

TAC 3 – 検証 – オーバーレイでのIP所有権の確認

使用例

ログ分析中に表示された特定のIPアドレスがSD-WANオーバーレイインフラストラクチャに含まれているのか、含まれていたのかを顧客に尋ねるために、TACエンジニアから送信されます。

Subject

[SR #]:IPアドレスの検証が必要

メッセージ

[顧客名]様

私は[Your Name]と申します。担当のCisco TACエンジニアです。

SD-WAN制御コンポーネントから提供されたadmin-techファイルの継続的な分析の一部として、次のIPアドレスがSD-WANオーバーレイインフラストラクチャに含まれているか、以前に含まれていた

かを検証するためにご協力ください。

問題のIPアドレス：

- [IPアドレス1]
- [IPアドレス2]

アセスメントを完了するために、次の点を確認してください。

1. このIPアドレスは、現在SD-WANオーバーレイのコンポーネント（vManage、vSmart、vBond、エッジデバイスなど）に関連付けられていますか？
2. このIPアドレスは、以前に廃止されたか、IPが変更された可能性のあるSD-WAN制御コンポーネントによって使用されていましたか。
3. このIPは、ディザスタリカバリ(DR)サイトまたはSD-WAN展開に関連するその他のインフラストラクチャと関連付けられていますか。

迅速な対応により、引き続き分析を行い、適切な次のステップを提供します。

ご不明な点がございましたら、お気軽にお問い合わせください。

よろしくお願いします。

Outlookで開く

①送信前に[カッコ付きのプレースホルダ]をすべて置き換えてください。

✉ Outlook（本文付き）を開く

↓ .emlテンプレートのダウンロード

TAC 4 – 結果 – 誤検出のクリア

使用例

自動スキャンによってフラグが立てられた最初のIoCが誤検出と判断された後に、TACエンジニアから送信されます。

Subject

アップデート：CVE-2026-20182のテクニカルレビュー：ケース[ケース番号]

メッセージ

お客様各位

SD-WAN制御コンポーネントから提供されたadmin-techファイルの手動レビューをエンジニアリングチームが実施する間、しばらくお待ちください。

徹底した調査の結果、自動スキャンプロセスによってフラグが立てられた侵害の初期指標(IOC)が誤検出であったと判断しました。つまり、IOCが有効ではないという評価です。

重要：この特定のアラートはすでにクリアされていますが、[CVE-2026-20182](#)^[1]に関連する脆弱性には、SD-WANファブリックの長期的なセキュリティと整合性を確保するために、ソフトウェアのアップグレードが必要なことに注意してください。

アップグレードをまだ完了していない場合：可能な限り早く、SD-WAN制御コンポーネントのフルアップグレードに優先順位を付けてください。アップグレードは、この脆弱性を効果的に修正する唯一の方法です。詳細な手順については、『[Cisco SD-WAN Upgrade Guide](#)^[2]』を参照してください。

アップグレードをすでに完了している場合：この検出が誤検出として確認され、ソフトウェアの修復をすでに実行しているため、これ以上の操作は必要ありません。この問題は解決したと考え、標準的な終了手順に進むことができます。

貴社のインフラストラクチャのセキュリティを優先させて頂き、ありがとうございます。ご不明な点やご不明な点がございましたら、お気軽にお問い合わせください。

よろしくお願いいたします。

Cisco Technical Assistance Center (TAC)

リンク：

[1] [公式セキュリティアドバイザリ](#)

[2] [Cisco SD-WANアップグレードガイド](#)

Outlookで開く

①送信前に[かっこ付きのプレースホルダ]をすべて置き換えてください。

✉ Outlookを開く（件名のみ）

📎 .emlテンプレートのダウンロード

TAC 5 – 重要 – IOCが特定されました、スケジュール確認コール

使用例

潜在的なセキュリティ侵害の指標が確認され、判明した項目と次のステップについて話し合うためにお客様から緊急のコールが必要になった時点で、TACエンジニアから送信されます。

Subject

緊急：CVE-2026-20182の分析結果：侵害の兆候を特定

メッセージ

お客様各位

SD-WAN制御コンポーネントに提供されているadmin-techファイルを分析する間、しばらくお待ちください。

技術的なレビューに続き、CVE-2026-20182に関連する潜在的なIndicators of Compromise(IoC)を特定しました。

これらの調査結果の性質を考えると、できるだけ早く技術的な詳細と推奨される次のステップについて話し合うことが重要です。具体的な調査結果を確認し、適切な改善策について話し合うために、御社のチームとの電話スケジュールを設定したいと考えています。

次のステップ：

- ・ 会議のスケジュールを設定する：調査結果を確認するために、近日中に必要な短い電話についてお知らせください（4～8時間以内など）。
- ・ SDWAN制御コンポーネントのアップグレード:SDWAN Manager、Controller、およびValidatorを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。

シスコの主な目標は、お客様の環境を保護し、潜在的なリスクを軽減することです。本件に関する迅速な対応に感謝するとともに、貴社との調整を楽しみにしています。

よろしくお願いします。

Outlookで開く

①送信前に[カッコ付きのプレースホルダ]をすべて置き換えてください。

✉ Outlook（本文付き）を開く

📎 .emlテンプレートのダウンロード

TAC 6 – 結果 – IoCの重複（終了およびリダイレクト）

使用例

IoC分析で同じ顧客/環境の以前のSRと一致する結果が確認されたときに、TACエンジニアから送信されます。現在のケースはクローズされ、お客様は修復ガイダンスがすでに提供されている元のSRにリダイレクトされます。

Subject

アップデート：CVE-2026-20182のテクニカルレビュー：ケース[SR #]（重複IoCが確認されました）

メッセージ

お客様各位

SD-WAN制御コンポーネントに提供されているadmin-techファイルを分析する間、しばらくお待ちください。シスコのスキャンングプロセスによってフラグが付けられた最初のIndicator of Compromise(IoC)は、[Original SR #]ですすでに伝達されているものと同じであると判断しました。前述したように、可能な限り早く環境を保護するために、緊急アップグレードを行い、『[TAC Remediation Guide](#)^[2]』に記載されている2つの修復パスのいずれかを使用して対処することを推奨します。詳細については、[CVE-2026-20182](#)^[1]の公式セキュリティアドバイザリを参照してください。

それでは私はこの案件のクローズに進みます。アップグレードまたは修復に関する詳細なガイダンスまたはテクニカルサポートを依頼するには、[元のSR番号]を使用してください。

よろしく申し上げます。

[名前]

リンク:

[1][公式セキュリティアドバイザリ](#)

[2][TAC修復ガイド](#)

Outlookで開く

①送信前に[かっこ付きのプレースホルダ]をすべて置き換えてください。

✉ Outlook（本文付き）を開く

📎 .emlテンプレートのダウンロード

TAC 7 – 修復 – オプションのフォローアップ（ポストコール）

使用例

IoCレビューコールの後に送信され、説明した修復パスを要約します。お客様は、オプションA（ローリングリスタートによる再導入）、オプションB（ハードカットオーバーによる再導入）、またはオプションC（フルシステムリビルド）を選択します。

Subject

メッセージ

お客様各位

今回の分析で判明した点について、お時間をいただき、ありがとうございました。前のコールで説明したように、環境を保護するために、次のいずれかの修復パスを使用して作業を進めることをお勧めします。

オプションA：ローリングリスタートによる再導入ネットワークのダウンタイムを回避することで運用継続性を優先しますが、移行プロセス中も脅威が存続するリスクが残ります。

説明：コントローラの再導入、およびSSHキーと証明書のローテーションを行います。既存のコントローラコンポーネントはvManageを介して移行中に接続され、新しいファブリックが導入されます。デバイスが移行されるとすぐにそれぞれ削除されます。

オプションB：ハードカットオーバーによる再導入より高いレベルのセキュリティ保証を提供します。新しいコントローラが古いコントローラに接続することはないため、完全な分離が行われます。これにより、すべてのデバイスで接続を再確立し、ルート/接続情報を交換する必要があるため、ネットワーク全体の運用に影響が及びます。停止時間は、サイトの数、交換されるプレフィックスの数などによって異なります。

説明：コントローラの再導入とSSHキーおよび証明書のローテーションを伴いますが、古いコントローラコンポーネントは再導入時に新しいファブリックから分離されます。

オプションC：システムの完全な再構築クリーンなベースラインを確立することで最高レベルのセキュリティ保証を提供しますが、これは最も複雑なアプローチであり、再構築中に設定に関連する不安定性が発生するリスクが高くなります。これは時間のかかるオプションであり、テンプレートとポリシーデータベースの再構築に関する専門知識が必要です。

次のステップ：

- これらの選択肢について社内で話し合い、どちらの方法を使用するかを決定してください。お客様が決定したら、実行フェーズを通してお客様を支援するための詳細なガイドンスまたはテクニカルサポートを提供できます。

シスコは、このプロセス全体を通じてお客様をサポートします。これらのオプションに関するご質問は、お問い合わせください。

よろしくお願いします。

Cisco Technical Assistance Center (TAC)

注：オプション1はアップグレードです。このアップグレードを考慮したシナリオはすでに実行されています。

Outlookで開く

①次の.emlダウンロードを使用します。送信する前に、すべての[カッコ付きプレースホルダ]を置き換えてください。

✉ Outlookを開く（件名のみ）

↓ .emlテンプレートのダウンロード

TAC 8 – 修復 – 侵害されたファブリックの更新されたオプション（オプション2のフォローアップ）

使用例

SD-WANファブリックが侵害され、以前にオプション2を実行したことがあり、そのファブリックが脅威アクターの永続性のリスクが残っていると考えられる顧客に通知する。セキュリティ侵害を受けたファブリックを再構築したお客様（およびバックアップ/既存のconfigDBに依存しなかったお客様）は、リスクがあると推測されず、この通信を受け取ることはありません。この通信は未定で送信されます。

Subject

緊急措置が必要：SD-WANインフラストラクチャの重大な脆弱性の修復

メッセージ

お客様各位

お客様のSD-WANファブリックを修復するための重要なアップデートを[SR#]および以前にお知らせしたセキュリティアドバイザリに記載の方法で提供します。このアップデートは、提供されたログがIndicators of Compromise(IOC)の証拠を示したファブリックに固有のものです。

以前はオプション2に基づく修復計画（ソフトウェアアップグレード、コントローラの再導入、SSHキーローテーションを組み込む）を選択されましたが、脅威の状況に対するシスコの分析は進化を続けています。これらの脆弱性のエクスポイトに関する新しい技術的な洞察から、持続性のリスクを軽減し、証明書チェーンの整合性を確保するために、追加の対策が強く求められることがわかります。

アクションが必要:

ルート証明書のローテーションを追加することで、より包括的な防御を提供できるように、推奨される修復方法を更新しました。

この修正では、ネットワークの計画的なダウンタイムを含む、追加のメンテナンス作業が必要になる場合があります。

お客様のネットワークのセキュリティと整合性がシスコの優先事項であることを踏まえ、3つの異なる修復オプションを開発しました。次の各オプションでは、運用上の影響とセキュリティ保証のバランスを考慮に入れて説明します。社内リスクポスチャは独自のものであるため、シスコは特定のパスを推奨できません。

オプションA：ローリングリスタートによる再導入ネットワークのダウンタイムを回避することで運用継続性を優先しますが、移行プロセス中も脅威が存続するリスクが残ります。

説明：コントローラの再導入、およびSSHキーと証明書のローテーションを行います。既存のコントローラコンポーネントはvManageを介して移行中に接続され、新しいファブリックが導入されます。デバイスが移行されるとすぐにそれぞれ削除されます。

オプションB：ハードカットオーバーによる再導入より高いレベルのセキュリティ保証を提供します。新しいコントローラが古いコントローラに接続することはないため、完全な分離が行われます。これにより、すべてのデバイスで接続を再確立し、ルート/接続情報を交換する必要があるため、ネットワーク全体の運用に影響が及びます。停止時間は、サイトの数、交換されるプレフィックスの数などによって異なります。

説明：コントローラの再導入とSSHキーおよび証明書のローテーションを伴いますが、古いコントローラコンポーネントは再導入時に新しいファブリックから分離されます。

オプションC：システムの完全な再構築クリーンなベースラインを確立することで最高レベルのセキュリティ保証を提供しますが、これは最も複雑なアプローチであり、再構築中に設定に関連する不安定性が発生するリスクが高くなります。これは時間のかかるオプションであり、テンプレートとポリシーデータベースの再構築に関する専門知識が必要です。

これらのオプションを確認し、リスク管理基準に最も適したアプローチを特定したら、このメッセージに返信してお知らせください。お客様の選択を受け取った後、メンテナンス期間を調整し、実行に必要な技術的な準備を開始します。

引き続き、安全なネットワークインフラストラクチャの維持に努めていただき、ありがとうございます。さらに技術的な説明が必要な場合は、Technical Assistance Center(TAC)でサービスリクエスト(SR)をオープンし、ご連絡ください。

敬具

『シスコ

Outlookで開く

①次の.emlダウンロードを使用します。送信する前に、すべての[カッコ付きプレースホルダ]を置き換えてください。

TAC 17 – リバーズ検索 – 以前はIoCを使用していなかったが、現在はIoCを使用している(CVE-2026-20182)

使用例

以前にIndicators of Compromise(IoC)が見つからないと通知されたお客様に送信されますが、その後のadmin-techログの内部レビューでCVE-2026-20182に関連するIoCが特定されています。改訂された結果を通知し、3つの修正オプション（オプションA、B、またはC）を提供します。

Subject

重要アップデート：CVE-2026-20182のIoCアセスメントの改訂 – 侵害の指標を確認済み – SR [SR#]

メッセージ

お客様各位

サービスリクエスト[SR#]の下、CVE-2026-20182に関して、Cisco Technical Assistance Center(TAC)にご協力いただき、ありがとうございます。

以前の対応では、SD-WANコントロールコンポーネントから提供されたadmin-techファイルの分析で、このアドバイザリに関連するIndicators of Compromise(IoC)が特定されなかったことをお知らせしました。お客様のセキュリティに対する継続的な取り組みの一環として、シスコはその後、お客様の組織のファブリックに関連する追加のadmin-techログデータの定期的な内部レビューを実施しました。

この後のレビューでは、最初のアセスメントで提示されなかったセキュリティ侵害の指標(IoC)を特定しました。これらの調査結果に対応するため、現在、シスコはお客様と協力して取り組んでいます。これらのIoCは、組織のファブリック内で修復処理を保証する疑わしいアクティビティが発生している可能性を示します。

シスコは、お客様に以前に伝達した結果を見直すことを認識しています。適切な修復を行うことができるように、お客様の環境を明確かつ正確に把握することを望んでいます。

アクションが必要:

この修正では、ネットワークの計画的なダウンタイムを含む、追加のメンテナンス作業が必要になる場合があります。

お客様のネットワークのセキュリティと整合性がシスコの優先事項であることを踏まえ、3つの異

なる修復オプションを開発しました。次の各オプションでは、運用上の影響とセキュリティ保証のバランスを考慮に入れて説明します。社内リスクポスチャは独自のものであるため、シスコは特定のパスを推奨できません。

オプションA：ローリングリスタートによる再導入ネットワークのダウンタイムを回避することで運用継続性を優先しますが、移行プロセス中も脅威が存続するリスクが残ります。

説明：コントローラの再導入、およびSSHキーと証明書のローテーションを行います。既存のコントローラコンポーネントはvManageを介して移行中に接続され、新しいファブリックが導入されます。デバイスが移行されるとすぐにそれぞれ削除されます。

オプションB：ハードカットオーバーによる再導入より高いレベルのセキュリティ保証を提供します。新しいコントローラが古いコントローラに接続することはないため、完全な分離が行われます。これにより、すべてのデバイスで接続を再確立し、ルート/接続情報を交換する必要があるため、ネットワーク全体の運用に影響が及びます。停止時間は、サイトの数、交換されるプレフィックスの数などによって異なります。

説明：コントローラの再導入とSSHキーおよび証明書のローテーションを伴いますが、古いコントローラコンポーネントは再導入時に新しいファブリックから分離されます。

オプションC：システムの完全な再構築クリーンなベースラインを確立することで最高レベルのセキュリティ保証を提供しますが、これは最も複雑なアプローチであり、再構築中に設定に関連する不安定性が発生するリスクが高くなります。これは時間のかかるオプションであり、テンプレートとポリシーデータベースの再構築に関する専門知識が必要です。

これらのオプションを確認し、リスク管理基準に最も適したアプローチを特定したら、このメッセージに返信してお知らせください。お客様の選択を受け取った後、メンテナンス期間を調整し、実行に必要な技術的な準備を開始します。

引き続き、安全なネットワークインフラストラクチャの維持に努めていただき、ありがとうございます。この電子メールに返信するか、Technical Assistance Center(TAC)の既存のサービスリクエスト(SR)を通じて、さらに技術的な説明が必要な場合はお知らせください。

敬具

『シスコ

Outlookで開く

① 次の .eml ダウンロードを使用します。送信する前に、すべての[カッコ付きプレースホルダ]を置き換えてください。

✉ Outlookを開く（件名のみ）

📎 .emlテンプレートのダウンロード

CloudOps 1 – プロアクティブ – クラウドスキャンでIoCが検出され、Admin-Techによる検証が必要

使用例

クラウドホスト型SD-WANファブリックのCisco CloudOpsセキュリティスキャンで潜在的なIndicators of Compromise(IoC)が検出されたときにプロアクティブに送信されます。お客様に代わってSRが開かれ、ログの完全分析を通じて検索結果を検証できるように、admin-techファイルを添付するよう求められます。

Subject

必要なアクション：セキュリティスキャン結果の検証にAdmin-Techファイルが必要 – SR [SR#]

メッセージ

お客様各位

シスコは先日、シスコオファアーの整合性のセキュリティ保護と監視に取り組む一環として、クラウドホスト型SD-WANファブリックのセキュリティスキャンを完了しました。このアクションは、報告されたセキュリティ上の問題に対して実行されました。スキャンにより、組織のファブリック内で疑わしい可能性のあるアクティビティが特定され、さらなる調査が必要になります。

このサービスリクエスト(SR)にadmin-techファイルを添付して、お客様の代わりに開いてもらえるようお願いしています。これにより、調査結果を検証し、調査を完了することができます。

完全な分析を有効にするには、すべてのSD-WAN制御コンポーネントからadmin-techファイルを収集してアップロードしてください。これらのファイルを生成する際には、必ず「Logs」と「Tech」の両方を選択してください。

- vSmarts (コントローラ):同時に収集するのではなく、一度に1つずつ収集します。
- vBonds (バリデータ):すべてのノードから収集します。
- マネージャ(vManage):クラスタ内のすべてのノード(アクティブおよびスタンバイDR)から収集します。

admin-techファイルを生成して安全に送信する手順を追った詳細な手順については、『[Cisco SD-WAN Admin-Tech Collection Guide](#)^[1]』を参照してください。

リクエストされたファイルを受け取ったら、当社のチームがファイルを分析し、確認されたアクティビティが侵害の真の指標であるかどうかを確認し、適切な次のステップについてアドバイスします。

引き続き、安全なネットワークインフラストラクチャの維持に努めていただき、ありがとうございます。このサービスリクエスト(SR)に返信して、技術的な詳細説明が必要な場合はお知らせください。

よろしくお願いします。

『シスコ

リンク:

[1] [Cisco SD-WAN Admin-Tech Collectionガイド](#)

Outlookで開く

①次の .eml ダウンロードを使用します。送信する前に、すべての[カッコ付きプレースホルダ]を置き換えてください。

✉ Outlookを開く（件名のみ）

↓ .emlテンプレートのダウンロード

以前に影響を受けたことがあり、オプションA、B、またはCを完了していないお客様へのWAVE 2Aの電子メール（オプション1と2を再実行する必要があります）

PSIRT2aのIOCがない場合のTAC 9テンプレート/リビルドが実施された(以前は影響を受けた)

使用例

SD-WANログでPSIRT2a忠告に関連するIndicators of Compromise(IoC)が示されず、ファブリックが以前に再構築されたお客様に送信されます。3つのオプション（オプション2のフォローアップ）を含む更新された修復ガイダンスを提供します。

Subject

緊急措置が必要：SD-WANインフラストラクチャの重大な脆弱性の修復 – SR [SR#]

メッセージ

お客様各位

サービスリクエスト[SR#]に記載されている最近のSD-WAN PSIRTアドバイザリに関して、Cisco Technical Assistance Center(TAC)にご連絡いただきありがとうございます。

SD-

WANファブリックから提供されたログと情報を確認した結果、2026年6月5日のSD-WAN脆弱性アドバイザリに関連するIndicators of Compromise(IOC)は見つかりませんでした。さらに、以前のアドバイザリに関連する修復の一環として、お客様の環境が以前に再構築されたことを理解しています。

これらの脆弱性に関して新たに特定された知見を踏まえ、SD-WANファブリックの推奨される修復ガイダンスに関する重要な最新情報をお知らせいたします。

お客様のSD-WANファブリックを修復するための重要なアップデートを[SR#]および以前にお知らせしたセキュリティアドバイザリに記載の方法で提供します。

以前はオプション2に基づく修復計画(ソフトウェアアップグレード、コントローラの再導入、SSHキーローテーションを組み込む)を選択されましたが、脅威の状況に対するシスコの分析は進化を続けています。これらの脆弱性のエクスポイトに関する新しい技術的な洞察から、持続性のリスクを軽減し、証明書チェーンの整合性を確保するために、追加の対策が強く求められることがわかります。

アクションが必要:

ルート証明書のローテーションを追加することで、より包括的な防御を提供できるように、推奨される修復方法を更新しました。

この修正では、ネットワークの計画的なダウンタイムを含む、追加のメンテナンス作業が必要になる場合があります。お客様のネットワークのセキュリティと整合性がシスコの優先事項であることを踏まえ、3つの異なる修復オプションを開発しました。次の各オプションでは、運用上の影響とセキュリティ保証のバランスを考慮に入れて説明します。社内リスクポスチャは独自のものであるため、シスコは特定のパスを推奨できません。

オプションA: ローリングリスタートによる再導入ネットワークのダウンタイムを回避することで運用継続性を優先しますが、移行プロセス中も脅威が存続するリスクが残ります。

説明: コントローラの再導入、およびSSHキーと証明書のローテーションを行います。既存のコントローラコンポーネントはvManageを介して移行中に接続され、新しいファブリックが導入されます。デバイスが移行されるとすぐにそれぞれ削除されます。

オプションB: ハードカットオーバーによる再導入より高いレベルのセキュリティ保証を提供します。新しいコントローラが古いコントローラに接続することはないため、完全な分離が行われます。これにより、すべてのデバイスで接続を再確立し、ルート/接続情報を交換する必要があるため、ネットワーク全体の運用に影響が及びます。停止時間は、サイトの数、交換されるプレフィックスの数などによって異なります。

説明: コントローラの再導入とSSHキーおよび証明書のローテーションを伴いますが、古いコント

ローラコンポーネントは再導入時に新しいファブリックから分離されます。

オプションC：システムの完全な再構築クリーンなベースラインを確立することで最高レベルのセキュリティ保証を提供しますが、これは最も複雑なアプローチであり、再構築中に設定に関連する不安定性が発生するリスクが高くなります。これは時間のかかるオプションであり、テンプレートとポリシーデータベースの再構築に関する専門知識が必要です。

これらのオプションを確認し、リスク管理基準に最も適したアプローチを特定したら、このメッセージに返信してお知らせください。お客様の選択を受け取った後、メンテナンス期間を調整し、実行に必要な技術的な準備を開始します。

引き続き、安全なネットワークインフラストラクチャの維持に努めていただき、ありがとうございます。この電子メールに返信するか、既存のサービスリクエストを通じて、技術的な詳細説明が必要な場合はお知らせください。

敬具

『シスコ

Outlookで開く

①次の.emlダウンロードを使用します。送信する前に、すべての[カッコ付きプレースホルダ]を置き換えてください。

✉ Outlookを開く（件名のみ）

📎 .emlテンプレートのダウンロード

PSIRT2aのIOCがyesの場合にTAC 10テンプレートを作成/再構築を実施(以前は影響あり)

使用例

SD-WANログにPSIRT2a忠告に関連するIndicators of Compromise(IoC)が示され、ファブリックが以前に再構築されたお客様に送信されます。3つのオプション（オプション2のフォローアップ）を含む更新された修復ガイダンスを提供します。

Subject

緊急措置が必要：SD-WANインフラストラクチャの重大な脆弱性の修復 – SR [SR#]

メッセージ

お客様各位

サービスリクエスト[SR#]に記載されている最近のSD-WAN PSIRTアドバイザリに関して、Cisco Technical Assistance Center(TAC)にご連絡いただきありがとうございます。

SD-WANファブリックから提供されたログを分析した後、シスコのチームは2026年6月5日のSD-WAN脆弱性アドバイザリに関連するIndicators of Compromise(IOC)を特定しました。また、以前のアドバイザリに関連する修復手順の一環として、お客様の環境が以前に再構築されたことも理解しています。

お客様のSD-WANファブリックを修復するための重要なアップデートを[SR#]および以前にお知らせしたセキュリティアドバイザリに記載の方法で提供します。このアップデートは、提供されたログがIndicators of Compromise(IOC)の証拠を示したファブリックに固有のものです。

以前はオプション2に基づく修復計画(ソフトウェアアップグレード、コントローラの再導入、SSHキーローテーションを組み込む)を選択されましたが、脅威の状況に対するシスコの分析は進化を続けています。これらの脆弱性のエクスポイトに関する新しい技術的な洞察から、持続性のリスクを軽減し、証明書チェーンの整合性を確保するために、追加の対策が強く求められることがわかります。

アクションが必要:

ルート証明書のローテーションを追加することで、より包括的な防御を提供できるように、推奨される修復方法を更新しました。

この修正では、ネットワークの計画的なダウンタイムを含む、追加のメンテナンス作業が必要になる場合があります。お客様のネットワークのセキュリティと整合性がシスコの優先事項であることを踏まえ、3つの異なる修復オプションを開発しました。次の各オプションでは、運用上の影響とセキュリティ保証のバランスを考慮に入れて説明します。社内リスクポスチャは独自のものであるため、シスコは特定のパスを推奨できません。

オプションA: ローリングリスタートによる再導入ネットワークのダウンタイムを回避することで運用継続性を優先しますが、移行プロセス中も脅威が存続するリスクが残ります。

説明: コントローラの再導入、およびSSHキーと証明書のローテーションを行います。既存のコントローラコンポーネントはvManageを介して移行中に接続され、新しいファブリックが導入されます。デバイスが移行されるとすぐにそれぞれ削除されます。

オプションB: ハードカットオーバーによる再導入より高いレベルのセキュリティ保証を提供します。新しいコントローラが古いコントローラに接続することはないため、完全な分離が行われます。これにより、すべてのデバイスで接続を再確立し、ルート/接続情報を交換する必要があるため、ネットワーク全体の運用に影響が及びます。停止時間は、サイトの数、交換されるプレフィックスの数などによって異なります。

説明：コントローラの再導入とSSHキーおよび証明書のローテーションを伴いますが、古いコントローラコンポーネントは再導入時に新しいファブリックから分離されます。

オプションC：システムの完全な再構築クリーンなベースラインを確立することで最高レベルのセキュリティ保証を提供しますが、これは最も複雑なアプローチであり、再構築中に設定に関連する不安定性が発生するリスクが高くなります。これは時間のかかるオプションであり、テンプレートとポリシーデータベースの再構築に関する専門知識が必要です。

これらのオプションを確認し、リスク管理基準に最も適したアプローチを特定したら、このメッセージに返信してお知らせください。お客様の選択を受け取った後、メンテナンス期間を調整し、実行に必要な技術的な準備を開始します。

引き続き、安全なネットワークインフラストラクチャの維持に努めていただき、ありがとうございます。この電子メールに返信するか、既存のサービスリクエストを通じて、技術的な詳細説明が必要な場合はお知らせください。

敬具

『シスコ

Outlookで開く

①次の.emlダウンロードを使用します。送信する前に、すべての[カッコ付きプレースホルダ]を置き換えてください。

✉ Outlookを開く（件名のみ）

↓ .emlテンプレートのダウンロード

PSIRT2a用のIOCがない場合のTAC 11テンプレート/それらが再構築されなかった (以前に影響を受けた)

使用例

SD-WANログにPSIRT2aアドバイザーに関連するIndicators of Compromise(IoC)が示されず、ファブリックが再構築されなかったお客様に送信されます。3つのオプション（オプション1のフォローアップ）を含む更新された修復ガイダンスを提供します。

Subject

緊急措置が必要：SD-WANインフラストラクチャの重大な脆弱性の修復 – SR [SR#]

メッセージ

お客様各位

サービスリクエスト[SR#]に記載されている最近のSD-WAN PSIRTアドバイザリに関して、Cisco Technical Assistance Center(TAC)にご連絡いただきありがとうございます。

SD-WANファブリックから提供されたログと情報を確認した結果、2026年6月5日のSD-WAN脆弱性アドバイザリに関連するIndicators of Compromise(IOC)を特定できませんでした。

また、前のアドバイザリに従って、お客様の環境が完全に再構築されていないことも理解しています。潜在的な発症を減らし、SD-WAN証明書の信頼チェーンの整合性を強化するために、以下の更新された修復ガイダンスを確認することをお勧めします。

これを念頭に、[SR#]および以前に通知されたセキュリティアドバイザリに記載されているように、SD-WANファブリックの修復に関する重要な更新を提供します。

以前はオプション1に基づいて修復計画を選択されましたが(ソフトウェアアップグレードとSSHキーローテーションを組み込む)、脅威の状況に関するシスコの分析は進化し続けています。これらの脆弱性のエクスプロイトに関する新しい技術的な洞察から、持続性のリスクを軽減し、証明書チェーンの整合性を確保するために、追加の対策が強く求められることがわかります。

アクションが必要:

ルート証明書のローテーションを追加することで、より包括的な防御を提供できるように、推奨される修復方法を更新しました。

この修正では、ネットワークの計画的なダウンタイムを含む、追加のメンテナンス作業が必要になる場合があります。お客様のネットワークのセキュリティと整合性がシスコの優先事項であることを踏まえ、3つの異なる修復オプションを開発しました。次の各オプションでは、運用上の影響とセキュリティ保証のバランスを考慮に入れて説明します。社内リスクポスチャは独自のものであるため、シスコは特定のパスを推奨できません。

オプションA: ローリングリスタートによる再導入ネットワークのダウンタイムを回避することで運用継続性を優先しますが、移行プロセス中も脅威が存続するリスクが残ります。

説明: コントローラの再導入、およびSSHキーと証明書のローテーションを行います。既存のコントローラコンポーネントはvManageを介して移行中に接続され、新しいファブリックが導入されます。デバイスが移行されるとすぐにそれぞれ削除されます。

オプションB: ハードカットオーバーによる再導入より高いレベルのセキュリティ保証を提供します。新しいコントローラが古いコントローラに接続することはないため、完全な分離が行われます。これにより、すべてのデバイスで接続を再確立し、ルート/接続情報を交換する必要があるため

、ネットワーク全体の運用に影響が及びます。停止時間は、サイトの数、交換されるプレフィックスの数などによって異なります。

説明：コントローラの再導入とSSHキーおよび証明書のローテーションを伴いますが、古いコントローラコンポーネントは再導入時に新しいファブリックから分離されます。

オプションC：システムの完全な再構築クリーンなベースラインを確立することで最高レベルのセキュリティ保証を提供しますが、これは最も複雑なアプローチであり、再構築中に設定に関連する不安定性が発生するリスクが高くなります。これは時間のかかるオプションであり、テンプレートとポリシーデータベースの再構築に関する専門知識が必要です。

これらのオプションを確認し、リスク管理基準に最も適したアプローチを特定したら、このメッセージに返信してお知らせください。お客様の選択を受け取った後、メンテナンス期間を調整し、実行に必要な技術的な準備を開始します。

引き続き、安全なネットワークインフラストラクチャの維持に努めていただき、ありがとうございます。この電子メールに返信するか、既存のサービスリクエストを通じて、技術的な詳細説明が必要な場合はお知らせください。

敬具

『シスコ

Outlookで開く

①次の.emlダウンロードを使用します。送信する前に、すべての[カッコ付きプレースホルダ]を置き換えてください。

✉ Outlookを開く（件名のみ）

↓ .emlテンプレートのダウンロード

PSIRT2aのIOCがyesの場合にTAC 12テンプレートが再構築されなかった(以前に影響を受けた)

使用例

SD-WANログにPSIRT2aアドバイザーに関連するIndicators of Compromise(IoC)が記録され、ファブリックが再構築されなかったお客様に送信されます。3つのオプション（オプション1のフォローアップ）を含む更新された修復ガイダンスを提供します。

Subject

緊急措置が必要：SD-WANインフラストラクチャの重大な脆弱性の修復 – SR [SR#]

メッセージ

お客様各位

サービスリクエスト[SR#]に記載されている最近のSD-WAN PSIRTアドバイザリに関して、Cisco Technical Assistance Center(TAC)にご連絡いただきありがとうございます。

SD-WANファブリックから提供されたログを分析した後、シスコのチームは2026年6月5日のSD-WAN脆弱性アドバイザリに関連するIndicators of Compromise(IOC)を特定しました。さらに、お客様の環境では、以前のアドバイザリに従って完全な再構築が行われていないことを理解しています。

これらのインジケータの存在と、脅威の状況に対する理解の進展を踏まえ、持続性のリスクを軽減し、SD-WAN証明書の信頼チェーンの整合性を確保するために、以下に示す更新された修復ガイドンスを確認して実装することが重要です。

お客様のSD-WANファブリックを修復するための重要なアップデートを[SR#]および以前にお知らせしたセキュリティアドバイザリに記載の方法で提供します。このアップデートは、提供されたログがIndicators of Compromise(IOC)の証拠を示したファブリックに固有のものであります。

以前はオプション1に基づいて修復計画を選択されましたが(ソフトウェアアップグレードとSSHキーローテーションを組み込む)、脅威の状況に関するシスコの分析は進化し続けています。これらの脆弱性のエクスプロイトに関する新しい技術的な洞察から、持続性のリスクを軽減し、証明書チェーンの整合性を確保するために、追加の対策が強く求められることがわかります。

アクションが必要:

ルート証明書のローテーションを追加することで、より包括的な防御を提供できるように、推奨される修復方法を更新しました。

この修正では、ネットワークの計画的なダウンタイムを含む、追加のメンテナンス作業が必要になる場合があります。お客様のネットワークのセキュリティと整合性がシスコの優先事項であることを踏まえ、3つの異なる修復オプションを開発しました。次の各オプションでは、運用上の影響とセキュリティ保証のバランスを考慮に入れて説明します。社内リスクポスチャは独自のものであるため、シスコは特定のパスを推奨できません。

オプションA: ローリングリスタートによる再導入ネットワークのダウンタイムを回避することで運用継続性を優先しますが、移行プロセス中も脅威が存続するリスクが残ります。

説明: コントローラの再導入、およびSSHキーと証明書のローテーションを行います。既存のコントローラコンポーネントはvManageを介して移行中に接続され、新しいファブリックが導入されます。デバイスが移行されるとすぐにそれぞれ削除されます。

オプションB: ハードカットオーバーによる再導入より高いレベルのセキュリティ保証を提供しま

す。新しいコントローラが古いコントローラに接続することはないため、完全な分離が行われます。これにより、すべてのデバイスで接続を再確立し、ルート/接続情報を交換する必要があるため、ネットワーク全体の運用に影響が及びます。停止時間は、サイトの数、交換されるプレフィックスの数などによって異なります。

説明：コントローラの再導入とSSHキーおよび証明書のローテーションを伴いますが、古いコントローラコンポーネントは再導入時に新しいファブリックから分離されます。

オプションC：システムの完全な再構築クリーンなベースラインを確立することで最高レベルのセキュリティ保証を提供しますが、これは最も複雑なアプローチであり、再構築中に設定に関連する不安定性が発生するリスクが高くなります。これは時間のかかるオプションであり、テンプレートとポリシーデータベースの再構築に関する専門知識が必要です。

これらのオプションを確認し、リスク管理基準に最も適したアプローチを特定したら、このメッセージに返信してお知らせください。お客様の選択を受け取った後、メンテナンス期間を調整し、実行に必要な技術的な準備を開始します。

引き続き、安全なネットワークインフラストラクチャの維持に努めていただき、ありがとうございます。この電子メールに返信するか、既存のサービスリクエストを通じて、技術的な詳細説明が必要な場合はお知らせください。

敬具

『シスコ

Outlookで開く

①次の.emlダウンロードを使用します。送信する前に、すべての[カッコ付きプレースホルダ]を置き換えてください。

✉ Outlookを開く（件名のみ）

↓ .emlテンプレートのダウンロード

新規のお客様向けWAVE 2A用Eメール（以前は影響を受けていません）

TAC 13 Template for no IOC / No Fixed Release Available(WAVE 2a — Await Fix)

使用例

SD-WANログにCVE-2026-20245に関連するIndicators of Compromise(IoC)が示されていないお客様に送信されます。ただし、お客様のプラットフォームおよびバージョンで現在使用できる修正済みソフトウェアリリースはありません。お客様に対し、暫定的な強化策を適用し、修正済みリリースの通知を待つように助言します。

Subject

アップデート：CVE-2026-20245のIoCアセスメント完了 – 修正済みリリースは現在利用不可 – SR [SR#]

メッセージ

お客様各位

サービスリクエスト[SR#]に基づき、CVE-2026-20245に関してCisco Technical Assistance Center(TAC)にご連絡いただきありがとうございます。

SD-WAN制御コンポーネントから提供されたadmin-techファイルの分析が完了しました。CVE-2026-20245に関連するIndicators of Compromise(IoC)は確認されたログに見つかりませんでした。

このレビューのために取得してシスコに提供するログデータの量は、[シスコSD-WAN強化ガイド](#)^[1]に従ってお客様の環境に設定されたログ保持期間によって制限されている可能性があります。

重要：修正済みソフトウェアリリースは現在提供されていません。

現在のプラットフォームおよびソフトウェアバージョンでは、この脆弱性を修正する修正済みソフトウェアリリースはありません。シスコのエンジニアリング部門では、修正済みリリースの提供に積極的に取り組んでいます。修正済みソフトウェアが入手可能になると、[公式のセキュリティアドバイザリ](#)^[2]が修正済みリリース情報で更新されます。

推奨される暫定処理：

修正済みリリースのリリースを待っている間は、次の強化対策を実施して問題の発生を抑えることを強くお勧めします。

- 強化のベストプラクティスの適用：『[Cisco SD-WAN強化ガイド](#)^[1]』の推奨事項を確認して実装し、攻撃対象を減らします。
- セキュリティアドバイザリを監視する：ご使用のプラットフォームの修正済みリリースの入手に関するアップデートについては、[公式のセキュリティアドバイザリ](#)^[2]を定期的に確認してください。
- アップグレードの計画：修正済みリリースの公開後すぐにアップグレードを実行できるように、アップグレード計画を今すぐ開始します。
- 環境の監視：異常な動作や予期しない設定変更がないか、SD-WAN制御コンポーネントの監視を

続行します。

次のステップ：

修正済みソフトウェアリリースが利用可能になった時点で、このケースを更新します。その時点で、できるだけ早く、すべてのSD-WAN制御コンポーネント（マネージャ、コントローラ、バリデータ）を修正バージョンにアップグレードすることを優先する必要があります。

BCS/LCSサブスクリプションをお持ちの場合は、アップグレード計画に関する追加ガイダンスについて、Cisco NCEまたはデリバリマネージャにお問い合わせください。

インフラストラクチャのセキュリティに対する皆様のご協力に感謝いたします。ご不明な点やご不明な点がございましたら、お気軽にお問い合わせください。

よろしくお願いします。

Cisco Technical Assistance Center (TAC)

リンク：

[1] [Cisco SD-WAN強化ガイド](#)

[2] [公式セキュリティアドバイザリ\(cisco-sa-sdwan-privesc-4uxFrdzx\)](#)

Outlookで開く

①送信前に[カッコ付きのプレースホルダ]をすべて置き換えてください。

✉ Outlookを開く（件名のみ）

📎 .emlテンプレートのダウンロード

TAC 14 IOCなし/修正済みリリースで利用可能なテンプレート（WAVE 2a – 今すぐアップグレード）

使用例

SD-WANログでCVE-2026-20245に関するIndicators of Compromise(IoC)が示されず、修正済みソフトウェアリリースが利用可能なお客様に送信されます。アップグレードの計画と実行を直ちに進めるように顧客に勧める。

Subject

更新：CVE-2026-20245のIoCアセスメント完了 – IoCが見つかりません、アップグレードが必要です – SR [SR#]

メッセージ

お客様各位

サービスリクエスト[SR#]に基づき、CVE-2026-20245に関してCisco Technical Assistance Center(TAC)にご連絡いただきありがとうございます。

SD-WAN制御コンポーネントから提供されたadmin-techファイルの分析が完了しました。CVE-2026-20245に関連するIndicators of Compromise(IoC)は確認されたログに見つかりませんでした。

このレビューのために取得してシスコに提供するログデータの量は、[シスコSD-WAN強化ガイド](#)^[1]に従ってお客様の環境に設定されたログ保持期間によって制限されている可能性があります。

重要：アップグレードが必要：

IoCは特定されていませんが、SD-WAN制御コンポーネントが修正済みソフトウェアリリースにアップグレードされるまで、基盤となる脆弱性は残ります。現在、ご使用のプラットフォームで修正済みリリースが利用可能です。

この脆弱性を修正する際には、最も重要なステップとして、アップグレードの計画と実行に優先順位を付けてください。このアップグレードをまだスケジュールしていない場合は、すぐにスケジュールしてください。

次のステップ：

1. すべてのSD-WANコントロールコンポーネントのアップグレード：マネージャ(vManage)、コントローラ(vSmart)、およびバリデータ(vBond)を、[公式セキュリティアドバイザリ](#)^[2]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。
2. アップグレードリソース：詳細なアップグレード手順については、次のシスコの公式ドキュメントを参照してください。
 - [Catalyst SD-WANアップグレードの開始](#)^[3]
 - [Cisco SD-WANアップグレードガイド](#)^[4]
3. ケースの終了：環境全体でソフトウェアのアップグレードが正常に完了したら、このケースを解決したと見なして、標準的な終了手順に進むことができます。

BCS/LCSサブスクリプションをお持ちの場合は、Cisco NCEまたはデリバリマネージャに連絡して、アップグレードプロセスに関する追加ガイダンスを受けてください。

引き続きケースをモニタリングします。10営業日以内に応答がない場合、シスコではこれ以上のサポートは必要ないと判断し、通常のTACケース終了手順に進みます。

よろしくお願いいたします。

Cisco Technical Assistance Center (TAC)

リンク:

- [1] [Cisco SD-WAN強化ガイド](#)
- [2] [公式セキュリティアドバイザリ\(cisco-sa-sdwan-privesc-4uxFrdzx\)](#)
- [3] [Catalyst SD-WANアップグレードの開始](#)
- [4] [Cisco SD-WANアップグレードガイド](#)

Outlookで開く

①送信前に[カッコ付きのプレースホルダ]をすべて置き換えてください。

✉ Outlookを開く (件名のみ)

↓ .emlテンプレートのダウンロード

IOCに関するTAC 15テンプレートが特定/修正済みリリースあり (WAVE 2a : 緊急アップグレード)

使用例

SD-WANログにCVE-2026-20245に関連するIndicators of Compromise(IoC)が記録され、修正済みソフトウェアリリースが入手可能なお客様に送信されます。早急にアップグレードを行い、結果と修復方法について話し合うレビューコールのスケジュールを設定するようにお客様にアドバイスします。

Subject

緊急 : CVE-2026-20245用のIoCが特定されました – 緊急アップグレードが必要 – SR [SR#]

メッセージ

お客様各位

サービスリクエスト[SR#]に基づき、CVE-2026-20245に関してCisco Technical Assistance Center(TAC)にご連絡いただきありがとうございます。

SD-WAN制御コンポーネントから提供されたadmin-techファイルを分析した後、当社のチームはCVE-2026-20245に関連するIndicators of Compromise(IoC)を特定しました。

これらの調査結果の性質を考えると、できるだけ早く技術的な詳細と推奨される次のステップについて話し合うことが重要です。具体的な調査結果を確認し、適切な修復方法について話し合うために、御社のチームとの電話スケジュールを設定したいと考えています。

必要な緊急措置：

1. **SD-WANコントロールコンポーネントをすぐにアップグレードする**：プラットフォームに対して修正済みのソフトウェアリリースを使用できます。Manager(vManage)、Controller(vSmart)、およびValidator(vBond)を、[公式セキュリティアドバイザリ](#)^[1]に記載されている修正済みソフトウェアバージョンにできるだけ早くアップグレードしてください。このアップグレードにより、脆弱性が即座に解消されます。
2. **レビューコールのスケジュールを立てる**：IoCの結果をレビューし、推奨される修復オプションについて話し合うために、近い[4 ~ 8時間以内]に簡単なコールが可能になったことをお知らせください。
3. **強化のベストプラクティスの適用**：修復の計画中に攻撃を受ける可能性を減らすために、『[Cisco SD-WAN Hardening Guide](#)^[2]』の推奨事項を確認して実装します。

アップグレードリソース：

- [Catalyst SD-WANアップグレードの開始](#)^[3]
- [Cisco SD-WANアップグレードガイド](#)^[4]

重要：アップグレード後は、特定されたセキュリティ侵害の重大度に応じて、追加の修復手順（コントローラの再導入や証明書のローテーションなど）が推奨される場合があります。これらについては、レビューコール中に説明します。

修復オプションの詳細については、『[TAC Remediation Guide](#)^[5]』も参照してください。

シスコの主な目標は、お客様の環境を保護し、潜在的なリスクを軽減することです。本件に関する迅速な対応に感謝するとともに、貴社との調整を楽しみにしています。

よろしくお願いいたします。

Cisco Technical Assistance Center (TAC)

リンク：

- [1] [Official Security Advisory\(cisco-sa-sdwan-privesc-4uxFrdzx\)](#)
- [2] [Cisco SD-WAN強化ガイド](#)
- [3] [Catalyst SD-WANアップグレードの開始](#)
- [4] [Cisco SD-WANアップグレードガイド](#)
- [5] [TAC修復ガイド](#)

Outlookで開く

①送信前に[かっこ付きのプレースホルダ]をすべて置き換えてください。

TAC 16 IOC用テンプレートが特定されました/修正済みリリースはありません (WAVE 2a – 強化および待機の修正)

使用例

SD-WANログにCVE-2026-20245に関連するIndicators of Compromise(IoC)が示されたが、そのプラットフォーム/バージョンに対して現在利用できる修正済みソフトウェアリリースがないお客様に送信されます。即時の強化に関するアドバイス、確認のための連絡のスケジュール、修正リリースが完全に修復されるのを待つ必要があることをお客様に通知します。

Subject

緊急：CVE-2026-20245用のIoCが特定されました – 現在利用可能な修正済みリリースはありません – SR [SR#]

メッセージ

お客様各位

サービスリクエスト[SR#]に基づき、CVE-2026-20245に関してCisco Technical Assistance Center(TAC)にご連絡いただきありがとうございます。

SD-WAN制御コンポーネントから提供されたadmin-techファイルを分析した後、当社のチームはCVE-2026-20245に関連するIndicators of Compromise(IoC)を特定しました。

これらの調査結果の重大度を踏まえ、できるだけ早く技術的な詳細と推奨される暫定措置について話し合うことが重要です。具体的な結果を確認するために、御社のチームとの電話スケジュールを設定させていただきたいと思います。

重要：修正済みソフトウェアリリースは現在提供されていません。

現在のプラットフォームおよびソフトウェアバージョンでは、この脆弱性を完全に修復できる修正済みソフトウェアリリースはありません。シスコのエンジニアリング部門では、修正済みリリースの提供に積極的に取り組んでいます。修正済みソフトウェアが入手可能になると、[公式のセキュリティアドバイザリ^{\[1\]}](#)が修正済みリリース情報で更新されます。

必要な緊急措置：

1. レビューコールのスケジュール：IoCの調査結果をレビューし、暫定的な封じ込め措置について議論するために、4～8時間以内に簡単なコールを受けられるかどうかをお知らせください。

2. 強化のベストプラクティスを直ちに適用：[Cisco SD-WAN強化ガイド](#)^[2]の推奨事項を確認して実装し、修正済みリリースの待機中に攻撃対象領域を縮小します。
3. 高度なモニタリング：SD-WAN制御コンポーネントを綿密にモニタリングし、異常な動作、予期しない設定変更、または不正なアクセス試行がないかどうかを確認します。
4. セキュリティアドバイザリを監視する：ご使用のプラットフォームの修正済みリリースの入手に関するアップデートについては、[公式のセキュリティアドバイザリ](#)^[1]を定期的に確認してください。
5. アップグレードの計画：修正済みリリースの公開後すぐにアップグレードを実行できるように、アップグレード計画を今すぐ開始します。

次のステップ：

修正済みソフトウェアリリースが利用可能になった時点で、このケースを更新します。その時点で、すべてのSD-WAN制御コンポーネント(Manager、Controller、Validator)の修正バージョンへのアップグレードをただちに優先する必要があります。アップグレードの後、電話で確認した結果に基づいて、追加の修復手順（コントローラの再導入や証明書のローテーションなど）について検討します。

修正済みリリースが利用可能になった後に適用される修復オプションの詳細については、『[TAC修復ガイド](#)^[3]』も参照してください。

シスコの主な目標は、お客様の環境を保護し、潜在的なリスクを軽減することです。本件に関する迅速な対応に感謝するとともに、貴社との調整を楽しみにしています。

よろしくお願いいたします。

Cisco Technical Assistance Center (TAC)

リンク：

[1] [Official Security Advisory\(cisco-sa-sdwan-privesc-4uxFrdzx\)](#)

[2] [Cisco SD-WAN強化ガイド](#)

[3] [TAC修復ガイド](#)

Outlookで開く

①送信前に[かっこ付きのプレースホルダ]をすべて置き換えてください。

✉ Outlookを開く（件名のみ）

📎 .emlテンプレートのダウンロード

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。