Catalyst SD-WANセキュリティアドバイザリの修正 – 2026年2月

内容

はじめに

このドキュメントでは、2026年2月25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修正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の脆弱性
- Cisco Catalyst SD-WANコントローラにおける認証バイパスの脆弱性

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 CSCws52722
- Cisco Bug ID CSCws33583
- Cisco Bug ID CSCws33584
- Cisco Bug ID CSCws33585
- Cisco Bug ID CSCws33586
- Cisco Bug ID CSCws33587
- Cisco Bug ID CSCws93470

是正ワークフローの概要

注：すべてのSD-WAN展開には脆弱性が存在するため、すぐに対処する必要があります。ただし、すべてのシステムが侵害の証拠を示すわけではありません。

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ら、PSIRTチームと協力する
- 侵害の兆候が検出されない場合は、アップグレードのガイダンスとサポートを提供します。

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、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:TACでは、お客様の環境に侵入の痕跡がないかどうかを評価します
4. 修復の実行: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：TACサービスリクエストをオープンする前に、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。これは、TACが環境を評価するために不可欠です。

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。

---

1. すべてのコントローラ(vSmarts)でadmin-techを実行します。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。

注:vSmart admin-techsは同時に実行しないでください。一度に1つずつ収集します。マネージャおよびバリデータのAdmin-techsは、任意の順序で収集できます。

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からすべてのadmin-techファイルを収集した後、Cisco TACサポートケースをオープンします。

必要なアクション：

1. ビジネスへの影響に適した重大度レベルでTAC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. PSIRTアドバイザリを参照する
4. TACの評価とガイダンスを待つ

⚠ 注意:TACはシステムのステータスを判別し、適切な次のステップを推奨します。

TACのガイダンスなしにこれ以上の手順を試さないでください

ステップ3:TACアセスメント

TACは、アップロードされたadmin-techファイルを分析し、システムのステータスを判断します。

この間：

- TACによる正式な評価を待ってから、何らかの措置を講じる
- TACから結果と次のステップを報告する

ステップ4：修復の実行（TACガイド）

TACは、評価に基づいて適切な修復プロセスを案内します。TACが提供するすべての指示に従ってください。

パスA：侵入の痕跡が見つかりません – アップグレード

TACが侵害の証拠がないことを確認した場合は、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。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、このセクションでリンクされているアップグレードガイドを参照してください。

警告：アップグレードは現在のメジャーリリースの範囲内で行う必要があります。TACのガイダンスがない場合は、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

パスB：侵入の痕跡の特定 – PSIRTガイド

TACがセキュリティ侵害の指標が存在することを確認した場合、お客様の環境に合わせてカスタマイズされた修復戦略を開発するためにPSIRTチームが協力します。TACとPSIRTが提供するすべてのガイダンスを実行します。

修正済みソフトウェアバージョン

次のソフトウェアリリースには、特定された脆弱性に対する修正が含まれています。

現在のバージョンに適用	修正済みバージョン	利用可能なソフトウェア
20.3、20.6、20.9	20.9.8.2*	20.9.8.2 vManage、vSmart、およびvBondのアップグレードイメージ
20.12の20.10、20.11、20.12.5以前	20.12.5.3	20.12.5.3 vManage、vSmart、およびvBondのアップグレードイメージ
20.12.6	20.12.6.1	20.12.6.1 vManage、vSmart、およびvBondのアップグレードイメージ
20.13、20.14、20.15.x	20.15.4.2	20.15.4.2 vManage、vSmart、およびvBondのアップグレードイメージ
20.16、20.17、20.18.x	20.18.2.1	20.18.2.1 vManage、vSmart、およびvBondのアップグレードイメージ

注:CDCS(Cisco-Hosted Cluster)をご使用のお客様の場合、20.15.405も修正済みのリリースです。これは特にシスコがホストするクラスタの導入に適用され、標準のアップグレードパスとは別に処理されます。

* リリース20.9以前の場合：ご使用のリリースの修正済みソフトウェア(20.9.8.2)は2/27で入手できます。シスコでは、より高いメジャーリリース(20.12、20.15、20.18)にアップグレードするの

ではなく、現在のメジャーリリース内に留まり、20.9.8.2リリースまで待つことを推奨します。現在20.9より前のバージョンを使用している場合は、20.9.8.2がアップグレードされるまで待ちます。引き続きTACで作業し、2027年2月27日に利用可能なソフトウェアリンクを再度確認してください。

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: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、すべての制御コンポーネントで実行する必要があります。

検証1：認証ログでの不正なSSHログインのチェック

ステップ1：有効なvManageシステムIPの特定

各vSmartコントローラにアクセスし、次を実行します。

```
west-vsmart# show control connections | inc "vmanage|PEER|IP"
```

出力例：

```
                                                  PEER
     PEER   PEER   PEER            SITE       DOMAIN  PRIV    PEER                    PUB
```

```
INDEX TYPE  PROT  SYSTEM IP       ID         ID      PRIVATE IP                          PORT    PUBLIC I
-------------------------------------------------------------------------------------------------------
0     vmanage dtls 10.1.0.18     101018     0       10.1.10.18                          12346   10.1.10.1
```

ステップ2：正規表現文字列の構築（vBondおよびvSmartのみ）

ステップ1のすべてのシステムIPをOR正規表現パターンに結合します。

```
system-ip1|system-ip2|...|system-ipn
```

ステップ2b:vManageシステムの追加ステップ

vManage自体でこれらのコマンドを実行する場合は、localhost IP(127.0.0.1)、ローカルシステムIP、すべてのクラスタIP、およびVPN 0トランスポートインターフェイスIPを正規表現に追加します。

```
system-ip1|system-ip2|...|system-ipn|127.0.0.1|
```

ローカルvManageシステムIPを検索するには、次のコマンドを使用します。

```
show control local-properties
```

VPN 0トランスポートインターフェイスIPとクラスタIPを見つけるには、次のコマンドを使用します。

```
show interface | tab
```

ステップ3：検証コマンドの実行

次のコマンドを実行して、REGEXをステップ2で得た正規表現の文字列に置き換えます。

```
west-vsmart# vs
west-vsmart:~$ zgrep "Accepted publickey for vmanage-admin from " /var/log/auth.log* | grep -vE "\s(REG
```

注：このコマンドは、予期しないソースからのvmanage-adminログインだけを表示するように認証ログをフィルタリングします。正規のログインは、vManage関連のIPからのみ発信される必要があります。

ステップ4：結果の解釈とTACのドキュメント

出力が表示されない場合は、次の手順を実行します。

- このデバイスでは侵入の痕跡は検出されない
- この結果をTACケースに文書化します。
- 残りのコントローラの評価を続行

ログ行が出力される場合：

- 示されている各IPアドレスを注意深く調べる
- IPがvManageインフラストラクチャ（クラスタIP、古いシステムIPなど）に関連していないことを確認します。
- 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
- ログエントリには、タイムスタンプと送信元IPアドレスが表示されます
- 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、タイムスタンプ、および送信元IPを含めます
- TACが公式評価の決定を行う

検証2：コントローラのsyslogで不正なピア接続をチェックする

このコマンドは、コントローラのsyslogファイルからすべてのピアタイプとピアシステムのipのペアを抽出し、確認できるようにリストとして出力します。疑わしいエントリに自動的にフラグが設定されることはありません。出力を調べて、各ピアシステムIPがSD-WANインフラストラクチャの既知の正当な部分かどうかを判断する必要があります。すべてのコントロールコンポーネント（コントローラ、マネージャ、およびバリデータ）でこれを実行します。

ステップ1：各制御コンポーネントでコマンドを実行します。

まず、vshellにアクセスし、ログディレクトリに移動します。

```
vs
cd /var/log
```

次に、次のコマンドを実行します。

```
awk '{
```

```
  match($0, /peer-type:([a-zA-Z0-9]+)[^ ]* peer-system-ip:([0-9.:]+)/, arr);
  if(arr[1] && arr[2]) print "(" arr[1] ", " arr[2] ")";
}' vsyslog* | sort | uniq
```

ステップ2：結果の解釈とTACへのドキュメントの提出

出力に既知のvManage/vSmart/vBondシステムIPのみが表示される場合：

- このチェックではセキュリティ侵害の兆候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。
- 残りの制御コンポーネントの評価を続行する

出力に認識されないピアシステムIPが含まれている場合：

- 示されている各IPアドレスとピアタイプを注意深く調べます
- IPが既知のSD-WANコントロールプレーンインフラストラクチャに関連していないことを確認します。
- 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
- この場合は、ピアタイプとピアシステムIPペアを指定してフルコマンド出力を含めてください
- TACが公式評価の決定を行う

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：すべての制御コンポーネントからadmin-techファイルを収集し、TACケースを開いてファイルをアップロードします。TACが環境を評価し、次のステップに関するガイダンスを提供します。

Q.どのバージョンにアップグレードすればよいですか。 A.できるだけ早い段階で、最も近い修正済みバージョンにアップグレードしてください。

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が環境を適切に評価するには、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ファイルが必要です。

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ーファイルを分析し、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はPSIRTチームと連携し、お客様に連絡を取って、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：使用する修正済みソフトウェアのバージョンを知るにはどうすればよいのですか。

A：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: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：いいえ。TACが改善措置を実施する前に、評価を完了してガイダンスを提供するのを待ってください。

Q：修復中にダウンタイムが発生する可能性はありますか。

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:PSIRTの修正は、今後の20.15.5リリースおよびその他の今後のリリースに含まれますか。

A：はい。修正は20.15.5およびその他の今後のリリースに含まれます。ただし、このドキュメントで説明されている脆弱性を緩和するためのアップグレードは、ただちに優先する必要があります（しばらくお待ちください）。

Q：セキュリティ侵害の兆候が見つからない場合、すべてのコントローラをアップグレードする必要がありますか。

A：はい。すべてのSD-WAN制御コンポーネント（vManage、vSmart、およびvBond）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する必要があります。コントローラのサブセットのみをアップグレードするだけでは不十分です。

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がサポートします。

Q：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: Cisco IOS XEデバイスは、このアドバイザリの影響を受けません。

Q：シスコのホステッドオーバーレイです。ACLを修正するか、SSPでアクションを実行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で確認できる独自のAllowed Inbound Rulesを確認し、こちら側の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。

SSP > Overlay Details > Allow Inbound rulesで確認してください。シスコが外部からクラウドホステッドコントローラにプロビジョニングするDay 0では、ポート22および830がデフォルトで常にブロックされていることに注意してください。

Q:CDCS/共有テナントを使用しています。どのバージョンにアップグレードしますか？

A：現在のバージョンに基づいて、共有テナントまたはCDCSクラスタは現在アップグレードの予定が入っているか、すでに修正済みバージョンにアップグレードされています。共有テナントとCDCSの修正済みリリースを次に示します。

1. 早期導入クラスタ=> 20.18.2.1（これは実際には標準リリースと同じです）

2. 推奨リリースクラスタ=> 20.15.405（PSIRT修正を含むCDCS固有バージョン）

CDCSのお客様は、このPSIRTに対応するために効果的な措置を講じる必要はありません。

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。