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

アドバイザリーID : cisco-sa-sdwan-rpa-EHchtZk
初公開日 : 2026-02-25 16:00
バージョン 1.0 : Final
CVSSスコア : 10.0
回避策 : No workarounds available
Cisco バグ ID : CSCws52722

CVE-2026-20127

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 Controller（以前のSD-WAN vSmart）およびCisco Catalyst SD-WAN Manager（以前のSD-WAN vManage）のピアリング認証の脆弱性により、認証されていないリモートの攻撃者が該当システムで認証をバイパスし、管理権限を取得する可能性があります。

この脆弱性は、該当システムのピアリング認証メカニズムが適切に機能していないことに起因しています。攻撃者は、細工された要求を該当システムに送信することにより、この脆弱性をエクスプロイト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、内部の高特権の非rootユーザアカウントとして該当するCisco Catalyst SD-WANコントローラにログインできる可能性があります。このアカウントを使用すると、攻撃者はNETCONFにアクセスし、SD-WANファブリックのネットワーク設定を操作できるようになります。

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-rpa-EHchtZk

該当製品

脆弱性のある製品

この脆弱性は、デバイスの設定に関係なく、Cisco Catalyst SD-WAN ControllerおよびCisco Catalyst SD-WAN Managerに影響を与えます。

この脆弱性は、次の展開タイプに影響を与えます。

- オンプレミス導入
- シスコホステッドSD-WANクラウド
- シスコホステッドSD-WANクラウド – シスコマネージド
- Cisco Hosted SD-WAN Cloud - FedRAMP環境

脆弱性が存在する Cisco 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。

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」セクションに記載されている製品のみが、これらの脆弱性の影響を受けることが分かっています。

詳細

重要：簡素化と一貫性を実現するため、Cisco SD-WANソリューションはCisco Catalyst SD-WANとしてブランドが変更されました。また、Cisco IOS XE SD-WANリリース17.12.1aおよびCisco Catalyst SD-WANリリース20.12.1からは、次のコンポーネントの変更が適用されます。

- Cisco SD-WANコントローラがCisco Catalyst SD-WANコントロールコンポーネントに
- Cisco SD-WAN vAnalyticsがCisco Catalyst SD-WAN Analyticsに
- Cisco SD-WAN vBondがCisco Catalyst SD-WAN Validatorになりました
- Cisco SD-WAN vManageがCisco Catalyst SD-WAN Managerに
- Cisco SD-WAN vSmartがCisco Catalyst SD-WAN Controllerに

すべてのコンポーネントブランド名の変更の一覧については、最新のリリースノートを参照してください。新しい名前への移行中に、ソフトウェア製品のユーザインターフェイスのアップデートに対する段階的なアプローチにより、ドキュメントセットに矛盾が生じる場合があります。

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コントローラシステムで、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。

不明または不正なIPアドレスからのvmanage-adminのAccepted publickeyに関連するエントリについて、/var/log/auth.logにあるauth.logファイルを監査することをお勧めします。次に例を示します。

```
2026-02-10T22:51:36+00:00 vm <auth.info> sshd[804]: Accepted publickey for vmanage-admin from <SYSTEM I
```

auth.logログファイルのIPアドレスを、Cisco Catalyst SD-WAN Manager Web UIのWebUI > Devices > System IPの順に選択してリストされている設定済みシステムIPと照合する必要があります。

Cisco Catalyst SD-WANコントローラまたはCisco Catalyst SD-WAN Managerが侵害されたかどうかを判断するには、Cisco Technical Assistance Center(TAC)でケースをオープンする必要があります。 新しいTAC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コマンドを発行することをお勧めします。これにより、admin-techファイルをCisco TACに提供して確認できます。

ピアリングイベント検証ガイダンス

Cisco Catalyst SD-WANログに記録されるすべての制御接続ピアリングイベントでは、手動による検証を行って正当性を確認する必要があります。特に、vmanageピアリングタイプに重点が置かれています。SD-WANインフラストラクチャに侵入した攻撃者は、不正なピア接続を確立することがよくあります。このピア接続は、表面的には正常に見えても予期しない時間に発生したり、認識されていないIPアドレスから発信されたり、環境のアーキテクチャと矛盾するデバイスタイプを含んだりすることがあります。正当なネットワーク運用と潜在的なセキュリティ侵害の指標を区別するには、包括的なレビュープロセスが不可欠です。

検証チェックリスト

- 各ピアリングイベントのタイムスタンプを、ご使用の環境の既知のメンテナンスウィンドウ、スケジュールされた設定変更、および通常の運用時間と比較して確認します。
- 資産インベントリと承認済みIP範囲を相互参照して、組織または承認済みパートナーが所有または運用するインフラストラクチャにパブリックIPアドレスが対応していることを確認します。
- ピアシステムのIPが、SD-WANトポロジ内の文書化されたデバイス割り当てと一致することを検証します。
- ピアタイプ(vmanage、vsmart、vedge、vbond)をレビューし、導入環境で期待されるデバイスの役割と一致していることを確認します。
- 同じソースIPまたはシステムIPからの複数のイベントを相互に関連付けて、偵察または永続的なアクセス試行のパターンを特定します。
- イベントのタイミングと認証ログ、変更管理レコード、およびユーザアクティビティを相互参照して、接続が承認されたユーザによって開始されたかどうかを確認します。

ログエントリの例

```
Jul 26 22:03:33 vSmart-01 VDAEMON_0[2571]: %Viptela-vSmart-VDAEMON_0-5-NTCE-1000001: control-connection
```

特定の例では、peer-system-ipが予期されるIPアドレススキーマin-useと一致するものとして検証

され、タイムスタンプがピアリングイベントの発生を引き起こす可能性のあるイベントと一致するものとして検証され、public-ipがピアリングイベントの予期される送信元と検証される必要があります。

回避策

この脆弱性に対処する回避策はありません。ただし、緩和策として、最初の修正済みリリースへのアップグレードを計画しているお客様は、次のガイダンスに従って、この脆弱性の影響を一時的に緩和することができます。

アクションの所有者	オンプレミス導入
[顧客（Customer）]	『Cisco Catalyst SD-WAN Getting Started Guide』の「Firewall Ports for Cisco Catalyst SD-WAN Deployments」セクションにあるガイドラインに従ってください。 独自のデータセンターで独自のCisco Catalyst SD-WAN導入をホストするお客様は、コントローラ内接続を保護する必要があります。シスコでは、アクセスコントロールリスト(ACL)、セキュリティグループルール、および/またはファイアウォールルールを追加して、既知のコントローラIPおよびその他の既知のIPのみを許可するように、ポート22およびポート830へのトラフィックを制限することを推奨しています。
アクションの所有者	シスコホステッドSD-WANクラウド
[顧客（Customer）]	これらのガードレールは、Cisco Hosted SD-WAN Cloud用に用意されています。
アクションの所有者	Cisco Hosted SD-WAN Cloud - FedRAMP環境
[顧客（Customer）]	これらのガードレールは、Cisco Hosted SD-WAN Cloud - FedRAMP環境に適しています。
アクションの所有者	シスコホステッドSD-WANクラウド – シスコマネージド
お客様とシスコ	これらのガードレールは、Cisco Hosted SD-WAN Cloud - Cisco Managed用に用意されています。

この緩和策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

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。これら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

次の表では、左の列にシスコ ソフトウェアリリースを記載しています。右側の列は、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最初のリリースを示しています。このセクションの表に記載されている適切な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お勧めします。

Cisco Catalyst SD-WANリリース	First Fixed Release（修正された最初のリリース）
20.91 より前	修正済みリリースに移行。
20.9	20.9.8.2（2026年2月27日予定）
20.111	20.12.6.1
20.12.5 20.12.6	20.12.5.3 20.12.6.1
20.131	20.15.4.2
20.141	20.15.4.2
20.15	20.15.4.2
20.161	20.18.2.1
20.18	20.18.2.1

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。

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。

追加情報

- コンポーネントとソフトウェアリリースの互換性を確認するには、『SD-WANコントローラコンポーネントの互換性マトリクス』を参照してください。
- アップグレードの計画に役立つ情報については、『Cisco Catalyst SD-WANアップグレードマトリックス』を参照してください。

不正利用事例と公式発表

Cisco PSIRTでは、この脆弱性が限定的に悪用されていることを認識しています。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

シスコは、この脆弱性を報告していただいたAustralian Signals DirectorateのAustralian Cyber Security Centerに感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa-EHchtZk

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2026年2月25日

利用規約

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。