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

アドバイザリーID : cisco-sa-sdwan-rpa2-v69WY2SW
初公開日 : 2026-05-14 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 : CSCwt50498

CVE-2026-20182

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

2026年5月：このセキュリティアドバイザリでは、2026年2月にCisco Catalyst SD-WANコントローラ認証バイパスの脆弱性が公開された後に発見され、修正された脆弱性の詳細と修正情報を提供しています。この新しいアドバイザリは、制御接続ハンドシェークの新しい脆弱性に関するものです。このアドバイザリの「侵害の指標」セクションには、システムチェックに役立つ「コントロール接続の表示」ガイダンスが含まれています。

Cisco Catalyst SD-WAN コントローラ（旧 SD-WAN vSmart）と Cisco Catalyst SD-WAN Manager（旧 SD-WAN vManage）でのピア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認証をバイパスし、影響を受けるシステムで管理者権限を取得する可能性があります。

この脆弱性は、影響を受けるシステムのピア認証メカニズムが正常に機能していないことが原因です。攻撃者は、巧妙に細工された要求を該当システムに送信することにより、この脆弱性を不正利用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ことで、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構成を操作することが可能になります。

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。

重要：潜在的な侵害のインジケータを保持するために、アップグレードの前に、SD-WAN環境内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必要があります。admin-techファイルが収集されたら、できるだけ早い時期にソフトウェアをアップグレードする必要があります。

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-rpa2-v69WY2SW

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 コントローラおよび Cisco Catalyst SD-WAN Manager に影響します。

この脆弱性は、次を含むすべての導入タイプに影響します。

- オンプレミス展開
- Cisco SD-WAN Cloud-Pro
- Cisco SD-WANクラウド（シスコマネージド）
- 政府機関向けCisco SD-WAN(FedRAMP)

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。

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、およびインターネットに公開されたポートがある Cisco Catalyst SD-WAN コントローラシステムは、侵害のリスクにさらされています。場合によっては、標準的な運用中にこれらの侵害の兆候が発生する可能性があります。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と比較して評価する必要があります。

/var/log/auth.log にある auth.log ファイルを監査して、次に示す例のように、未知の IP アドレスまたは不正な IP アドレスからの Accepted publickey for vmanage-admin に関連する項目がないかどうか調べることをお勧めします。

```
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] > [デバイス（Devices）] > [システムIP（System IP）] 列にリストされている設定済みのシステム

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際に支援が必要な場合は、Cisco Technical Assistance Center（TAC）でケースをオープンする必要があります。 TACケースは、タイトルにCVE-ID CVE-2026-20182を使用して、重大度3として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 デプロイメント内の各制御コンポーネントから request admin-tech コマンドを発行し、admin-tech ファイルを Cisco TAC に提供して確認してもらうことができます。

ピアリングイベント検証に関するガイダンス

Cisco Catalyst SD-WANログで特定されるコントロール接続ピアリングイベントはすべて、正当性を確認するために手動の検証が必要であり、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に関連したりする可能性があります。適切なネットワーク運用と、侵害の兆候となり得る事象とを区別するためには、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、既知のメンテナンス期間、予定されている設定変更、環境の通常の運用時間に照らして確認します。
- アセットインベントリおよび承認された IP 範囲と照合することにより、パブリック IP アドレスが、組織または認定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対応するものであることを確認します。
- ピアシステム 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確認します。
- ピアタイプ（vmanage、vsmart、vedge、vbond）を確認し、デプロイメントで想定されるデバイスのロールと整合していることを確認します。
- 同じ送信元 IP またはシステム IP からの複数のイベントを関連付けて、偵察活動や継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を認証ログ、変更管理記録、およびユーザーアクティビティと照合し、その接続が権限のある担当者によって行われたもの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。

コントロール接続ガイダンスの表示

コマンド出力にstate:upおよびno challenge-ackが存在して侵害が発生しているかどうかを確認するには、show control connections detailコマンドまたはshow control connections-history detailコマンドを使用します。この情報がコマンド出力に表示される場合は、Cisco TACでサービスリクエストをオープンし、サポートを依頼してください。

コントローラまたはマネージャのCLIから：show control connections detailまたはshow control connections-history detailのいずれかを使用します。

バリデータのCLIから：show orchestrator connections detailまたはshow orchestrator connections-history detailのいずれかを使用します。

出力例：

<#root>

```
------------------------------------------------------------------------
 REMOTE-COLOR- default SYSTEM-IP- 2.2.2.2   PEER-PERSONALITY- vmanage
------------------------------------------------------------------------
site-id             562
domain-id           0
protocol            dtls
protocol-version    DTLS1_2
cipher-name         ECDHE-RSA-AES256-GCM-SHA384
private-ip          10.0.0.1
private-port        12346
public-ip           192.168.1.1
public-port         50825
org-name            orgname-example
```

state

up

```
 [Local Err: NO_ERROR] [Remote Err: NO_ERROR]
uptime              0:00:16:58
hello interval      1000
hello tolerance     12000
peer-session-id      0x00eda0acc5
```

<#root>

```
  Tx Statistics-
  --------------
    hello                   3423293
    connects                0
    registers               0
    register-replies        0
    challenge               1
    challenge-response      0


challenge-ack           0  <-- challenge-ack 0


    teardown                0
    teardown-all            0
    vmanage-to-peer         0
    register-to-vmanage     1
    create-cert-reply       0
```

<#root>

```
  Rx Statistics-
  --------------
    hello                   3423291
    connects                0
    registers               0
    register-replies        0
    challenge               0
    challenge-response      1


 challenge-ack           0  <-- challenge-ack 0


    teardown                0
    vmanage-to-peer         1
    register-to-vmanage     0
    create-cert             0
```

回避策

この脆弱性に対処する回避策はありません。

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	20.9.9.1
20.10	20.12.7.1
20.111	20.12.7.1
20.12	20.12.5.4 20.12.6.2 20.12.7.1
20.131	20.15.5.2
20.141	20.15.5.2
20.15	20.15.4.4 20.15.5.2
20.161	20.18.2.2
20.18	20.18.2.2
26.1	26.1.1.1

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。

また、クラウドベースのCisco SD-WAN Cloud(Cisco Managed)リリース20.15.506でも、この脆弱性に対処しています。ユーザの対処は必要ありません。サービス GUI のヘルプ機能を使用すると、現在の修復ステータスやソフトウェアバージョンを確認できます。

追加情報が必要なお客様は、Cisco TACまたは契約したメンテナンスプロバイダーに連絡することをお勧めします。

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、『Catalyst SD-WAN制御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ついては、Cisco Catalyst SD-WAN Upgrade Matrix を参照してください。
- その他の修復方法については、『Remediate Catalyst SD-WAN Security Advisory - May 2026』を参照してください。

不正利用事例と公式発表

2026年5月、Cisco Product Security Incident Response Team(PSIRT)は、この脆弱性の限定的なエクスプロイトに気づきました。こ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Rapid7社のシニアプリンシパルセキュリティ研究者Stephen Less氏とシニアセキュリティ研究者Jonah Burgess氏に感謝いたします。

URL

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

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5月14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。