

Cisco Catalyst SD-WAN Manager における API 認証バイパスの脆弱性



Advisory ID : cisco-sa-sdwan-webauth-xr8beuuU

[CVE-2026-76504](#)

初公開日 : 2026-09-30 13:00

注 : 2026-10-02 23:18

バージョン 1.1 : Final

CVSSスコア : [9.8](#)

回避策 : No workarounds available

Cisco Bug ID : [CSCww79570](#)

日本語の情報は原文の英語の非公式な翻訳です。日本語と英語のバージョンに相違がある場合は、英語のバージョンが優先されます。

概要

Cisco Catalyst SD-WAN ManagerのAPIセッションベースの認証管理における脆弱性により、認証されていないリモートの攻撃者が、管理者ユーザの特権を使用して該当システムにアクセスできる可能性があります。

この脆弱性は、HTTP要求でのURIエンコーディングの不適切な処理に起因します。この処理により、特定のAPIエンドポイントへのアクセスを制限する認証規則を要求がバイパスできるようになります。攻撃者は、該当システムのAPIに巧妙に細工されたHTTP要求を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、攻撃者は認証をバイパスし、管理者ユーザとしてAPIにアクセスできる可能性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。この脆弱性に対処する回避策はありません。

Live Protect シールド

シスコは、CVE-2026-76504 に対する Live Protect シールドをリリースしました。これは、ソフトウェアのアップグレード計画を立てるための時間を確保できるよう、一時的なセキュリティカバレッジを提供するためのもので、ガバナンスや規則遵守のためにお客様が必要とする可能性がある情報を保持することなどが含まれます。

このシールドが提供するののは、一時的な部分的保護に限られます。この脆弱性を修正する唯一の方法は、このアドバイザリの「[修正済みリリース](#)」セクションに記載されているように、[最初の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です](#)。シスコでは、問題を修復するため、システムのアップグレードを優先させ、できるだけ早く実施することを強く推奨します。

シールドを展開する前に、以下の情報をお読みください。

- 副作用/制限：このシールドが適用される場合

URIエンコーディングを使用する正当なユーザは、SDWAN Managerにログインできない可能性があります。

- Cisco Catalyst SD-WAN 向けの Live Protect の詳細については、
<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/26x-later/network-monitoring/network-monitoring-guide/live-protect-for-cisco-catalyst-sd-wan.html> を参照してください。

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-webauth-xr8beuuU>

該当製品

脆弱性のある製品

この脆弱性は、システム設定に関係なく、Cisco Catalyst SD-WAN Managerに影響を与えます。

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指標

インターネットに公開されている Cisco Catalyst SD-WAN Manager 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 Manager 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セキュリティ侵害の指標(IOC)が発生することがあります。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に対して評価を行う必要があります。

重要：次のIOCの例は、要求での%6aのURIエンコード文字jとしての使用を示しています。これは一例に過ぎず、この脆弱性により、要求でエンコードされた1文字を使用してこの脆弱性を不正利用することが可能になります。

不明または不正なIPアドレスからのj_security_checkに関連するエントリについて、
/var/log/nms/containers/service-proxy/serviceproxy-access.logにあるserviceproxy-access.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。

[2026-09-29T23:11:13.948-05:00] "POST /%6a_security_check HTTP/1.1" 200 - 48 0 4 - "10.10.10.47,192.168

不明または不正なIPアドレスからのj_security_checkに関連するエントリ、特にユーザに呼び出される名前がviptela-reserved-で始まる名前を含むエントリに対するvmanage-server.logファイル(/var/log/nms/vmanage-server.log)を監査することをお勧めします。次に例を示します。

29-Sep-2026 23:11:13,952 CDT [] [vManage-new] [UserUtils] (default task-127462) |default| Request Store

Cisco Catalyst SD-WAN Managerが侵害されたかどうかを確認するには、Cisco Technical Assistance Center(TAC)でケースをオープンしてください。Cisco TACケースは、タイトルにCVE-ID CVE-2026-76504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環境のCisco Catalyst SD-WAN Manager(vManage)でrequest admin-techコマンドを使用することを推奨します。これにより、Cisco TACにadmin-techファイルを提供して、確認を受けることができます。

viptela-reservedシステムサービスアカウントについては、『[Cisco Catalyst SD-WANシステムおよびインターフェイス構成ガイド](#)』の「認証、認可、アカウンティング」セクションで説明しています。

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、オンプレミスに展開されているお客様環境向けの緩和策として、セキュリティが確保されていないネットワーク（インターネットなど）からのシステムアクセスを制限する必要があります。インターネットからのシステムアクセスが必要な場合、信頼できる既知のホストからのアクセス、かつユーザーガイドに記載されているポートおよびプロトコルを使用したアクセスのみに制限します。ファイアウォールなどのフィルタリングデバイスの背後でCisco Catalyst SD-WAN 制御コンポーネントを保護して、システムとの間のトラフィックをフィルタ処理し、信頼できる既知のホストのみがシステムにトラフィックを送信できるようにします。詳細については、『[Cisco Catalyst SD-WAN Hardening Guide](#)』を参照してください。

Cisco Catalyst SD-WAN クラウドホスト型環境の場合、この緩和策はすでに展開済みです。

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。この脆弱性を修正し、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。

修正リリース

次の表では、左の列にシスコソフトウェアの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 ソフトウェアリリース	第 1 修正済みリリース
20.9 よりも前	修正済みリリースに移行。
20.9	20.9.10.1
20.12	20.12.8.2
20.15	20.15.6.1
20.18	20.18.4.1
26.1	26.1.2.1
26.2	26.2.1

シスコは、クラウドベースの Cisco SD-WAN Cloud (Cisco Managed) リリース 20.15.605 においても、この脆弱性に対処しています。ユーザー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。

その他の情報が必要な場合は、Cisco TAC もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

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、『[Catalyst SD-WAN Control Component Compatibility Matrix](#)』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。

推奨事項

シスコでは、該当システムを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推奨しています。

セキュリティ強化のための一般的な推奨事項

- ・ インターネットなどの安全でないネットワークからシステムへのアクセスを防止します。システムへのインターネットアクセスが必要な場合、信頼できる既知のホストからのアクセス、かつユーザーガイドに記載されているポートおよびプロトコルを使用したアクセスのみに制限します。
- ・ Cisco Catalyst SD-WAN 制御コンポーネントを、ファイアウォールなどのフィルタリングデバイスの背後で保護し、システムとの間で送受信されるトラフィックをフィルタリングするとともに、既知の信頼できるホストにのみシステムへのトラフィックの送信を許可します。2 層ファイアウォールの使用によって、ネットワークプランニングの柔軟性が高まり、エンドユーザーが外部 DMZ に直接接続することを防止できます。Cisco Catalyst SD-WAN ソフトウェアのユーザーガイドの展開に関するセクションを参照してください。
- ・ Web ログトラフィックを定期的に監視し、システムとの間で予期しないトラフィックがないかどうかを確認します。可能であれば、ログは外部サーバーに送信し、十分なログデータを使用して事後調査を実行できるように十分な期間にわたって保持する必要があります。
- ・ システムを Cisco Catalyst SD-WAN ソフトウェアの最新バージョンにアップグレードします。
- ・ デフォルトの管理者パスワードを、より安全なパスワードに変更します。必要なアクセス要件に基づいてユーザ アカウントを作成し、管理者アカウントへのアクセスを制限する。また、すべての管理者に対してオペレータ アカウントを作成します。
- ・ SSL/TLS を使用する場合は、認証局 (CA) から SSL 証明書を取得します。

詳細については、『Cisco Catalyst SD-WAN Hardening Guide』を参照してください。

不正利用事例と公式発表

2026 年 9 月、Cisco PSIRT は、この脆弱性が実際にエクスプロイトされていることを把握しました。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。

送信元

この脆弱性は Cisco Cisco Technical Assistance Center (TAC) サポートケースの解決中に発見されました。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-webauth-xr8beuuU>

改訂履歴

バージョン	説明	セクション	Status	日付
1.1	Live Protectシールドの可用性に関する情報を追加。	概要	Final	2026年10月2日
1.0	初版リリース	—	Final	2026 年 9 月 30 日

利用規約

ソフトウェアのダウンロードおよびテクニカルサポート

Cisco.com の [シスコサポート & ダウンロード](#) ページには、ライセンスとダウンロードに関する情報が記載されています。このページには、マイデバイス (My Devices) ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。お客様がソフトウェアをダウンロードできるのは、シスコから直接、あるいはシスコ認定再販業者やシスコ認定パートナーを通じて調達されたもので、ライセンスが有効なものに限ります。

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、[Cisco Technical Assistance Center \(TAC \)](#) に連絡してアップグレードを入手してください。無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

[ソフトウェアのアップグレードを検討する](#) 際には、関連するシスコ製品の[アドバイザリ](#)を定期的に参照して、侵害を受ける可能性とアップグレード ソリューション一式を確認してください。いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center (TAC) もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

利用規約の詳細

シスコは、商品適格性または特定目的への適合性に関する保証を含め、明示的か黙示的かを問わず、いかなる種類の保証も表明しません。前述の一般論に限定されることなく、シスコは、本情報の正確性または完全性を保証するものではありません。コンテンツは「現状のまま」提供されます。本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。

本セキュリティアドバイザリに含まれる情報のコピーや要約には、事実誤認を引き起こしたり、

重要な情報が欠落していたりする可能性があります。本セキュリティアドバイザリの最新版については、[シスコ セキュリティ アドバイザリ](#) ページをご覧ください。Cisco 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評価します。詳細については、[シスコのセキュリティ脆弱性ポリシー](#)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。