Cisco Catalyst SD-WANの脆弱性

アドバイザリーID : cisco-sa-sdwan-authbp-qwCX8D4v
初公開日 : 2026-02-25 16:00
バージョン 1.0 : Final
CVSSスコア : 9.8
回避策 : No workarounds available
Cisco バグ ID : CSCws33583 CSCws93470 CSCws33584 CSCws33585 CSCws33586 CSCws33587

CVE-2026-20129
CVE-2026-20128
CVE-2026-20126
CVE-2026-20122
CVE-2026-20133

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 Manager（以前のSD-WAN vManage）の複数の脆弱性により、攻撃者が該当システムにアクセスし、権限をルートに昇格させ、機密情報にアクセスし、任意のファイルを上書きできる可能性があります。

これらの脆弱性の詳細については本アドバイザリの「詳細情報」セクションを参照してください。

シスコはこれら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。これら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-authbp-qwCX8D4v

該当製品

脆弱性のある製品

これらの脆弱性は、デバイスの設定に関係なく、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、これらの脆弱性の影響を受けることが分かっています。

シスコは、Cisco Catalyst SD-WAN Managerリリース20.18以降が、CVE-2026-20128およびCVE-2026-20129で説明されている脆弱性の影響を受けないことを確認しました。

詳細

これらの脆弱性は依存関係にはなく、いずれかの脆弱性をエクスプロイトするために別の脆弱性をエクスプロイトする必要はありません。

脆弱性の詳細は以下のとおりです。

CVE-2026-20129:Cisco Catalyst SD-WAN Managerの認証バイパスの脆弱性

Cisco Catalyst SD-WAN ManagerのAPIユーザ認証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、netadminロールを持つユーザとして該当システムにアクセスする可能性があります。

この脆弱性は、APIに送信される要求の認証が不適切なことに起因します。攻撃者は、該当システムのAPIに巧妙に細工された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netadminロールの権限でコマンドを実行できる可能性があります。

注：Cisco Catalyst SD-WAN Managerリリース20.18以降はこの脆弱性の影響を受けません。

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。

バグID: CSCws33587
CVE ID：CVE-2026-20129
セキュリティ影響評価（SIR）：致命的
CVSS ベーススコア：9.8
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE-2026-20126:Cisco Catalyst SD-WAN Managerの特権昇格の脆弱性

Cisco Catalyst SD-WAN Managerの脆弱性により、権限の低い認証されたローカルの攻撃者が、基盤となるオペレーティングシステムのルート権限を取得する可能性があります。

この脆弱性は、REST APIのユーザ認証メカニズムが不十分であることに起因します。攻撃者は、該当システムのREST APIに要求を送信することで、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、基盤となるオペレーティングシステムに対する root

権限を取得する可能性があります。

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。

バグID: CSCws93470
CVE ID：CVE-2026-20126
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：7.8
CVSS ベクトル：CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE-2026-20133：Cisco Catalyst SD-WAN Manager における情報漏えいの脆弱性

Cisco Catalyst SD-WAN Manager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の機密情報を表示できる可能性があります。

この脆弱性は、ファイルシステムのアクセス制限が不十分であることに起因します。攻撃者は、該当システムのAPIにアクセスすることで、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、攻撃者は基盤となるオペレーティングシステムの機密情報を読み取る可能性があります。

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。

バグID: CSCws33583
CVE ID：CVE-2026-20133
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：7.5
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVE-2026-20122:Cisco Catalyst SD-WAN Managerの任意のファイルを上書きする脆弱性

Cisco Catalyst SD-WAN ManagerのAPIの脆弱性により、認証されたリモートの攻撃者がローカルファイルシステム上の任意のファイルを上書きできるようになる可能性があります。この脆弱性をエクスプロイトするには、攻撃者は該当システムでAPIアクセスを持つ有効な読み取り専用クレデンシャルを持っている必要があります。

この脆弱性は、該当システムのAPIインターフェイスでの不適切なファイル処理に起因します。攻撃者は、ローカルファイルシステムに悪意のあるファイルをアップロードすることで、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、攻撃者は該当システムの任意のファイルを上書きし、vmanage ユーザ権限を取得できる可能性があります。

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。

バグID: CSCws33584、CSCws33586
CVE ID：CVE-2026-20122
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：7.1
CVSSベクトル： CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L

CVE-2026-20128：Cisco Catalyst SD-WAN Manager における情報漏えいの脆弱性

Cisco Catalyst SD-WAN ManagerのData Collection Agent(DCA)機能の脆弱性により、認証されたローカルの攻撃者が該当システムのDCAユーザ権限を取得する可能性があります。この脆弱性を不正利用するには、攻撃者は該当システムで有効なvmanageクレデンシャルを持っている必要があります。

この脆弱性は、該当システムのDCAユーザのクレデンシャルファイルの存在に起因します。攻撃者は、権限の低いユーザとしてファイルシステムにアクセスし、該当システムからDCAパスワードを含むファイルを読み取ることで、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、攻撃者は影響を受ける別のシステムにアクセスし、DCAユーザ権限を取得できる可能性があります。

注：Cisco Catalyst SD-WAN Managerリリース20.18以降はこの脆弱性の影響を受けません。

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。

バグID: CSCws33585
CVE ID：CVE-2026-20128
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.5
CVSS ベクトル：CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

回避策

これら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のリリースを記載しています。右の列は、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、およびこれら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 Manager 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、本アドバイザリに記載されている脆弱性の不正利用事例とその公表は確認しておりません。

出典

これらの脆弱性は、Cisco Advanced Security Initiatives Group(ASIG)のArthur Vidineyevによる社内セキュリティテストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v

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

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 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。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、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。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

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。