Cisco Catalyst SD-WAN Manager の脆弱性

アドバイザリーID : cisco-sa-sdwan-mltvnps2-JxpWm7R
初公開日 : 2026-05-14 16:00
バージョン 1.0 : Final
CVSSスコア : 8.6
回避策 : No workarounds available
Cisco バグ ID : CSCwt38739 CSCwt55544 CSCwt38767

CVE-2026-20209
CVE-2026-20224
CVE-2026-20210

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、リモート攻撃者が機密情報へのアクセス、権限の昇格、またはアプリケーションへの不正アクセスを行う可能性があります。

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。

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お勧めします。

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-mltvnps2-JxpWm7R

該当製品

脆弱性のある製品

デバイスの設定に関係なく、Cisco Catalyst SD-WAN Manager がこれらの脆弱性の影響を受けます。

これらの脆弱性は、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。

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お勧めします。

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

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。さらに、いずれかの脆弱性の影響を受けるソフトウェアリリースであっても、他の脆弱性の影響は受けない場合があります。

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お勧めします。

脆弱性の詳細は以下のとおりです。

CVE-2026-20224:Cisco Catalyst SD-WAN ManagerのXML外部エンティティインジェクションの脆弱性

Cisco Catalyst SD-WAN Manager（旧称SD-WAN vManage）のWeb UI(Web UI)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、該当システムに保存されている任意のファイルを読み取る可能性があります。攻撃者は、有効なユーザクレデンシャルを持つ必要はありません。

この脆弱性は、XMLファイルを解析する際のXML External Entity(XXE)エントリの不適切な処理に起因します。攻撃者は、該当システムに巧妙に細工された要求を送信することにより、この脆弱性をエクスプロイトする可能性があります。不正利用に成功すると、攻撃者は該当システムに保存されている任意のファイル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:CSCwt55544
CVE ID：CVE-2026-20224

セキュリティ影響評価（SIR）：致命的
CVSS ベーススコア：8.6
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

CVE-2026-20209：Cisco Catalyst SD-WAN Manager の権限昇格の脆弱性

Cisco Catalyst SD-WAN Manager（以前のSD-WAN vManage）のWeb UI(Web UI)の脆弱性により、読み取り専用権限を持つ認証されたリモートの攻撃者が、権限を低から高に昇格させ、高権限ユーザとしてアクションを実行できる可能性があります。

この脆弱性は、機密セッション情報が監査ログに記録されるために存在します。攻撃者は、Cisco Catalyst SD-WAN Managerの読み取り専用権限を高特権ユーザの権限に昇格させることで、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、攻撃者は高特権ユーザとしてアクションを実行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:CSCwt38739
CVE ID：CVE-2026-20209
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.4
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

CVE-2026-20210：Cisco Catalyst SD-WAN Manager の権限昇格の脆弱性

Cisco Catalyst SD-WAN Manager（以前のSD-WAN vManage）のWeb UI(Web UI)における脆弱性により、読み取り専用権限を持つ認証されたリモートの攻撃者が、該当システムで設定を変更したり、不正なアクションを実行したりする可能性があります。

この脆弱性は、デバイス設定およびテンプレート内の機密情報の修正に失敗したために存在します。攻撃者は、読み取り専用権限を高特権ユーザの権限に昇格させることで、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、高特権ユーザとしてCisco Catalyst SD-WAN Manager内の設定にアクセスしたり、変更したり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。

バグID:CSCwt38767
CVE ID：CVE-2026-20210
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.4
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/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 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。

その他の情報が必要な場合は、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。

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。

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

シスコは、これらの脆弱性を報告していただいた次の方々に感謝いたします。

- Computacenter社のElise Imison氏：CVE-2026-20209およびCVE-2026-20210
- Khaled AlshaikhおよびKhalid Alharthi:CVE-2026-20224

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-mltvnps2-JxpWm7R

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

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。