Cisco Catalyst SD-WAN Manager の脆弱性

アドバイザリーID : cisco-sa-sdwan-vman-sc-LRLfu2z
初公開日 : 2023-09-27 16:00
最終更新日 : 2023-10-25 16:37
バージョン 1.3 : Final
CVSSスコア : 9.8
回避策 : No workarounds available
Cisco バグ ID : CSCvw59643 CSCvz62234 CSCwf68936 CSCwf55823 CSCwd46383 CSCwh03202

CVE-2023-20253
CVE-2023-20252
CVE-2023-20262
CVE-2023-20034
CVE-2023-20254

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（旧称 Cisco SD-WAN vManage）の複数の脆弱性により、攻撃者が、該当インスタンスにアクセスしたり、該当システムでサービス妨害（DoS）状態を引き起こしたりす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-vman-sc-LRLfu2z

該当製品

脆弱性のある製品

これらの脆弱性の影響を受けるのは、Cisco Catalyst SD-WAN Manager です。

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、これらの脆弱性が次のシスコ製品に影響を与えないことを確認しました。

- IOS XE ソフトウェア
- SD-WAN cEdge ルータ
- SD-WAN vEdge ルータ

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

脆弱性の詳細は以下のとおりです。

CVE-2023-20252：Cisco Catalyst SD-WAN Manager で確認された不正アクセスの脆弱性

Cisco Catalyst SD-WAN Manager のセキュリティ アサーション マークアップ言語（SAML）API 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任意のユーザーとしてアプリケーションに不正にアクセスする可能性があります。

この脆弱性は、SAML API の不適切な認証チェックに起因します。攻撃者は、要求を SAML API に直接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、攻撃者がアプリケーションへのアクセスに十分な認証トークンを生成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：CSCwh03202
CVE ID：CVE-2023-20252
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-2023-20253：Cisco Catalyst SD-WAN Manager で確認された不正な設定ロールバックの脆弱性

Cisco Catalyst SD-WAN Manager の CLI 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ローカルの攻撃者が、許可をバイパスしてコントローラ設定をロールバックし、その後、この設定がダウンストリームルータに展開される可能性があります。

この脆弱性は、Cisco Catalyst SD-WAN Manager CLI での不適切なアクセス制御の適用に起因し

ます。CLI への読み取り専用アクセス権を持つ攻撃者は、Cisco Catalyst SD-WAN Manager コントローラで設定ロールバックを開始することで、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、攻撃者が該当 Cisco Catalyst SD-WAN Manager インスタンスの設定をロールバックし、その後、この設定がダウンストリームルータに展開され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：CSCvz62234
CVE ID：CVE-2023-20253
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：8.4
CVSS ベクトル：CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:H

CVE-2023-20034：Cisco Catalyst SD-WAN Manager における情報漏えいの脆弱性

Cisco Catalyst SD-WAN Manager で使用される Elasticsearch のアクセス制御実装における脆弱性により、認証されていないリモート攻撃者が、Elasticsearch ユーザーの権限で該当システムの Elasticsearch データベースにアクセスする可能性があります。

この脆弱性は、Elasticsearch サービスに関する Cisco Catalyst SD-WAN Manager での不適切なアクセス制御に起因します。攻撃者は、到達可能な Cisco Catalyst SD-WAN Manager システム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、攻撃者がElasticsearch ユーザーとして Elasticsearch データベースのコンテンツを表示できるようにな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：CSCvw59643
CVE ID：CVE-2023-20034
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-2023-20254：Cisco Catalyst SD-WAN Manager における承認バイパスの脆弱性

Cisco Catalyst SD-WAN Manager マルチテナント機能のセッション管理システムにおける脆弱性により、認証されたリモート攻撃者が、同じ Cisco Catalyst SD-WAN Manager インスタンスによって管理されている別のテナントにアクセスす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、マルチテナント機能を有効にする必要があります。

この脆弱性は、Cisco Catalyst SD-WAN Manager システム内のユーザーセッション管理が不十分

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。エクスプロイトに成功すると、攻撃者が別のテナントに関する情報にアクセスしたり、設定を変更したり、場合によってはテナントをオフラインにして、DoS 状態を引き起こしたり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：CSCwf55823、CSCwf68936
CVE ID：CVE-2023-20254
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：7.2
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVE-2023-20262：Cisco Catalyst SD-WAN Manager におけるサービス妨害の脆弱性

Cisco Catalyst SD-WAN Manager の SSH サービスにおける脆弱性により、認証されていないリモート攻撃者がプロセスのクラッシュを引き起こし、その結果として SSH アクセスのみのサービス妨害（DoS）状態が発生する可能性があります。この脆弱性は、システムが機能しつづけることを妨げるものではなく、Web UI アクセスは影響を受けません。

この脆弱性は、該当システムがエラー状態のときにリソース管理が不十分であることに起因します。攻撃者は、悪意のあるトラフィックを該当システムに送信することで、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、攻撃者がSSH プロセスのクラッシュとリロードを引き起こし、SSH サービスのサービス妨害（DoS）状態を発生させ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：CSCwd46383
CVE ID：CVE-2023-20262
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.3
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

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

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様

は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

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。

ソフトウェアのアップグレードを検討する際には、シスコ セキュリティ アドバイザリ ページで入手でき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。

サービス契約をご利用でないお客様

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 TAC（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）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。

修正済みリリース

次の表では、最初の列に Cisco Catalyst SD-WAN Manager のリリースを示します。その次の列に、そのリリースがこのアドバイザリに記載された 1 つ以上の脆弱性の影響を受けるかどうかと、各脆弱性に対処するための最初の修正済みリリースを示します。

Release	CVE-2023-20252 重大 SIR	CVE-2023-20253 高 SIR	CVE-2023-20034 高 SIR	CVE-2023-20254 高 SIR	CVE-2023-20262 中 SIR
20.3 より前	影響なし。	影響なし。	修正済みリリースに移行。	影響なし。	修正済みリリースに移行。
20.3	影響なし。	影響なし。	20.3.4	影響なし。	20.3.7
20.4	影響なし。	修正済みリリースに移行。	修正済みリリースに移行。	修正済みリリースに移行。	修正済みリリースに移行。
20.5	影響なし。	修正済みリリースに移行。	修正済みリリースに移行。	修正済みリリースに移行。	修正済みリリースに移行。
20.6	影響なし。	20.6.2	20.6.1	20.6.3.4	20.6.6
20.7	影響なし。	20.7.1	20.7.1	修正済みリリースに移行。	修正済みリリースに移行。
20.8	影響なし。	20.8.1	影響なし。	修正済みリリースに移行。	修正済みリリースに移行。
20.9	20.9.41	20.9.1	影響なし。	20.9.3.2	20.9.3
20.10	影響なし。	20.10.1	影響なし。	20.10.1.2	修正済みリリースに移行。
20.11	修正済みリリースに移行します。[1]。	20.11.1	影響なし。	20.11.1.2	20.11.1
20.12	影響なし。	影響なし。	影響なし。	影響なし。	20.12.1

1. CVE-2023-20252 については、リリース 20.9.3.2 および 20.11.1.2 のみが影響を受けます。20.9 および 20.11 Train の以前のリリースは影響を受けません。

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されたリリース情報のみを検証します。

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

CVE-2023-20034、CVE-2023-20252、CVE-2023-20253、および CVE-2023-20262：これらの脆弱性は、内部セキュリティテストで発見されました。

CVE-2023-20254：この脆弱性を報告してくださった Liquid C2 社の Heba Farahat 氏および Hosam Gemei 氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-vman-sc-LRLfu2z

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.3	CVE-2023-20262の修正済みリリースを更新。	修正済みリリース	Final	2023-OCT-25
1.2	CVE-2023-20253 および CVE-2023-20254 の修正済みリリースを更新。	修正済みリリース	Final	2023 年 10 月 6 日
1.1	CVE-2023-20252 の修正済みリリースを更新。	修正済みリリース	Final	2023 年 9 月 29 日
1.0	初回公開リリース	—	Final	2023 年 9 月 27 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。