Cisco SD-WAN vManage ソフトウェアのコマンドインジェクションの脆弱性

アドバイザリーID : cisco-sa-clibypvman-sKcLf2L
初公開日 : 2020-07-15 16:00
バージョン 1.0 : Final
CVSSスコア : 7.8
回避策 : No workarounds available
Cisco バグ ID : CSCvs11282

CVE-2020-3388

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 SD-WAN vManage ソフトウェアの CLI の脆弱性により、認証されたローカルの攻撃者がルート権限で実行される任意のコマンドを挿入する可能性があります。

この脆弱性は、入力に対する不十分な検証に起因します。攻撃者は、デバイスに認証され、巧妙に細工された入力を CLI に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。CLI にアクセスするには、攻撃者は認証される必要があります。エクスプロイトに成功すると、攻撃者は root 権限でコマンド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。

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-clibypvman-sKcLf2L

該当製品

脆弱性のある製品

この脆弱性は、Cisco SD-WAN vManage ソフトウェアリリースに影響を与えます。

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。

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- IOS XE SD-WAN ソフトウェア
- SD-WAN cEdge ルータ
- SD-WAN vBond Orchestrator ソフトウェア
- SD-WAN vEdge ルータ
- SD-WAN vSmart コントローラソフトウェア

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。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 https://www.cisco.com/c/en/us/products/end-user-license-agreement.html に記載の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。

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。

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

次の表に示す適切な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お勧めします。本アドバイザリは以下のアドバイザリを含むコレクションの一部です。お客様におかれましては、これらも考慮したうえでアップグレード ソリューション全体をご確認ください。

- cisco-sa-sdw-dos-KWOdyHnB:Cisco SD-WANソリューションソフトウェアのDoS脆弱性
- cisco-sa-sdscred-HfWWfqBj:Cisco SD-WANソリューションソフトウェアのスタティッククレデンシャルの脆弱性
- cisco-sa-vedgfpdos-PkqQrnwV:Cisco SD-WAN vEdgeルータのDoS脆弱性
- cisco-sa-fpdos-hORBfd9f:Cisco SD-WAN vEdgeルータのDoS脆弱性
- cisco-sa-clibypvman-sKcLf2L:Cisco SD-WAN vManageソフトウェアのコマンドインジェクションの脆弱性
- cisco-sa-vmdirtrav-eFdAxsJg:Cisco SD-WAN vManageソフトウェアのディレクトリトラバーサルの脆弱性
- cisco-sa-vmanrce-4jtWT28P:Cisco SD-WAN vManageソフトウェアのリモートコード実行の脆弱性

Cisco SD-WAN vManage ソフトウェアリリース	この脆弱性に対する最初の修正リリース	First Fixed Release for All Vulnerabilities Described in the Collection of Advisories
18.3 より前	修正済みリリースに移行。	修正済みリリースに移行。
18.3	修正済みリリースに移行。	修正済みリリースに移行。
18.4	18.4.5	修正済みリリースに移行。
19.2	19.2.2	19.2.3
19.3	修正済みリリースに移行。	修正済みリリースに移行。
20.1	20.1.1	修正済みリリースに移行。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）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やその公表を確認していません。

出典

この脆弱性を報告していただいた Orange CERT/CC に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clibypvman-sKcLf2L

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	2020 年 7 月 15 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。