

Cisco SD-WAN ソリューションにおいて任意のファイルが上書きされる脆弱性

High

アドバイザリーID : cisco-sa-20190123-sdwan-file-write

[CVE-2019-1650](#)

初公開日 : 2019-01-23 16:00

バージョン 1.0 : Final

CVSSスコア : [8.8](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCvi69862](#)

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 ソリューションの脆弱性により、認証されたリモートの攻撃者が、該当デバイスの基盤となるオペレーティング システム上で任意のファイルを上書きする場合があります。

この脆弱性は、影響を受けるソフトウェアの CLI での **save** コマンドの入力の検証が不適切なことに起因しています。攻撃者は、影響を受けるデバイスの CLI で **save** コマンドを変更することで、この脆弱性をエクスプロイトできます。エクスプロイトに成功すると、攻撃者は該当デバイスの基盤となるオペレーティング システム上で任意のファイルを上書きし、権限を *root* ユーザーに昇格させる場合があります。

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ました。この脆弱性に対処する回避策はありません。

このアドバイザリーは、次のリンクより確認できます。

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-sdwan-file-write>

該当製品

脆弱性のある製品

この脆弱性は、リリース 18.4.0 より前の Cisco SD-WAN ソリューションを実行している下記のシスコ製品に影響を及ぼします。

- vBond Orchestrator ソフトウェア
- vEdge 100 シリーズ ルータ
- vEdge 1000 シリーズ ルータ
- vEdge 2000 シリーズ ルータ
- vEdge 5000 シリーズ ルータ
- vEdge Cloud ルータ プラットフォーム
- vManage ネットワーク管理用ソフトウェア
- vSmart コントローラ ソフトウェア

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[脆弱性が存在する製品の](#)セクションにリストされている製品だけ既知この脆弱性によって影響されるためである。

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 アップデートを提供しています。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、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、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です。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、[Cisco Security Advisories and Alerts 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完全なアップグレード ソリューション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は新規リリースでも継続して適切なサポートが受けられることを確認してください。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 に連絡してアップグレードを入手してください。

<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

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

Cisco SD-WAN ソリューションのリリース 18.4.0 では脆弱性が修正済みです。

Cisco SD-WAN ソリューションは、[すべて参照 (Browse all)] をクリックし、次の場所にアクセスすることで、Cisco.com の [Software Center](#) からダウンロードできます。

vBond、vEdge Cloud、および vSmart

1. [ルータ (Routers)] > [Software-Defined WAN (SD-WAN)] > [SD-WAN] > [SD-WANソフトウェアアップデート (SD-WAN Software Update)] にアクセスします。
2. 左側のパネルで、[最新リリース (Latest Release)] の下にある [18.4.0] をクリックします。
3. [vSmart、vEdge Cloud およびvBond 18.4.0アップグレードイメージ (vSmart, vEdge Cloud and vBond 18.4.0 upgrade image)] を選択します。

vEdge 100、1000、および 2000 シリーズ ルータ

1. [ルータ (Routers)] > [Software-Defined WAN (SD-WAN)] > [vEdgeルータ (vEdge Router)] > [vEdgeルータモデル (vEdge Router Model)] を選択します。
2. 左側のパネルで、[最新リリース (Latest Release)] の下にある [18.4.0] をクリックします。
3. [vEdge 100b、vEdge 100m、vEdge 1000、vEdge 2000ルータ用のvEdge 18.4.0アップグレードイメージ (vEdge 18.4.0 Upgrade Image for vEdge 100b, vEdge 100m, vEdge 1000, vEdge 2000 Routers)] を選択します。

vManage ネットワーク管理用ソフトウェア

1. [ルータ (Routers)] > [Software-Defined WAN (SD-WAN)] > [SD-WAN] > [SD-WANソフトウェアアップデート (SD-WAN Software Update)] にアクセスします。
2. 左側のパネルで、[最新リリース (Latest Release)] の下にある [18.4.0] をクリックします。
3. [vManage 18.4.0アップグレードイメージ (vManage 18.4.0 upgrade image)] を選択します。

不正利用事例と公式発表

Cisco Product Security Incident Response Team (PSIRT) では、本アドバイザリに記載されている脆弱性のエクスプロイト事例やその公表を確認していません。

出典

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-sdwan-file-write>

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.0	初回公開リリース		最終版	2019 年 1 月 23 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、単独の転載や意識を施した場合、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。