Cisco SD-WAN ソリューションのコマンド インジェクションの脆弱性

High

アドバイザリーID : cisco-sa-20180905-sd-wan-injection

初公開日 : 2018-09-05 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 : CSCvi69903 CSCvi69802

CVE-2018-0433

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 Command Line Interface （ CLI ）の脆弱性は*ルート 特権*と実行される任意のコマンドをインジェクトする認証された、ローカル攻撃者を可能に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にによって認証し、CLI ユーティリティに巧妙に細工された 入力を入れることこの脆弱性を不正利用する可能性があります。

攻撃者は CLI ユーティリティにアクセスするために認証する必要があります。 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。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180905-sd-wan-injection

該当製品

脆弱性のある製品

この脆弱性は、リリース 18.3.0 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。

- 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
- vManage ネットワーク管理システム
- vEdge Cloud ルータ プラットフォーム
- vSmart コントローラ ソフトウェア
- vBond Orchestrator 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。

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、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 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

この脆弱性は、Cisco SD-WAN ソリューションのリリース 18.3.0 で修正されています。

このソフトウェアは Cisco. Com の Software Center からダウンロードできます。[すべて参照（Browse all）] をクリックし、次の手順でアクセスします。

vBond、vEdge Cloud、および vSmart

1. **ルータ**へのナビゲート **> ソフトウェア定義された WAN（SD-WAN）> SD-WAN > SD-WAN ソフトウェア アップデート**。
2. 左パネルから、**最新リリース**の下で 18.3.0 をクリックして下さい。
3. **vSmart、vEdge Cloud および vBond 18.3.0 アップグレード イメージを**選択して下さい。

vEdge 100、1000、および 2000 シリーズ ルータ

1. **> ソフトウェア定義された WAN（SD-WAN）はルータ**に **> vEdge ルータ > vEdge ルータ モデル** ナビゲート します。
2. 左パネルから、**最新リリース**の下で 18.3.0 をクリックして下さい。
3. **vEdge 100b のための vEdge 18.3.0 アップグレード イメージを、vEdge 100m、vEdge 1000、vEdge 2000 ルータ**選択して下さい。

vManage ネットワーク管理用ソフトウェア

1. **ルータ**へのナビゲート **> ソフトウェア定義された WAN（SD-WAN）> SD-WAN > SD-WAN ソフトウェア アップデート**。
2. 左パネルから、**最新リリース**の下で 18.3.0 をクリックして下さい。
3. **vManage 18.3.0 アップグレード イメージを**選択して下さい。

注: Cisco vEdge 5000 シリーズ ルータ向けのソフトウェアは、Viptela カスタマー サポート ポータルからダウンロードできます。

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-20180905-sd-wan-injection

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2018-September-05

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。