# 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


アドバイザリーID : cisco-sa-20180718-sdwan-coinj
初公開日 : 2018-07-18 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 : CSCvi69751

CVE-2018-0351

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 ソリューションのコマンドライン tcpdump ユーティリティの脆弱性により、認証されたローカルの攻撃者が、root 権限で実行される任意のコマンドを挿入できる場合があります。

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 tcpdump ユーティリティに送信することで、この脆弱性をエクスプロイトする可能性があります。

tcpdump ユーティリティ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-20180718-sdwan-coinj

## 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。

- 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、[シスコのセキュリティアドバイザリおよびアラート（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 Cisco Service Contract 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 POS 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（Routers）] > [Software-Defined 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. 左側のパネルの [最新のリリース（Latest Release）] の下の [18.3.0] をクリックします
3. [vSmart、vEdge CloudおよびvBond 18.3.0アップグレードイメージ（vSmart, vEdge Cloud and vBond 18.3.0 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. 左側のパネルの [最新のリリース（Latest Release）] の下の [18.3.0] をクリックします
3. [vEdge 100b、vEdge 100m、vEdge 1000、vEdge 2000 ルータ用のvEdge 18.3.0アップグレードイメージ（vEdge 18.3.0 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. 左側のパネルの [最新のリリース（Latest Release）] の下の [18.3.0] をクリックします
3. [vManage 18.3.0アップグレードイメージ（vManage 18.3.0 upgrade image）] を選択します

注：Cisco vEdge 5000シリーズルータ用のソフトウェアは、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）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

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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180718-sdwan-coinj

## 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 | 2018 年 7 月 18 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。