Cisco SD-WAN ソリューションソフトウェアのサービス妨害の脆弱性

High	**アドバイザリーID :** cisco-sa-sdw-dos-KWOdyHnB **初公開日 :** 2020-07-15 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 8.6 **回避策 :** No workarounds available **Cisco バグ ID :** CSCvj14805	CVE-2020-3351

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 ソリューションソフトウェアの脆弱性により、認証されていないリモートの攻撃者がサービス妨害（DoS）状態を引き起こす可能性があります。

この脆弱性は、UDP パケットでカプセル化された Cisco SD-WAN のピアリングメッセージの検証が適切に行われていないことに起因します。 攻撃者は、巧妙に細工された UDP メッセージをターゲットシステム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。 エクスプロイトに成功すると、攻撃者はデバイス上のサービスで障害を発生させ、そのサービスを利用するターゲットデバイスなどのデバイスに影響を与える DoS 状態を引き起こす可能性があります。

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。

このアドバイザリは、次のリンクより確認できます。
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdw-dos-KWOdyHnB

該当製品

脆弱性のある製品

この脆弱性は、リリース 17.2.7 または 18.3.0 より前の Cisco SD-WAN ソリューションソフトウェアを実行している次のシスコ製品に影響を与えます。

- SD-WAN vBond Orchestrator ソフトウェア
- SD-WAN vEdge 100 シリーズ ルータ
- SD-WAN vEdge 1000 シリーズ ルータ
- SD-WAN vEdge 2000 シリーズ ルータ
- SD-WAN vEdge 5000 シリーズ ルータ
- SD-WAN vEdge クラウドルータ
- SD-WAN vManage ソフトウェア
- SD-WAN 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リストされている製品だけがこの脆弱性の影響を受けることが知られています。

シスコでは、この脆弱性が Cisco IOS XE SD-WAN ソフトウェアには影響を与えないことを確認しています。

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、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

この脆弱性は、Cisco SD-WAN ソリューションソフトウェアのリリース 17.2.7 以降とリリース 18.3.0 以降で修正されています。

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サービス妨害の脆弱性
- cisco-sa-sdscred-HfWWfqBj： Cisco SD-WAN ソリューションソフトウェアの静的ログイン情報の脆弱性
- cisco-sa-vedgfpdos-PkqQrnwV： Cisco SD-WAN vEdge ルータのサービス妨害の脆弱性
- cisco-sa-fpdos-hORBfd9f： Cisco SD-WAN vEdge ルータのサービス妨害の脆弱性
- 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

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-sdw-dos-KWOdyHnB

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	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。