

Cisco SD-WAN vManage ソフトウェア情報公開脆弱性

Medium	アドバイザーID : cisco-sa-vmanwebid-5QWMCvt	CVE-2020-3437
	初公開日 : 2020-07-15 16:00	
	バージョン 1.0 : Final	
	CVSSスコア : 6.5	
	回避策 : No workarounds available	
	Cisco バグ ID : CSCvt65026	

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 ソフトウェアのウェブベースの管理インターフェイスの脆弱性はデバイスの根本的なファイルシステムで任意ファイルを読み込む認証される、リモート攻撃者可能にする可能性があります。

脆弱性は不十分なファイル スコープ制限が原因です。 攻撃者はファイルシステムの特定のファイル参照を作成することおよびウェブベースの管理インターフェイスを通してアクセスすることによってこの脆弱性を不正利用する可能性があります。 正常なエクスプロイトは攻撃者が基礎オペレーティング システムのファイルシステムからの任意ファイルを読むことを可能にす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-vmanwebid-5QWMCvt>

該当製品

脆弱性のある製品

パブリケーションの時に、この脆弱性は Cisco SD-WAN vManage ソフトウェア リリースにリリース 19.2.3 より先に該当しました。

最も完全な、現在の情報についてはこのアドバイザリの上でバグIDの詳細 セクションを参照して下さい。

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。

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

[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。

修正済みリリース

出版物の時に、Cisco SD-WAN vManage ソフトウェアリリース 19.2.3 およびそれ以降はこの脆弱性のための修正が含まれていました。

最も完全な、現在の情報についてはこのアドバイザリの上でバグIDの詳細 セクションを参照して下さい。

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

Cisco はこの脆弱性を報告するためにウォールマート セキュリティのジョニー Yu に感謝することを望みます。

URL

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanwebid-5QWMCvt>

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-JUL-15

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。