

Cisco Data Center Network Managerの認証バイパスの脆弱性

Medium	アドバイザーID : cisco-sa-dcnm-bypass-auth-mVDR6ygT	CVE-2020-3540
	初公開日 : 2020-08-19 16:00	
	バージョン 1.0 : Final	
	CVSSスコア : 6.3	
	回避策 : No workarounds available	
	Cisco バグ ID : CSCvu68927	

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 Data Center Network Manager(DCNM)ソフトウェアのWebベース管理インターフェ이스の脆弱性により、認証されたりモートの攻撃者が、適切な認証なしでデータを表示、変更、および削除できる可能性があります。

この脆弱性は、管理者専用のリソースへのアクセスを制限できないことに起因します。低レベルの権限を持つ攻撃者は、巧妙に細工されたURLを該当デバイスに送信することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、管理者の権限を持つユーザと同じ方法で、テンプレートの一覧表示、表示、作成、編集、および削除が可能になります。

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-dcnm-bypass-auth-mVDR6ygT>

該当製品

脆弱性のある製品

発行時点では、この脆弱性はリリース11.4(1)より前のCisco DCNMソフトウェアリリースに影響を与えました。

最も完全で最新の情報については、このアドバイザリの上部にあるBug IDの「詳細」セクションを参照してください。

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

公開時点で、Cisco DCNMソフトウェアリリース11.4(1)以降には、この脆弱性に対する修正が含まれています。

最も完全で最新の情報については、このアドバイザリの上部にあるBug IDの「詳細」セクションを参照してください。

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

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

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8月19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。