Cisco Data Center Network Manager で権限が昇格される脆弱性

Medium	**アドバイザリーID :** cisco-sa-dcnm-privescal-zxfCH7Dg **初公開日 :** 2020-07-15 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 :** CSCvt54515	CVE-2020-3380

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 ）の CLI の脆弱性は基礎オペレーティング システムの任意のコマンドを*定着させ*、実行する特権を上げる認証された、ローカル攻撃者を可能にする可能性があります。

脆弱性は影響を受けた CLI コマンドの実行中に不十分な制限が原因です。 攻撃者は fmserver ユーザとしてによって認証し、特定のコマンドに悪意のある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。 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 システムの任意のコマンドを*定着させ*、実行する特権を上げる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-dcnm-privescal-zxfCH7Dg

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 DCNM ソフトウェア リリースにリリース 11.4(1) 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、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 DCNM ソフトウェアリリース 11.4(1) 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

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-dcnm-privescal-zxfCH7Dg

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。