

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



アドバイザーID : [cisco-sa-dcnm-auth-bypass-JkubGpu3](#) [CVE-2020-3376](#)
初公開日 : 2020-07-29 16:00
バージョン 1.0 : Final
CVSSスコア : [7.3](#)
回避策 : No workarounds available
Cisco バグ ID : [CSCvt54527](#)

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) のデバイス マネージャ アプリケーションで脆弱性が確認されました。認証されていないリモートからの攻撃者が該当デバイスで認証をバイパスし、任意のコマンドを実行する可能性があります。

この脆弱性は、認証を実行するソフトウェアの障害に起因します。Cisco DCNM でホストされている URL のいずれかが参照されると、この脆弱性がエクスプロイトされる危険性があります。エクスプロイトに成功すると、攻撃者は Cisco DCNM 内の特定機能とやり取りして、使用できるようになります。

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ソフトウェア アップデートを提供しています。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-dcnm-auth-bypass-JkubGpu3>

該当製品

脆弱性のある製品

この脆弱性は、OVA の展開、Windows DCNM-SAN のインストール、Linux DCNM-SAN のインストールといった DCNM-SAN の展開に影響を与えます。

この脆弱性の影響を受けるのは、Cisco DCNM ソフトウェアのリリース 11.0(1)、11.1(1)、11.2(1)、および 11.3(1) です。

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。](#)

シスコでは、この脆弱性が Cisco Data Center Network Manager リリース 7.x および 10.x には影響を及ぼさ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 <https://www.cisco.com/c/en/us/products/end-user-license-agreement.html> に記載の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。

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です。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 (https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html) に連

[絡してアップグレードを入手してください。](#)

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

Cisco DCNM ソフトウェアのリリース 11.4(1) 以降では、この脆弱性は修正されています。

Cisco.com の [Software Center からソフトウェアをダウンロードするには、次の手順を実行します。](#)

1. [すべてを参照 (Browse All)] をクリックします。
2. [クラウドおよびシステムの管理 (Cloud and Systems Management)] > [データセンターインフラストラクチャの管理 (Data Center Infrastructure Management)] > [Data Center Network Manager] の順に選択します。
3. Data Center Network Manager のページの左側にあるペインからリリースを選択します。

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-dcnm-auth-bypass-JkubGpu3>

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	2020 年 7 月 29 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。

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。