Cisco Data Center Network Manager のパス トラバーサルの脆弱性

High

アドバイザリーID : cisco-sa-dcnm-path-trav-2xZOnJdR

初公開日 : 2020-07-29 16:00

バージョン 1.0 : Final

CVSSスコア : 8.8

回避策 : No workarounds available

Cisco バグ ID : CSCvu28384

CVE-2020-3383

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)のアーカイブユーティリティの脆弱性により、認証されたリモートの攻撃者が該当デバイスでディレクトリトラバーサル攻撃を行う可能性があります。

この脆弱性は、アーカイブファイル内に埋め込まれているパスの正しい入力検証がないことに起因します。攻撃者は、巧妙に細工された要求を該当デバイスに送信することにより、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、攻撃者はログインユーザの権限でシステム内の任意のファイルを書き込むことができます。

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-path-trav-2xZOnJdR

該当製品

脆弱性のある製品

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が 11.4(1) より前の場合です。

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

シスコでは、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、アクセスまたはその他の方法で使用した場合、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、シスコから直接、あるいはシスコ認定リセラーまたはパートナーからそのソフトウェアの有効なライセンスを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

Cisco DCNM ソフトウェアリリース 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）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-path-trav-2xZOnJdR

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 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。