Cisco Data Center Network ManagerのREST APIの脆弱性

Medium	**アドバイザリーID :** cisco-sa-dcnm-api-path-TpTApx2p **初公開日 :** 2021-01-20 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 :** CSCvu28385 CSCvt82606 CSCvu28383	CVE-2021-1133 CVE-2021-1135 CVE-2021-1255

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REST APIエンドポイントにおける複数の脆弱性により、認証されたリモートの攻撃者が適切な権限なしでデータを表示、変更、削除できる可能性があります。

これらの脆弱性の詳細については本アドバイザリの「詳細情報」セクションを参照してください。

シスコはこれら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ています。これら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-api-path-TpTApx2p

該当製品

脆弱性のある製品

公開時点では、これらの脆弱性はリリース11.4(1)より前のCisco DCNM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バグ 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。

詳細

これらの脆弱性は依存関係にはなく、これらの脆弱性の1つを悪用しても、他の脆弱性を悪用する必要はありません。さらに、いずれかの脆弱性の影響を受けるソフトウェアリリースであっても、他の脆弱性の影響は受けない場合があります。

これらの脆弱性の詳細については、次のとおりです。

CVE-2021-1133:Cisco Data Center Network Managerのパストラバーサルの脆弱性

Cisco Data Center Network Manager(DCNM)のREST APIの脆弱性により、権限の低いアカウントを持つ認証されたリモートの攻撃者が、該当デバイスに対してパストラバーサル攻撃を実行できる可能性があります。

この脆弱性は、API に対するユーザ入力の検証が不十分であることに起因します。攻撃者は、巧妙に細工された要求を API 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、攻撃者はファイルシステム上の任意のファイルを削除でき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ています。この脆弱性に対処する回避策はありません。

Bug ID:CSCvt82606
CVE-ID:CVE-2021-1133
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.5
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

CVE-2021-1255:Cisco Data Center Network Managerのパストラバーサルの脆弱性

Cisco Data Center Network Manager(DCNM)の特定のREST APIエンドポイントの脆弱性により、認証されたリモートの攻撃者が該当デバイスに対してパストラバーサル攻撃を実行できる可能性があります。

この脆弱性は、不十分なパス制限の適用に起因します。攻撃者は、該当デバイスに巧妙に細工された HTTP 要求を送信することにより、この脆弱性をエクスプロイトすることができます。エク

スプロイトに成功すると、攻撃者は該当デバイス上の任意のファイルを上書きまたはリストでき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ています。この脆弱性に対処する回避策はありません。

Bug ID:CSCvu28383
CVE-ID:CVE-2021-1255
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：4.6
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N

CVE-2021-1135:Cisco DCNMソフトウェアの設定バイパスの脆弱性

Cisco Data Center Network Manager(DCNM)の特定のREST APIエンドポイントにおける脆弱性により、認証されたリモートの攻撃者が該当デバイスのセキュリティ制御をバイパスし、デフォルトのサーバ設定を変更できる可能性があります。

この脆弱性は、denylist実装での比較が正しくないことに起因します。攻撃者は、該当ソフトウェアに特別に巧妙に細工されたネットワークトラフィックを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、攻撃者は該当デバイスのサーバ設定を変更でき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ています。この脆弱性に対処する回避策はありません。

Bug ID:CSCvu28385
CVE-ID:CVE-2021-1135
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：4.3
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N

回避策

これら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アップグレード ソリューション一式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。

修正済みリリース

公開時点では、Cisco DCNMリリース11.4(1)以降に、これら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バグ 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とその公表は確認しておりません。

出典

この脆弱性は、シスコ内部でのシステム 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-api-path-TpTApx2p

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	2021 年 1 月 20 日

利用規約

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。