Cisco Data Center Network Managerの脆弱性

Medium	**アドバイザリーID :** cisco-sa-dcnm-xss-vulns-GuUJ39gh **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 :** CSCvv00638 CSCvv87589 CSCvv87614 CSCvv87602 CSCvv00646 CSCvv00645 CSCvv00642 CSCvv07930 CSCvv87608 CSCvv00644 CSCvv00643 CSCvv00654 CSCvu68933 CSCvu50101	CVE-2021-1250 CVE-2021-1253 CVE-2021-1286 CVE-2021-1249

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Webベース管理インターフェイスにおける複数の脆弱性により、*ネットワークオペレータ*権限を持つリモート攻撃者が、インターフェイスのユーザに対してクロスサイトスクリプティング(XSS)攻撃またはリフレッシュファイルダウンロード(RFD)攻撃を実行す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-xss-vulns-GuUJ39gh

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11.5(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、これら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、いずれかの脆弱性を工クスプロイトするために、他の脆弱性を工クスプロイトする必要はありません。また、いずれかの脆弱性の影響を受ける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-2021-1249:Cisco DCNMのクロスサイトスクリプティングの脆弱性

Cisco DCNMのWebベース管理インターフェイスの複数の脆弱性により、認証されたリモートの攻撃者がインターフェイスのユーザに対してXSS攻撃を実行する可能性があります。

これらの脆弱性は、Webベースの管理インターフェイスによる不十分な入力検証に起因します。攻撃者は、インターフェイスの特定のデータフィールドに悪意のあるデータを挿入することにより、これら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、攻撃者は該当インターフェイスのコンテキストで任意のスクリプトコードを実行したり、ブラウザベースの機密情報にアクセスする可能性があります。

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。

Bug ID:CSCvv00645、CSCvu50101、CSCvu49711、CSCvu68933
CVE ID：CVE-2021-1249
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:R/S:C/C:L/I:L/A:L

CVE-2021-1286:Cisco DCNM Reflected File Downloadの脆弱性

Cisco DCNMのWebベース管理インターフェイスに複数の脆弱性が存在するため、認証されてい

ないリモートの攻撃者が該当デバイスのインターフェイスのユーザに対してRFD攻撃を実行する可能性があります。

これらの脆弱性は、Webベースの管理インターフェイスによ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、インターフェイスに悪意のある入力を送信するリンクをクリックするように認証されたユーザを誘導することで、これら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で任意のスクリプトコードを実行できる可能性があります。

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。

Bug ID:CSCvv87608、CSCvv87589、CSCvv87602
CVE ID：CVE-2021-1286
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.1
CVSSベクトル：CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:N/I:H/A:N

CVE-2021-1250:Cisco DCNMのクロスサイトスクリプティングの脆弱性

Cisco DCNMのWebベース管理インターフェイスの複数の脆弱性により、認証されたリモートの攻撃者がインターフェイスのユーザに対してXSS攻撃を実行する可能性があります。

これらの脆弱性は、Webベースの管理インターフェイスによる不十分な入力検証に起因します。攻撃者は、インターフェイスの特定のデータフィールドに悪意のあるデータを挿入することにより、これら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、攻撃者は該当インターフェイスのコンテキストで任意のスクリプトコードを実行したり、ブラウザベースの機密情報にアクセスする可能性があります。

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。

Bug ID:CSCv00642、CSCv87614、CSCv00638、CSCv00644、CSCv00654、CSCv00643
CVE ID：CVE-2021-1250
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.9
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:L

CVE-2021-1253:Cisco DCNMの永続的なクロスサイトスクリプティングの脆弱性

Cisco DCNMのWebベース管理インターフェイスの複数の脆弱性により、認証されたリモートの攻撃者がインターフェイスのユーザに対してXSS攻撃を実行する可能性があります。

これらの脆弱性は、Webベースの管理インターフェイスによる不十分な入力検証に起因します。

攻撃者は、インターフェイスの特定のデータフィールドに悪意のあるデータを挿入することにより、これら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、攻撃者は該当インターフェイスのコンテキストで任意のスクリプトコードを実行したり、ブラウザベースの機密情報にアクセスする可能性があります。

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。

Bug ID:CSCvv07930、CSCvv00646
CVE ID：CVE-2021-1253
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.9
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:L

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 Data Center Network Manager(DCNM)リリース11.5(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-xss-vulns-GuUJ39gh

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。