

# Cisco Data Center Network Manager における任意のファイルのダウンロードに関する脆弱性



アドバイザリーID : [cisco-sa-20190626-dcnm-file-dwnld](#) [CVE-2019-1621](#)  
初公開日 : 2019-06-26 16:00  
最終更新日 : 2019-09-19 16:08  
バージョン 1.1 : Final  
CVSSスコア : [7.5](#)  
回避策 : No workarounds available  
Cisco バグ ID : [CSCvo64651](#)

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이스の脆弱性により、認証されていないリモートの攻撃者が該当デバイスの機密ファイルにアクセスできる危険性があります。

この脆弱性は、該当の DCNM ソフトウェアにおける権限の設定が不適切であることに起因しています。攻撃者は、該当デバイスの Web ベース管理インターフェ이스に接続して特定の URL を要求することにより、この脆弱性を不正利用できます。不正利用が成功すると、攻撃者が該当デバイスの基盤となるファイルシステムから任意のファイルをダウンロードできる危険性があります。

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。

このアドバイザリーは、次のリンクより確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190626-dcnm-file-dwnld>

## 該当製品

### 脆弱性のある製品

この脆弱性は、リリース 11.2(1) より前の Cisco Data Center Network Manager ( DCNM ) ソフトウェアリリースに影響します。

## 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。](#)

## 詳細

攻撃者は、該当の DCNM デバイスで使用可能な特定の Web サーブレットを使用して、基盤となるファイルシステムから任意のファイルをダウンロードできます。

DCNM ソフトウェア リリース 11.0(1) 以前で攻撃者がこの脆弱性を不正利用するには、DCNM の Web ベース管理インターフェイスに対して認証される必要があります。

DCNM ソフトウェア リリース 11.1(1) では、未認証の状態では該当の Web サーブレットにアクセスし、認証されていない攻撃者がこの脆弱性を不正利用できます。

該当の Web サーブレットは、DCNM ソフトウェア リリース 11.2(1) で完全に削除されています。

## 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、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 Cisco Service Contract 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 POS 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

この脆弱性は、DCNM ソフトウェア リリース 11.2(1) 以降で修正されています。

このソフトウェアは、Cisco.com の [Software Center から次の手順でダウンロードできます。](#)

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] ページの左側のペインにあるリリースにアクセスします。

## 不正利用事例と公式発表

Cisco Product Security Incident Response Team ( PSIRT ) は、アドバイザリで説明されている脆弱性に対して概念実証段階のエクスプロイト コードが入手可能であることを認識しています。

このアドバイザリで説明されている脆弱性の悪用に関する情報は Cisco PSIRT に寄せられていません。

## 出典

iDefense の Vulnerability Contributor Program にこの脆弱性を報告していただいた個人のセキュリティ研究者である Pedro Ribeiro 氏に感謝いたします。

## URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190626-dcnm-file-dwnld>

## 改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	概念実証段階の 익스プロイト の可用性が記載されています。	不正利用事例と公式発表	Final	2019年9月19日
1.0	初回公開リリース	—	Final	2019年6月26日

## 利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザー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。