

# Cisco Data Center Network ManagerのJBoss EAPの不正アクセスの脆弱性



アドバイザリーID : cisco-sa-20200102-[CVE-2019-15999](#)  
dcnm-unauth-access  
初公開日 : 2020-01-02 16:00  
最終更新日 : 2020-01-15 15:57  
バージョン 1.1 : Final  
CVSSスコア : [5.4](#)  
回避策 : No workarounds available  
Cisco バグ ID : [CSCvs00139](#)

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)のアプリケーション環境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JBoss Enterprise Application Platform(JBoss EAP)への不正アクセスを取得する可能性があります。

この脆弱性は、JBoss EAPの認証設定の誤った設定に起因します。攻撃者は、特定の権限の低いアカウントで認証を行うことで、この脆弱性をエクスプロイト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JBoss EAPへの不正アクセスを取得できる可能性があります。これは、内部システムアカウントに限定する必要があります。

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-20200102-dcnm-unauth-access>

## 該当製品

### 脆弱性のある製品

公開時点では、この脆弱性は、Microsoft Windows、Linux、および仮想アプライアンスプラットフォーム用のリリース11.3(1)より前のCisco DCNMソフトウェア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。](#)

## 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

[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。

## 修正済みリリース

公開時点では、Cisco DCNMソフトウェアリリース11.3(1)以降にこ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。

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、この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 익스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

シスコは、この脆弱性を報告していただいたPatchAdvisorのHarrison Neal氏に感謝いたします。

## URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200102-dcnm-unauth-access>

## 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	익스プロイトコードの入手状況に関する情報を更新。	不正利用事例と公式発表	Final	2020年1月15日
1.0	初回公開リリース	—	Final	2020年1月2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。