Cisco Data Center Network Manager の認証バイパスの脆弱性

アドバイザリーID : cisco-sa-20190626-dcnm-bypass
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 : 9.8
回避策 : No workarounds available
Cisco バグ ID : CSCvo64641

CVE-2019-1619

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で管理権限を使用して認証をバイパスし、任意のアクションを実行できる危険性があります。

この脆弱性は、該当の DCNM ソフトウェアでセッションが適切に管理されていないことに起因しています。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、この脆弱性を不正利用する可能性があります。不正利用が成功すると、該当デバイスの管理アクセス権を攻撃者に取得され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-bypass

該当製品

脆弱性のある製品

この脆弱性は、リリース 11.1(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、該当デバイスで使用可能な特定の Web サーブレットに巧妙に細工された HTTP 要求を送信することにより、管理ユーザのパスワードを知らなくても有効なセッション Cookie を取得できます。

シスコは、DCNM ソフトウェア リリース 11.0(1) で該当の Web サーブレットの使用を停止しました。このバージョンには既知の攻撃ベクトルはありません。

シスコは、DCNM ソフトウェア リリース 11.1(1) で該当の Web サーブレットを完全に削除しました。

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

シスコは、Cisco DCNM ソフトウェア リリース 11.1(1) 以降でこの脆弱性を修正しました。

Cisco Data Center Network Manager 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-bypass

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	概念実証段階のエクス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

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。