Cisco Digital Network Architecture Center の認証バイパスの脆弱性

Critical

アドバイザリーID : cisco-sa-20180516-dna2

初公開日 : 2018-05-16 16:00

バージョン 1.0 : Final

CVSSスコア : 10.0

回避策 : No workarounds available

Cisco バグ ID : CSCvi09394

CVE-2018-0271

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 Digital Network Architecture（DNA）Centerの API ゲートウェイの脆弱性により、認証されていないリモートの攻撃者が認証をバイパスし、重要なサービスにアクセスする可能性があります。

この脆弱性は、要求を処理する前に URL の正規化に失敗することに起因します。 攻撃者は、この問題を不正利用するために設計した巧妙に細工された URL を送信することで、この脆弱性を不正利用する可能性があります。 不正利用に成功すると、攻撃者は重要なサービスに非認証でアクセスし、DNA Center の権限を昇格させる場合があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180516-dna2

該当製品

脆弱性のある製品

この脆弱性は、Cisco DNA Center ソフトウェア リリース1.1.2 より前のリリースに影響します。

DNA Center ソフトウェア リリースの判別

システムで実行されている Cisco DNA Center は、管理者が Web ブラウザを使用して、HTTPS 経由で Cisco DNA Center にアクセスすることで確認できます。 [設定（Settings）] をクリックし、ドロップダウン メニューから [DNA Centerバージョン情報（About DNA Center）] を選択すると、リリースが表示されます。 [パッケージを表示（Show Packages）] をクリックし、[システムバージョン（System version）].を確認します。

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。

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 アップデートを提供しています。 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、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、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、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シスコのサービス契約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購入先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、Cisco DNA Center リリース 1.1.2 以降で修正されています。

Cisco DNA Center は、DNA Center ISO イメージがプリインストールされた状態でシスコから購入する専用物理アプライアンスです。 システムの更新は、Cisco Cloud からインストールすることができます。Cisco.com の Software Center からはダウンロードできません。 管理者がソフトウェアのシステム更新機能を使用することで、Cisco DNA Center の修正済みリリースにアップグレードできます。 詳細については、*Cisco Digital Network Architecture Center 管理者ガイド*、およびインストールするリリースのリリース ノート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やその公表を確認していません。

出典

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180516-dna2

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2018 年 5 月 16 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、単独の転載や意訳を施した場合、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。