

Cisco Nexus Dashboard の証明書の検証における脆弱性

High

アドバイザーID : cisco-sa-nd-tlsvid- [CVE-
TbAQLp3N](#) [2022-
20860](#)
初公開日 : 2022-07-20 16:00
バージョン 1.0 : Final
CVSSスコア : [7.4](#)
回避策 : No workarounds available
Cisco バグ ID : [CSCwa75442](#)

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 NexusダッシュボードのSSL/TLS実装における脆弱性により、認証されていないリモートの攻撃者が、関連するコントローラとの通信を変更したり、機密情報を表示したりできる可能性があります。

この脆弱性は、Cisco NexusダッシュボードがCisco Application Policy Infrastructure Controller(APIC)、Cisco Cloud APIC、またはCisco Nexus Dashboard Fabric Controller(旧Data Center Network Manager(DCNM)コントローラ)への接続を確立する際に、SSLサーバ証明書が検証されないことに起因しています。攻撃者は、該当デバイスとコントローラ間のトラフィックを中間者技術を使用して代行受信し、巧妙に細工されたされた証明書を使用使用してしてコントローラになりすますことで、こ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、攻撃者はデバイス間の通信を変更したり、これらのコントローラの管理者クレデンシャルなどの機密情報を表示したりできる可能性があります。

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。

このアドバイザーは、次のリンクより確認できます。

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nd-tlsvid-TbAQLp3N>

該当製品

脆弱性のある製品

この脆弱性は、Cisco Nexusダッシュボードに影響します。

注：リリース2.0(1d)より前のすべてのリリースでは、Cisco NexusダッシュボードはCisco Application Services Engineと呼ばれていました。

脆弱性が存在する Cisco ソフトウェアリリースについては、このアドバイザリの「[修正済みソフトウェア](#)」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

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。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャンネルからセキュリティ修正を取得する必要があります。

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。

Cisco.com の [Cisco Support and Downloads ページ](#)には、ライセンスとダウンロードに関する情報が記載されています。このページには、[マイデバイス (My Devices)] ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。

[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。

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

次の表では、左の列にシスコソフトウェアのリリースを記載しています。右側の列は、リリースがこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこの脆弱性に対する修正を含む最初のリリースを示しています。このセクションの表に記載されている適切な [修正済みソフトウェアリリースにアップグレードすることをお勧めします。](#)

Cisco Nexus Dashboard リリース	First Fixed Release (修正された最初のリリース)
1.1	修正済みリリースに移行。
2.0	修正済みリリースに移行。
2.1	修正済みリリースに移行。
2.2	2.2(1h)

Product Security Incident Response Team (PSIRT; プロダクト セキュリティ インシデント レスポンス チーム) は、このアドバイザリに記載されている該当するリリース情報と修正されたリリース情報のみを検証します。

不正利用事例と公式発表

Cisco PSIRT では、本アドバイザリに記載されている脆弱性の不正利用事例やその公表は確認しておりません。

出典

この脆弱性は、Cisco Advanced Security Initiatives Group (ASIG) の Logan Sanderson による内部セキュリティテストで発見されました。

URL

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nd-tlsvld-TbAQLp3N>

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	-	最終版	2022年7月20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。