

Cisco NexusダッシュボードファブリックコントローラのSSHホストキー検証の脆弱性



アドバイザリーID : cisco-sa-ndfc-shkv-

snQJtjrp

初公開日 : 2025-06-04 16:00

バージョン 1.0 : Final

CVSSスコア : [8.7](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwm50501](#)

[CVE-2025-20163](#)

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 Dashboard Fabric Controller(NDFC)のSSH実装の脆弱性により、認証されていないリモートの攻撃者がCisco NDFC管理対象デバイスになりすますことができるようになる可能性があります。

この脆弱性は、SSHホストキーの検証が不十分であることに起因します。攻撃者は、Cisco NDFC管理対象デバイスへのSSH接続に対してMachine-in-the-Middle攻撃を実行することにより、この脆弱性を不正利用する可能性があります。これにより、攻撃者がこのトラフィックを代行受信する可能性があります。エクスプロイトに成功すると、攻撃者は管理対象デバイスになりすましてユーザクレデンシャルを取得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-ndfc-shkv-snQJtjrp>

該当製品

脆弱性のある製品

この脆弱性は、デバイスの設定に関係なく、Cisco NDFC に影響を与えます。

注 : Cisco NDFCリリース11.5以前は、Cisco Data Center Network Manager(DCNM)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](#)にリストされている製品だけがこの脆弱性の影響を受けることが知られています。

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- Nexus Dashboard Insights
- Nexus Dashboard Orchestrator (NDO)

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 [シスコサポート & ダウンロードページ](#)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 (https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html) に連絡してアップグレードを入手してください。

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)
3.1	修正済みリリースに移行。
3.2	3.2(2f)

注 : Cisco Nexus Dashboard リリース 3.1(1k) 以降、Cisco NDFC は Cisco Nexus Dashboard の統合リリースで配布されます。Cisco Nexusダッシュボードリリース3.2(2f)には、この脆弱性に対する修正が含まれているCisco NDFCリリース12.2.3が含まれています。リリース12.2.3より前のすべてのCisco NDFCリリースは、この脆弱性の影響を受けるため、上の表に示すように、適切な修正済みCisco Nexusダッシュボードリリースに移行する必要があります。

注 : この脆弱性に対する修正は、新しいSSHホストキー検証機能です。この機能はデフォルトでは無効になっているため、現在の機能と下位互換性があります。詳細については、『[Cisco NDFCの概要と初期設定](#)』ドキュメントの「SSHホストキーの不一致」セクションを参照してください。Cisco Nexusダッシュボードの将来のリリースでは、この機能はデフォルトで有効になる予定であり、追加の設定が必要になる可能性があります。詳細については、リリース固有の設定ガイドを参照してください。

シスコの 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済み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REQON B.V.のHarm Blankers、Jasper Westerman、およびYanick de Paterに感謝いたします。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-shkv-snQJtjrp>

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	—	Final	2025年6月4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。