

Cisco NexusダッシュボードおよびNexusダッシュボードファブリックコントローラの不正なREST APIの脆弱性



アドバイザリーID : cisco-sa-nshs-urapi-

[CVE-2025-](#)

gJuBVFpu

[20348](#)

初公開日 : 2025-08-27 16:00

[CVE-2025-](#)

バージョン 1.0 : Final

[20347](#)

CVSSスコア : [5.4](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwp01069](#) [CSCwo82143](#)

[CSCwo82145](#)

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ダッシュボードおよびCisco Nexusダッシュボードファブリックコントローラ (NDFC)のREST APIエンドポイントにおける複数の脆弱性により、認証された権限の低いリモート攻撃者が、影響を受けるデバイスで機密情報を表示したり、ファイルをアップロードして変更したりする可能性があります。

これらの脆弱性は、一部のREST APIエンドポイントに認可コントロールがないために存在します。攻撃者は、巧妙に細工されたAPI要求を該当エンドポイントに送信することで、これら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、HTTPプロキシやNTP設定に関する機密情報へのアクセス、イメージのアップロード、該当デバイス上のイメージファイルの損傷など、限定された管理者機能を実行できる可能性があります。

注：これらの脆弱性は、REST APIエンドポイントのサブセットにのみ影響し、Webベースの管理インターフェイスには影響しません。

シスコはこれら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。これら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-nshs-urapi-gJuBVFpu>

該当製品

脆弱性のある製品

公開時点で、これらの脆弱性はデバイス設定に関係なく、Cisco NexusダッシュボードとCisco NDFCに影響を与えていました。

このアドバイザリの公開時点で脆弱性が存在するシスコ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。このアドバイザリの先頭にあるバグIDの詳細情報のセクションで、最新の情報を確認してください。

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、これらの脆弱性の影響を受けることが分かっています。

シスコは、これらの脆弱性が次のシスコ製品に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

これら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 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。

修正済みリリース

発行時点では、次の表に示すリリース情報は正確でした。このアドバイザリの先頭にあるバグIDの詳細情報のセクションで、最新の情報を確認してください。

Cisco Nexus Dashboard リリース	First Fixed Release (修正された最初のリリース)
3.2 以前	修正済みリリースに移行。
4.1	4.1(1g)

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 NDFCのこれらの脆弱性を解決するには、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します。

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とその公表は確認しておりません。

出典

この脆弱性は、シスコ内部でのシステム セキュリティ テストによって発見されました。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nshs-urapi-gJuBVFpu>

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8月27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。