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における不正なREST APIの脆弱性

Medium

アドバイザリーID : cisco-sa-ndhs-uaapi-Jh4V6zpN
初公開日 : 2024-10-02 16:00
バージョン 1.0 : Final
CVSSスコア : 6.3
回避策 : No workarounds available
Cisco バグ ID : CSCwj33029 CSCwj09986 CSCwk04220 CSCwk11265 CSCwk04255
CVE-2024-20441 CVE-2024-20442 CVE-2024-20477 CVE-2024-20438

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における複数の脆弱性により、認証された低特権のリモート攻撃者が、該当デバイスで限られたnetwork-admin機能を実行できる可能性があります。

これらの脆弱性の詳細については本アドバイザリの「詳細情報」セクションを参照してください。

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-ndhs-uaapi-Jh4V6zpN

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に影響を与えました。

注：Cisco Nexusダッシュボードリリース3.1(1k)以降では、Cisco NDFCはCisco Nexusダッシ

ユボードの統合リリースで配布されます。

公開時点で脆弱性が確認されている Cisco ソフトウェアの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。最新情報については、本アドバイザリ上部のバグIDの「詳細」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)

詳細

これらの脆弱性は依存関係にはなく、いずれかの脆弱性をエクスプロイトするために別の脆弱性をエクスプロイトする必要はありません。さらに、いずれかの脆弱性の影響を受けるソフトウェアリリースであっても、他の脆弱性の影響は受けない場合があります。

脆弱性の詳細は以下のとおりです。

CVE-2024-20438:Cisco NDFCの不正なREST APIエンドポイントの脆弱性

Cisco NDFCのREST APIエンドポイントの脆弱性により、認証された権限の低いリモート攻撃者が、該当デバイスでファイルの読み取りまたは書き込みを行う可能性があります。

この脆弱性は、一部のREST APIエンドポイントで認証制御が欠落していることが原因で発生します。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により、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、デバイス設定情報の読み取り、ファイルのアップロード、アップロードされたファイルの変更など、一部のnetwork-admin機能を実行できる可能性があります。

注：この脆弱性は、REST APIエンドポイントのサブセットのみに影響し、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。

バグID:CSCwj09986、CSCwj33029
CVE ID：CVE-2024-20438
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.3

CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L

CVE-2024-20441:Cisco NDFCの不正なREST APIエンドポイントの脆弱性

Cisco NDFCの特定のREST APIエンドポイントにおける脆弱性により、認証された低特権のリモート攻撃者が該当デバイスの機密情報を学習できる可能性があります。

この脆弱性は、影響を受けるREST APIエンドポイントの権限制御が不十分であることに起因します。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により、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、攻撃者は設定ファイルのみ、または完全なバックアップファイルをダウンロードし、機密の設定情報を取得できる可能性があります。この脆弱性は、特定のREST APIエンドポイントにのみ影響し、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。

バグID:CSCwk04220
CVE ID：CVE-2024-20441
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.7
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N

CVE-2024-20442:Cisco Nexusダッシュボードの不正なREST APIエンドポイントの脆弱性

Cisco NexusダッシュボードのREST APIエンドポイントにおける脆弱性により、認証された権限の低いリモート攻撃者が、該当デバイスで限定的な管理者アクションを実行できる可能性があります。

この脆弱性は、一部のREST APIエンドポイントで許可コントロールが不十分であることに起因します。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により、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、Web UIの一部の表示、設定のみまたは完全バックアップファイルの生成、テクニカルサポートファイルの削除など、一部の管理者機能を実行できる可能性があります。この脆弱性は、REST APIエンドポイントのサブセットのみに影響し、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。

バグID:CSCwk04255
CVE ID：CVE-2024-20442
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.4
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

CVE-2024-20477:Cisco NDFCの不正なREST APIエンドポイントの脆弱性

Cisco NDFCの特定のREST APIエンドポイントにおける脆弱性により、認証された低特権のリモート攻撃者が、該当デバイスにファイルをアップロードまたは削除できる可能性があります。

この脆弱性は、影響を受けるREST APIエンドポイントで認証制御が欠落していることが原因で存在します。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により、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、攻撃者は特定のコンテナにファイルをアップロードしたり、そのコンテナ内の特定のフォルダからファイルを削除したりできます。この脆弱性は、特定のREST APIエンドポイントにのみ影響し、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。

バグID:CSCwk11265
CVE ID：CVE-2024-20477
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：5.4
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L

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。

修正済みリリース

このドキュメントの発行時点では、次の表に示すリリース情報は正確でした。最新情報については、本アドバイザリ上部のバグIDの「詳細」セクションを参照してください。

左の列にはCiscoソフトウェアリリースが、右の列にはそのリリースが本アドバイザリに記載された脆弱性の影響を受けるかどうか、またどのリリースにこれらの脆弱性に対する修正が含まれているかを示します。

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

Cisco NDFC リリース	First Fixed Release（修正された最初のリリース）
11.5 以前	脆弱性なし
12.0	12.2.2

注：Cisco Nexusダッシュボードリリース3.1(1k)以降では、Cisco NDFCはCisco Nexusダッシュボード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(1e)には、Cisco NDFCリリース12.2.2が含まれています。

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とその公表は確認しておりません。

出典

これらの脆弱性は、Cisco Advanced Security Initiatives Group(ASIG)のMichael Blunt、Clayton Gilmer、およびRohan Raoによる社内セキュリティテストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndhs-uaapi-Jh4V6zpN

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	2024年10月2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。

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。