Cisco Nexusダッシュボード設定のバックアップにおけるREST APIの不正アクセスの脆弱性

Medium

アドバイザリーID : cisco-sa-nd-cbid-5YqkOSHu
初公開日 : 2026-04-01 16:00
バージョン 1.0 : Final
CVSSスコア : 6.5
回避策 : No workarounds available
Cisco バグ ID : CSCwq66302

CVE-2026-20042

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ダッシュボードの設定バックアップ機能の脆弱性により、暗号化パスワードを持ち、完全または設定専用バックアップファイルにアクセスできる攻撃者が、機密情報にアクセスできる可能性があります。

この脆弱性は、暗号化されたバックアップファイルに認証の詳細が含まれているために存在します。影響を受けるデバイスの有効なバックアップファイルと暗号化パスワードを持つ攻撃者によって、バックアップファイルが復号化される可能性があります。攻撃者は、バックアップファイルの認証の詳細を使用して、該当デバイスの内部のみのAPIにアクセス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rootユーザとして基盤となるオペレーティングシステムで任意のコマンドを実行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-nd-cbid-5YqkOSHu

該当製品

脆弱性のある製品

公開時点で、この脆弱性は、デバイス設定に関係なく、Cisco Nexusダッシュボードの脆弱性のあるリリースを実行しているシスコデバイスに影響を与えました。

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スタンドアロン製品には影響を与えないことを確認しました。

- Nexus Dashboard Fabric Controller（NDFC）
- Nexus Dashboard Insights
- Nexus Dashboard Orchestrator（NDO）

注：Cisco Nexus Dashboardバージョン3.1(1k)以降では、Unified Nexus Dashboardソフトウェアイメージに上記のリストの製品が含まれています。統合イメージの一部として、これらの製品は影響を受け、Cisco Nexusダッシュボードの修正済みリリースで修正されています。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。

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

シスコでは、回避策や緩和策（該当する場合）は、修正済みソフトウェアリリースへのアップグレードが利用可能になるまでの一時的な解決策であると考えています。この脆弱性を完全に修正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載されている修正済みソフトウェアにアップグレードすることを強く推奨します。

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。

左側の列にはシスコソフトウェアリリース、右側の列に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リリースが示されています。

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

Cisco Nexus Dashboard リリース	First Fixed Release（修正された最初のリリース）
4.2	脆弱性なし

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おりません。

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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nd-cbid-5YqkOSHu

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	2026年4月1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。