

Cisco NexusダッシュボードのLDAPユーザ名列挙の脆弱性



アドバイザリーID : cisco-sa-nd-unenum-2xFFh472 [CVE-2025-20150](#)

初公開日 : 2025-04-16 16:00

バージョン 1.0 : Final

CVSSスコア : [5.3](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwk04469](#)

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ダッシュボードの脆弱性により、認証されていないリモート攻撃者がLDAPユーザアカウントを列挙できる可能性があります。

この脆弱性は、LDAP認証要求の不適切な処理に起因します。攻撃者は、該当システムに認証要求を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、攻撃者はどのユーザ名が有効なLDAPユーザアカウントであるかを特定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-nd-unenum-2xFFh472>

該当製品

脆弱性のある製品

公開時点で、LDAPがリモート認証プロバイダーとして設定されている場合、この脆弱性はCisco Nexusダッシュボードに影響を与えました。

このアドバイザリー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、このアドバイザリーの「[修正済みソフトウェア](#)」セクションを参照してください。このアドバイザリーの先頭にあるバグ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。

LDAPがリモート認証プロバイダーとして設定されているかどうかを確認する

LDAPがリモート認証プロバイダーとして設定されているかどうかを確認するには、次の手順を実行します。

1. Nexusダッシュボードの管理コンソールに移動します。
2. メインナビゲーションメニューから、Admin > Authenticationの順に選択します。
3. 設定済みのログインドメインについて、Realm 列を確認して、LDAPが設定されているかどうか、およびProviders 列にゼロ以外の数値が含まれているかどうかを確認します。

ログインドメインのRealm列にLDAPが設定されており、Providers列にゼロ以外の数値が設定されている場合、そのソフトウェアはこの脆弱性の影響を受けます。

注：この脆弱性の影響を受けるのは、LDAP認証のみです。他のすべての認証方式は、この脆弱性の影響を受けません。

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。

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

[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。

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)
3.1 以前	修正済みリリースに移行。
3.2	3.2(2f)

注：Cisco Nexus Dashboard Release 3.1(1k)以降、Cisco Nexus Dashboard Fabric Controller(NDFC)、Cisco Nexus Dashboard Insights(NDI)、およびCisco Nexus Dashboard Orchestrator(NDO)は、Cisco Nexus Dashboard Unifiedリリースで配布されます。

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-unenum-2xFFh472>

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4月16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。