Cisco Nexus Dashboard Hosted Servicesの情報開示の脆弱性

Medium

アドバイザリーID : cisco-sa-ndhs-idv-Bk8VqEDc
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 : CSCwk96544 CSCwk96526 CSCwm28892

CVE-2024-20490
CVE-2024-20491

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)、Cisco Nexus Dashboard Insights、およびCisco Nexus Dashboard Orchestrator(NDO)のロギング機能における複数の脆弱性により、攻撃者がテクニカルサポートファイルにアクセスして機密情報を表示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-idv-Bk8VqEDc

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 NDFC、Cisco Nexus Dashboard Insights、およびCisco NDOに影響を与えました。

注：Cisco Nexus Dashboard Release 3.1(1k)以降、Cisco NDFC、Cisco Nexus Dashboard Insights、およびCisco NDOは、Cisco Nexus Dashboard Unified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。

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-2024-20490:Cisco NDFCおよびCisco NDOの情報漏洩の脆弱性

Cisco Nexus Dashboard Fabric Controller(NDFC)およびCisco Nexus Dashboard Orchestrator(NDO)のロギング機能の脆弱性により、テクニカルサポートファイルへのアクセス権を持つ攻撃者が機密情報を閲覧する可能性があります。

この脆弱性は、HTTPプロキシクレデンシャルがテクニカルサポートファイルに保存されている内部ログに記録される可能性があるために存在します。攻撃者は、該当システムから生成されたテクニカルサポートファイルにアクセスすることで、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、Nexusダッシュボードで設定されたHTTPプロキシサーバの管理者クレデンシャルをクリアテキストで表示して外部ネットワークに到達できるようになります。

注：デバッグログとテクニカルサポートファイルは機密情報が含まれている可能性があるため、安全に保存し、信頼できる関係者とのみ共有することを推奨します。

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。

バグID:CSCwk96526、CSCwm28892
CVE ID：CVE-2024-20490
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.3
CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N

CVE-2024-20491:Cisco Nexus Dashboard Insightsの情報開示における脆弱性

Cisco Nexus Dashboard Insightsのロギング機能の脆弱性により、テクニカルサポートファイルへ

のアクセス権を持つ攻撃者が機密情報を表示できる可能性があります。

この脆弱性は、リモートコントローラのクレデンシャルがtech supportファイルに保存されている内部ログに記録されることに起因します。攻撃者は、該当システムから生成されたテクニカルサポートファイルにアクセスすることで、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、リモートコントローラの管理者クレデンシャルをクリアテキストで表示できる可能性があります。

注：デバッグログとテクニカルサポートファイルは機密情報が含まれている可能性があるため、安全に保存し、信頼できる関係者とのみ共有することを推奨します。

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。

バグID:CSCwk96544
CVE ID：CVE-2024-20491
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.3
CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N

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 NDFCリリース(CVE-2024-20490)	First Fixed Release（修正された最初のリリース）
12.0 以前	脆弱性なし
12.1	修正済みリリースに移行。
12.2	12.2.2.241

Cisco Nexus Dashboard Insightsリリース(CVE-2024-20491)	First Fixed Release（修正された最初のリリース）
6.3 以前	修正済みリリースに移行。
6.4	脆弱性なし
6.5	6.5.1.32

Cisco NDOリリース(CVE-2024-20490)	First Fixed Release（修正された最初のリリース）
4.1 以前	修正済みリリースに移行。
4.2	4.2(3o)
4.3	修正済みリリースに移行。
4.4	4.4.1.1012

注：Cisco Nexus Dashboard Release 3.1(1k)以降、Cisco Cisco NDFC、Cisco Nexus Dashboard Insights、およびCisco NDOは、Cisco Nexus Dashboard Unified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(1i)には、Cisco NDFCリリース12.2.2.241、Cisco Nexus Dashboard Insightsリリース6.5.1.32、およびCisco NDOリリース4.4.1.1012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-ndhs-idv-

Bk8VqEDc

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

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。