

Cisco NX-OSソフトウェアのセキュリティ強化 リリース：2026年10月



Advisory ID : cisco-sa-hardening-nxosw1-[CVE-2026-76457](#)
cWzSbtR
初公開日 : 2026-10-07 16:00
バージョン 1.0 : Final
CVSSスコア : [9.8](#)
回避策 : No workarounds available
Cisco Bug ID : [CVE-2026-76453](#)
[CVE-2026-76459](#)
[CVE-2026-76458](#)

日本語の情報は原文の英語の非公式な翻訳です。日本語と英語のバージョンに相違がある場合は、英語のバージョンが優先されます。

概要

予防的なセキュリティと製品の品質に対するシスコの継続的な取り組みの一環として、Cisco NX-OSソフトウェアエンジニアリングチームは、包括的な社内セキュリティレビューを実施しました。このレビューの結果、社内で見つめられた複数の脆弱性に対処するソフトウェアのセキュリティ強化リリースが公開されました。

これらの脆弱性は内部テストで見つめられたものであり、現時点でエクスプロイトの事例は確認されていません。お客様によるパッチ適用を支援し、開示プロセスを効率化するために、シスコはこれらの問題をその根本的な脆弱性クラス (Common Weakness Enumeration (CWE)) ごとに分類し、1 つの共通脆弱性識別子 (CVE ID) を割り当てました。

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-hardening-nxosw1-cWzSbtR>

該当製品

脆弱性のある製品

これらの脆弱性は、デバイス設定に関係なく、Cisco NX-OSソフトウェアの脆弱性のあるリリースを実行する次のシスコ製品に影響を与えます。

- MDS 9000 シリーズ マルチレイヤ スイッチ
- Nexus 3000 シリーズ スイッチ
- Nexus 7000 シリーズ スイッチ
- ACIモードのNexus 9000シリーズファブリックスイッチ
- スタンドアロン NX-OS モードの Nexus 9000 シリーズ スイッチ
- UCS 6300 シリーズ ファブリック インターコネクト
- UCS 6400 シリーズ ファブリック インターコネクト
- UCS 6500 シリーズ ファブリック インターコネクト
- UCS 6600 シリーズ ファブリック インターコネクト
- UCS Xシリーズ ダイレクト ファブリック インターコネクト 9108 100G

脆弱性が存在する Cisco 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。

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

次の表に、これらのソフトウェア強化リリースで対処されている脆弱性クラスの概要を示します。各 CVE ID に割り当てられる CVSS スコアは、その特定の CWE カテゴリ内で最も影響の大きい 1 つの根本的な脆弱性がもたらす可能性がある最大のシビラティ（重大度）を表しています。

CVE ID	CVSS最高スコア	脆弱性クラス (最高レベルの CWE)	説明
CVE-2026-76453	8.8	CWE-707	不適切な無害化 (コマンド、OS、引数の挿入を含む)
CVE-2026-76455	9.8	CWE-284	不適切なアクセス制御 (承認、認証、権限、およびバイパスなど)
CVE-2026-76456	8.6	CWE-20	不適切な入力検証 (入力検証、パストラバーサル、外部パス制御など)
CVE-2026-76457	8.6	CWE-125	範囲外の読み取り (バッファオーバー読み取りと機密情報の公開をカバーします)
CVE-2026-76458	8.6	CWE-703	例外条件の不適切な処理 (不明な例外、到

CVE ID	CVSS最高スコア	脆弱性クラス (最高レベルのCWE)	説明
			達可能なアサーションを含む)
CVE-2026-76459	9.8	CWE-787	範囲外の書き込み (スタックベースのバッファオーバーフロー、ヒープベースのバッファオーバーフロー、従来のバッファオーバーフロー、および不正なバッファサイズの計算を対象とします)

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

これらの脆弱性を修正し、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。

修正リリース

次の表では、左の列にシスコソフトウェアリリースを示します。右の列は、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、およびこれらの脆弱性に対する修正を含む最初のリリースを示しています。このセクションの表に記載されている適切な修正済みソフトウェアリリースにアップグレードすることをお勧めします。

MDS 9000 シリーズ マルチレイヤ スイッチ

Cisco NX-OS ソフトウェアリリース	第 1 修正済みリリース
9.3 以前	修正済みリリースに移行。
9.4	9.4(5a)

スタンドアロンNX-OSモードのNexus 3000シリーズスイッチおよびNexus 9000シリーズスイッチ

Cisco NX-OS ソフトウェアリリース	第 1 修正済みリリース
10.3 以前	10.3(10)
10.4	10.4(8)
10.5	10.5(6)
10.6	10.6(4)

Nexus 7000 シリーズ スイッチ

Cisco NX-OS ソフトウェアリリース	第 1 修正済みリリース
8.3 以前	修正済みリリースに移行。
8.4	8.4(14)

ACIモードのNexus 9000シリーズファブリックスイッチ

Cisco NX-OS ソフトウェアリリース	第 1 修正済みリリース
16.0 以前	16.0(9h)
16.1	16.1(6g)
16.2	16.2(3g)

UCS 6300、6400、6500、6600シリーズおよび9108 100 Gファブリックインターコネクト

Cisco UCS ソフトウェアリリース	UCS Managerマネージドモードの最初の修正済みリリース	UCS Intersightマネージドモードの最初の修正済みリリース
4.2 以前	修正済みリリースに移行。	修正済みリリースに移行。
4.3	4.3(6j)	4.3(6.260049) 4.3(6.260059)
6.0	6.0(2e)	6.0(2.260080)

注：リリース4.3(6.260059)は、Cisco 9108 100Gファブリックインターコネクト専用です。

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。

送信元

これらの脆弱性は、既存のテストプロセスおよびフロンティアの AI モデルを使用した内部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->

改訂履歴

バージョン	説明	セクション	Status	日付
1.0	初版リリース	—	Final	2026年10月7日

利用規約

ソフトウェアのダウンロードおよびテクニカルサポート

Cisco.com の [シスコサポート & ダウンロード](#) ページには、ライセンスとダウンロードに関する情報が記載されています。このページには、マイデバイス (My Devices) ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。お客様がソフトウェアをダウンロードできるのは、シスコから直接、あるいはシスコ認定再販業者やシスコ認定パートナーを通じて調達されたもので、ライセンスが有効なものに限ります。

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、[Cisco Technical Assistance Center \(TAC \)](#) に連絡してアップグレードを入手してください。無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

[ソフトウェアのアップグレードを検討する](#) 際には、関連するシスコ製品の[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。

利用規約の詳細

シスコは、商品適格性または特定目的への適合性に関する保証を含め、明示的か黙示的かを問わず、いかなる種類の保証も表明しません。前述の一般論に限定されることなく、シスコは、本情報の正確性または完全性を保証するものではありません。コンテンツは「現状のまま」提供されます。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。

本セキュリティアドバイザリに含まれる情報のコピーや要約には、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。本セキュリティアドバイザリの最新版については、[シスコ セキュリティ アドバイザリ](#) ページをご覧ください。Cisco 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評価します。詳細については、[シスコのセキュリティ脆弱性ポリシー](#)を参照してください。

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。