

Cisco Nexus 3000および9000シリーズスイッチのMPLS OAMにおけるリモートコード実行の脆弱性



Advisory ID : cisco-sa-moam-rce-uBTzYV7 [CVE-2026-](#)

初公開日 : 2026-10-07 16:00

[76465](#)

バージョン 1.0 : Final

CVSSスコア : [9.8](#)

回避策 : No workarounds available

Cisco Bug ID : [CSCwu19799](#)

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

Cisco Nexus 3000シリーズスイッチおよびCisco Nexus 9000シリーズスイッチ用Cisco NX-OSソフトウェアのMPLS Operation, Administration, and Maintenance(OAM)機能の脆弱性により、認証されていないリモートの攻撃者がroot権限で任意のコードを実行したり、該当デバイスにサービス妨害(DoS)状態を引き起こしたりする可能性があります。

この脆弱性は、該当デバイスがMPLSエコー要求パケットを処理する際の検証が不適切なことに起因します。攻撃者は、該当デバイスのIPアドレスに巧妙に細工されたMPLSエコー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root権限で任意のコードを実行し、プロセスのクラッシュを引き起こす可能性があります。その結果、デバイスがリロードされ、DoS状態が発生する可能性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。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-moam-rce-uBTzYV7>

本アドバイザリは一連のアドバイザリの一部です。これらのアドバイザリとリンクの一覧については、[2026年10月7日発行のCisco Advance Notification, Security Advisories](#)を参照してください。Cisco NX-OSソフトウェアの改善点と修正プログラムの詳細については、『[Cisco NX-OSソフトウェアセキュリティ強化リリース：2026年10月](#)』を参照してください。

該当製品

脆弱性がある製品

この脆弱性の影響を受けるのは、次のシスコ製品で Cisco NX-OS ソフトウェアの脆弱性が存在するリリースを実行しており、かつ MPLS OAM 機能が有効になっている場合です。

- Nexus 3000 シリーズ 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

注：Silicon One ASICを搭載したCisco Nexus 9000シリーズスイッチは、MPLS OAM機能をサポートしていないため（有効化できません）、この脆弱性の影響を受けません。

Cisco Nexus 3000および9000シリーズスイッチでは、MPLS OAM機能はデフォルトで無効になっています。

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。

MPLS OAMのステータスの判別

Cisco Nexus 3000または9000シリーズスイッチでMPLS OAM機能が有効に設定されているかどうかを確認するには、Cisco NX-OSのCLIでshow feature | include mpls_oamコマンドを使用します。次の例は、MPLS OAM機能が有効になっているスイッチの出力を示しています。

```
switch# show feature | include mpls_oam
mpls_oam                1                enabled
```

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[脆弱性が存在する製品](#)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シスコ製品には影響を与えないことを確認しました。

- FirePOWER 1000 シリーズ
- Firepower 2100 シリーズ
- FirePOWER 4100 シリーズ
- Firepower 9300セキュリティアプライアンス
- MDS 9000 シリーズ マルチレイヤ 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

- Cisco Secure Firewall 200 シリーズ
- Cisco Secure Firewall 1200 シリーズ
- Cisco Secure Firewall 3100 シリーズ
- Cisco Secure Firewall 4200 シリーズ
- Cisco Secure Firewall 6100 シリーズ
- 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

詳細

MPLS OAM機能は、MPLS pingおよびMPLS tracerouteを使用したMPLSネットワーク内のデータプレーン障害の特定に使用できる診断機能を提供します。詳細については、『[Cisco Nexus 9000シリーズNX-OSラベルスイッチングコンフィギュレーションガイド、リリース10.3\(x\)](#)』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。

MPLS OAM機能が不要な場合は、この機能を無効にすることで攻撃ベクトルが排除されるため、この脆弱性を緩和できます。MPLS OAM機能を無効にするには、Cisco Nexus 3000または9000シリーズスイッチで、グローバルコンフィギュレーションモードでCisco NX-OS CLIコマンドno feature mpls oamを使用します。

この緩和策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

Live Protect シールド

シスコは、Cisco NX-OSソフトウェアのこの脆弱性を一時的に緩和するために、CVE-2026-76465用の[Live Protectシールド](#)をリリースしました。

Cisco NX-OS ソフトウェア用の Live Protect の詳細については、『[Cisco Nexus 9000 Series NX-OS Security Configuration Guide](#)』を参照してください。

注：Live Protect シールドは、ソフトウェアの更新が予定されるまでの間、そのギャップを埋めるための一時的な緩和策です。この脆弱性を修正するには、このアドバイザリの「[修正済みソフトウェア](#)」セクションに記載されている修正済みソフトウェアリリースにアップグレードします。

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。

Cisco NX-OS ソフトウェア

お客様が Cisco NX-OS ソフトウェアの脆弱性による侵害の可能性を判断できるように、シスコは [Cisco Software Checker](#) を提供しています。このツールを使うことで、特定のソフトウェアリリースに関連するすべてのシスコ セキュリティ アドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース（「First Fixed」）を特定できます。また、該当する場合には、Software Checker により判別されたすべてのアドバイザリに記載のすべての脆弱性が修正された最初のリリース（「Combined First Fixed」）を特定できます。

このツールを使用するには、「[Cisco Software Checker](#)」ページの手順に従います。または、次のフォームを使用して、特定のソフトウェアリリースに影響を及ぼす脆弱性を検索します。このフォームを使用するには、次の手順に従います。

1. ツールで検索するアドバイザリを選択します。このアドバイザリのみ、[セキュリティ影響評価 \(SIR\)](#) が「重大」または「高」のアドバイザリのみ、すべてのアドバイザリのいずれかです。
2. 該当するソフトウェアを選択します。
3. 該当するプラットフォームを選択します。
4. リリース番号を入力します。たとえば、Cisco Nexus 3000 シリーズ スイッチの場合は 10.4(4)、ACI モードの Cisco NX-OS ソフトウェアの場合は 16.0(8e) です。
5. [チェック (Check)] をクリックします。

2		Critical,High,Medium
このアドバイザのみ		Cisco NX-OS ソフトウェア
あらゆるプラットフォーム		
Enter release number	Check	

不正利用事例と公式発表

Cisco Product Security Incident Response Team (PSIRT) 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を確認していません。

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-moam-rce-uBTzYV7>

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。