

ACIモードのCisco Nexus 9000シリーズファブリックスイッチにおけるエンドポイントグループコントラクトバイパスの脆弱性



Advisory ID : cisco-sa-aci-epgcbp-SfDU7NLf

[CVE-2026-20038](#)

初公開日 : 2026-10-07 16:00

バージョン 1.0 : Final

CVSSスコア : [5.8](#)

回避策 : No workarounds available

Cisco Bug ID : [CSCwr18270](#)

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

ACIモードのCisco Nexus 9000シリーズファブリックスイッチのエンドポイントグループ(EPG)コントラクト機能における脆弱性により、認証されていないリモートの攻撃者がEPGコントラクトをバイパスできる可能性があります。

この脆弱性は、EPG契約の不適切な制御に起因します。攻撃者は、該当デバイスを介してDHCPトラフィックに割り当てられたUDP送信元ポートと宛先ポートを使用してIPv4またはIPv6パケット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、攻撃者は該当デバイスでEPGコントラクトをバイパスでき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-aci-epgcbp-SfDU7NLf>

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。また、Cisco NX-OSソフトウェアの改善と修正についてのその他のドキュメントについては、『[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

脆弱性のある製品

公開時点では、デバイスの設定にかかわらず、この脆弱性はACIモードのCisco Nexus 9000シリーズファブリックスイッチに影響を与えていました。

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、この脆弱性の影響を受けることが分かっています。

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 3000 シリーズ スイッチ
- Nexus 7000 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
- 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

ACIモードでのCisco Nexus 9000シリーズファブリックスイッチのソフトウェアのデフォルト設定では、スイッチの初期化中にDHCPv4およびDHCPv6トラフィックの暗黙的なルールがプログラムされます。これらのルールは常にDHCP関連のトラフィックを許可し、ユーザ定義のコントラクトルールよりも高い優先順位を持ちます。その結果、このトラフィックに対して設定されたコントラクトまたは一般的な暗黙の拒否は適用されません。DHCPの暗黙的な許可ルールが常に

優先されます。

この脆弱性に対する修正は設定ノブであり、管理者がCisco APIC REST APIを介してDHCP暗黙ルールを無効(unprogram)にしたり、再有効にしたりできます。暗黙的なルールが無効の場合、DHCPトラフィックに対するユーザ定義のコントラクトpermit、deny、およびredirectアクションが許可されます。ACIモードのCisco Nexus 9000シリーズファブリックスイッチのソフトウェアのデフォルトの動作では、暗黙のルールが有効になっています。

この新しい設定ノブの詳細については、『[Cisco APIC基本設定ガイド、リリース6.2\(x\)](#)』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。

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。

修正リリース

この脆弱性を修正するには、次のすべての手順を実行する必要があります。

- Cisco APICをリリース6.0(9h)、リリース6.1(6g)、リリース6.2(3g)以降にアップグレードします。
- ACIモードのCisco Nexus 9000シリーズファブリックスイッチを、リリース16.0(9h)、リリース16.1(6g)、リリース16.2(3g)以降にアップグレードします。
- このアドバイザリの「[詳細](#)」セクションで説明されている設定ノブを適用します。詳細については、『[Cisco APIC基本設定ガイド、リリース6.2\(x\)](#)』を参照してください。

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。

送信元

この脆弱性を報告していただいたCANCOM Austria AGのSystem Integration Network SolutionsのWilhelm Putz氏に感謝いたします。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-epgcbp-SfDU7NLf>

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。

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。