Cisco Nexus 3000および9000シリーズスイッチのProtocol Independent Multicastバージョン6におけるDoS脆弱性

Medium

アドバイザリーID : cisco-sa-nxospc-pim6-vG4jFPh
CVE-2025-20262
初公開日 : 2025-08-27 16:00
バージョン 1.0 : Final
CVSSスコア : 5.0
回避策 : No workarounds available
Cisco バグ ID : CSCwn69044

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

スタンドアロンNX-OSモードのCisco Nexus 3000シリーズスイッチおよびCisco Nexus 9000シリーズスイッチのProtocol Independent Multicast Version 6(PIM6)機能の脆弱性により、認証された低特権のリモート攻撃者がPIM6プロセスのクラッシュを引き起こし、その結果サービス妨害(DoS)状態が発生する可能性があります。

この脆弱性は、PIM6一時データクエリの不適切な処理に起因します。攻撃者は、NX-API REST、NETCONF、RESTConf、gRPC、またはモデル駆動型テレメトリのいずれかの方法を介して、巧妙に細工された一時的なクエリを該当デバイスに送信することで、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者はPIM6プロセスをクラッシュさせて再起動させ、潜在的な隣接関係のフラップを引き起こし、PIM6および一時的なクエリープロセスのDoSを引き起こす可能性があります。

一時的なクエリの例については、『Cisco Nexus 9000 Series NX-OS Programmability Guide, Release 9.3(x)』の「gRPCの一時的なデータについて」セクションを参照してください。

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-nxospc-pim6-vG4jFPh

このアドバイザリは、2025年8月に公開されたCisco FXOSおよびNX-OSソフトウェアセキュリテ

ィアドバイザリバンドルの一部です。これらのアドバイザリとリンクの一覧については、『シスコイベントレスポンス：Cisco FXOSおよびNX-OSソフトウェアに関するセキュリティアドバイザリ公開資料（半年刊、2025年8月）』を参照してください。

該当製品

脆弱性のある製品

この脆弱性の公開時点では、スタンドアロンNX-OSモードでPIM6機能が有効で、次の機能の少なくとも1つが有効になっているCisco Nexus 3000シリーズスイッチおよびCisco Nexus 9000シリーズスイッチに影響が及びました。

- NX-API
- NETCONFの
- RESTCONF（再起動）
- gRPC
- モデル駆動型テレメトリ

注：Protocol Independent Multicast(PIM)バージョン4(PIM4)機能は影響を受けません。

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。

PIM6機能が有効になっているかどうかの確認

PIM6機能が有効になっているかどうかを確認するには、次の例に示すようにshow feature | include pim6 CLIコマンドを使用します。

<#root>

```
Switch#
show feature | include pim6

pim6                  1          enabled
```

セカンダリ機能が有効になっているかどうかの確認

この脆弱性の影響を受けるには、スイッチでPIM6が有効になっていて、上記の機能の少なくとも1つが有効になっている必要があります。リストされた機能のいずれかが有効になっているかどうかを確認するには、show feature | include featurenameコマンドを使用して、featurenameを次のように置き換えます。

- nxapi
- NetConf
- restconf
- grpc
- テレメトリ

これらの機能はすべてデフォルトで無効になっています。

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。

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
- VMware vSphere 向け Nexus 1000 Virtual Edge
- Nexus 5500 プラットフォーム スイッチ
- Nexus 5600 プラットフォーム スイッチ
- Nexus 6000 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
- Cisco Secure Firewall 3100 シリーズ
- Cisco Secure Firewall 4200 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 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

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。

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)などです。
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	

関連情報

Cisco Nexus スイッチに最適な Cisco NX-OS ソフトウェアリリースの決定に際してサポートが必要な場合は、以下の推奨リリースに関するドキュメントを参照してください。セキュリティ アドバイザリでより新しいリリースが推奨されている場合は、そのアドバイザリのガイダンスに従うことをお勧めします。

Cisco MDS シリーズ スイッチ

Cisco Nexus 3000 Series Switches
Cisco Nexus 5500 プラットフォーム スイッチ
Cisco Nexus 5600 プラットフォームスイッチ
Cisco Nexus 6000 Series Switches
Cisco Nexus 7000 Series Switches
Cisco Nexus 9000 Series Switches
ACI モードの Cisco Nexus 9000 シリーズ スイッチ

Cisco UCS ソフトウェアに最適なリリースを確認するには、デバイスのリリースノートに記載されている推奨リリースに関するドキュメントを参照してください。

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-nxospc-pim6-vG4jFPh

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8月27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。