Cisco Nexus 9000シリーズスイッチのSilicon Oneにおけるリモートコード実行の脆弱性

アドバイザリーID : cisco-sa-n9k-s1-rce-EH8dEtr
初公開日 : 2026-09-02 16:00
バージョン 1.0 : Final
CVSSスコア : 9.8
回避策 : Yes
Cisco バグ ID : CSCwu32817

CVE-2026-20212

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 9000シリーズスイッチのSilicon One統合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、root権限でコードを実行する可能性があります。

この脆弱性は、デフォルトのレイヤ3(L3)Virtual Routing and Forwarding(VRF)でTCPポート43210および43211がアクセス可能であることに起因しています。 エクスプロイトに成功すると、攻撃者は該当デバイスに接続し、巧妙に細工された入力を送信できます。この入力は、root権限でコードとして実行される可能性があります。この脆弱性が不正利用されると、S1HALプロセスがクラッシュし、デバイスがリロードされる可能性があります。

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。本脆弱性に対処する回避策がいくつかあります。

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-n9k-s1-rce-EH8dEtr

該当製品

脆弱性のある製品

Cisco Nexus 9000シリーズスイッチにSilicon One ASICが搭載されている場合、この脆弱性の影響を受けます。

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。

公表時点では、次の製品識別子(PID)を持つCisco Nexus 9000シリーズスイッチにはSilicon One ASICが含まれています。

- N9324C-SE1U
- N9348Y2C6D-SE1U
- N9364E-SG2-O
- N9364E-SG2-Q
- N9396T12C-SE1
- N9348Y12C-SE1
- N9396Y12C-SE1
- N9336C-SE1
- N9K-C9804
- N9K-C9808

デバイスのPIDを確認するには、show module CLIコマンドを使用します。次の例では、デバイスのPIDはN9336C-SE1で、これは、この脆弱性の影響を受けるデバイスのリストにあります。

```
<#root>

switch#

show module

Mod Ports                  Module-Type                              Model           Status
--- ----- ---------------------------------------------- --------------------- --------
1    36   36x40/100G QSFP28 Ethernet Module

N9336C-SE1

            ok
```

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

- Nexus 3000 シリーズ スイッチ
- Nexus 7000 シリーズ スイッチ
- 「脆弱性のある製品」セクションに一覧されているモデル以外のNexus 9000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

回避策

この脆弱性に対処する回避策はありません。

この脆弱性のリモートからの不正利用を防ぐには、インフラストラクチャアクセスコントロールリスト(iACL)を使用して、該当デバイス宛ての必要な管理およびコントロールプレーントラフィックのみを許可します。または、iACLを使用して、宛先ポートが43210または43211のローカルに設定されたIPアドレスを宛先とするすべてのTCPパケットを明示的に拒否することもできます。

iACLの詳細については、『Cisco NX-OSソフトウェア強化ガイド』を参照してください。

この回避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。

保護シールドのライブ

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-2026-20212用のLive Protectシールドをリリースしました。

Cisco NX-OSソフトウェアのLive Protect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、ソフトウェアのアップデートをスケジュールできるようになるまでの間、このギャップを埋めるための一時的な緩和策です。この脆弱性を完全に修正するには、

Cisco Software Checkerを使用して、修正済みの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て、このアドバイザリで説明されている障害の発生を防ぐために、お客様はこのアドバイザリで説明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お勧めします。

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	

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 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

この脆弱性は Cisco Cisco Technical Assistance Center（TAC）サポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-n9k-s1-rce-EH8dEtr

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	2026年9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。