Cisco Nexus 3000 および 9000 シリーズ スイッチのヘルスモニタリング診断におけるサービス妨害（DoS）の脆弱性

High

アドバイザリーID : cisco-sa-n3kn9k-healthdos-eOqSWK4g
初公開日 : 2025-02-26 16:00
バージョン 1.0 : Final
CVSSスコア : 7.4
回避策 : Yes
Cisco バグ ID : CSCwk41797 CSCwj98161

CVE-2025-20111

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 スイッチのヘルスモニタリング診断における脆弱性により、認証されていない隣接する攻撃者が、デバイスの予期しないリロードを引き起こし、サービス妨害（DoS）状態を発生させる可能性があります。

この脆弱性は、特定のイーサネットフレームが適切に処理されないことに起因します。攻撃者が、該当するデバイスに細工されたイーサネットフレームを一定の速度で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、攻撃者は標的デバイスのリロードを引き起こすことができるようになります。

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-n3kn9k-healthdos-eOqSWK4g

このアドバイザリは、2025 年 2 月に公開された Cisco FXOS および NX-OS ソフトウェアのセキュリティ アドバイザリ バンドルの一部です。アドバイザリとリンクの一覧については、『Cisco Event Response: February 2025 Semiannual Cisco FXOS and NX-OS Software Security Advisory Bundled Publication』を参照してください。

該当製品

脆弱性のある製品

この脆弱性は、デバイスの設定に関係なく、脆弱性のある Cisco NX-OS ソフトウェアリリースを実行している次のシスコ製品に影響を与えます。

- Nexus 3100 シリーズ スイッチ
- Nexus 3200 シリーズ スイッチ
- Nexus 3400 シリーズ スイッチ
- Nexus 3600 シリーズ スイッチ
- スタンドアロン NX-OS モードの Nexus 9200 シリーズ スイッチ
- スタンドアロン NX-OS モードの Nexus 9300 シリーズ スイッチ
- スタンドアロン NX-OS モードの Nexus 9400 シリーズ スイッチ

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
- 「脆弱性のある製品」セクションに示されているモデル以外の Nexus 3000 シリーズ スイッチ
- 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
- 「脆弱性のある製品」セクションに示されているモデル以外のスタンドアロン NX-OS モードの 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 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

セキュリティ侵害の痕跡

『Cisco Security Indicators of Compromise Reference Guide』にはよく見られる IoC が記載されており、このシスコ セキュリティ アドバイザリで公開されている脆弱性の影響を受ける可能性のあるデバイスを特定するのに役立ちます。

この脆弱性の不正利用に成功すると、L2ACLRedirect ヘルスモニタリング診断テスト、特に Nexus 3100 および 3200 シリーズ スイッチでは、RewriteEngineLoopback ヘルスモニタリング診断テストが連続して失敗する可能性があります。テストが 10 回連続して失敗すると、次の syslog メッセージのいずれかがシステムログファイルに記録されます。

<#root>

```
SWITCH %$ VDC-1 %$ %DIAG_PORT_LB-2-L2ACLREDIRECT_LOOPBACK_TEST_FAIL: Module:1 Test:
```

L2ACLRedirect

```
Loopback failed 10 consecutive times. Faulty module: affected ports:1  Error:Loopback test failed. Pack
```

```
SWITCH %$ VDC-1 %$ %DIAG_PORT_LB-2-REWRITE_ENGINE_LOOPBACK_TEST_FAIL: Module:1 Test:
```

RewriteEngine

```
 Loopback failed 10 consecutive times. Faulty module:  Error:Loopback test failed. Packets lost on the
```

このログメッセージの後に、理由コード「Kernel Panic」でデバイスがリブートします。

L2ACLRedirect および RewriteEngineLoopback ヘルスモニタリング診断テストの詳細については、『Cisco Nexus 9000 シリーズ NX-OS システム管理構成ガイド』の「ランタイムまたはヘルスモニタリング診断」セクションを参照してください。

注：L2ACLRedirect および RewriteEngineLoopback ヘルスモニタリング診断テストの失敗は、この脆弱性と関係のない理由で発生する可能性もあり、この脆弱性の不正利用の結果ではない場合もあります。

回避策

この脆弱性に対処する回避策はありません。ただし、この回避策は Field Notice FN72433 の修正が含まれていない Cisco NX-OS ソフトウェアリリースには推奨されません。これらのリリースで回避策を実装すると、コントロールプレーンが長期間不安定になる可能性があります。影響を受けるリリースのリストと追加情報については、Field Notice を参照してください。

診断テスト L2ACLRedirect が繰り返し失敗する場合にデバイスのリロードを停止するには、次の

設定コマンドを使用してデフォルトのテスト動作を上書きし、エラーのみを記録します。

```
<#root>

nxos#

configure

 nxos(config)#

event manager applet l2acl_override override __L2ACLRedirect

 nxos(config-applet)#

 action 1 syslog priority emergencies msg l2aclFailed
```

テストが 10 回連続して失敗すると、次の syslog メッセージがシステムログファイルに表示されます。

```
SWITCH %$ VDC-1 %$ %DIAGCLIENT-2-EEM_ACTION_HM_SHUTDOWN: Test


           has been disabled as a part of default EEM action


SWITCH %$ VDC-1 %$ %DIAG_PORT_LB-2-L2ACLREDIRECT_LOOPBACK_TEST_FAIL: Module:1 Test:L2ACLRedirect Loopback failed 10 consec


SWITCH %$ VDC-1 %$ %EEM_ACTION-0-EMERG: l2aclFailed
```

Cisco Nexus 3100 および 3200 シリーズ スイッチの場合、失敗したテストは RewriteEngineLoopback, であるため、回避策は次の設定コマンドを使用して RewriteEngineLoopback 診断テストを上書きすることです。

```
<#root>

nxos#

configure

 nxos(config)#

event manager applet rewrite_override override __RewriteEngineLoopback

 nxos(config-applet)#
```

```
action 1 syslog priority emergencies msg RewriteEngineFailed
```

テストが 10 回連続して失敗すると、次の syslog メッセージがシステムログファイルに表示されます。

```
SWITCH %$ VDC-1 %$ %DIAGCLIENT-2-EEM_ACTION_HM_SHUTDOWN: Test

           has been disabled as a part of default EEM action

SWITCH %$ VDC-1 %$ %DIAG_PORT_LB-2-L2ACLREDIRECT_LOOPBACK_TEST_FAIL: Module:1 Test:RewriteEngine Loopback failed 10 consec

SWITCH %$ VDC-1 %$ %EEM_ACTION-0-EMERG: RewriteEngineFailed
```

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。

修正済みソフトウェア

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されるこ

とはありません。

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。

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。

サービス契約をご利用でないお客様

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 TAC（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）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。

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

7.0(3)I7(5)、ACI モードの Cisco NX-OS ソフトウェアの場合は 14.0(1h) 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-n3kn9k-healthdos-eOqSWK4g

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 2 月 6 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。