Cisco Nexus 9000シリーズスイッチの双方向フォワーディング検出におけるDoS脆弱性

High

アドバイザリーID : cisco-sa-nxos-bfd-dos-wGQXrzxn

CVE-2022-20623

初公開日 : 2022-02-23 16:00

最終更新日 : 2022-02-23 18:54

バージョン 1.1 : Final

CVSSスコア : 8.6

回避策 : No workarounds available

Cisco バグ ID : CSCvx75912

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シリーズスイッチ用Cisco NX-OSソフトウェアの双方向フォワーディング検出(BFD)トラフィックのレートリミッタの脆弱性により、認証されていないリモートの攻撃者が該当デバイスでBFDトラフィックをドロップする可能性があります。

この脆弱性は、BFDレートリミッタ機能の論理エラーに起因します。攻撃者は、巧妙に細工されたトラフィックストリームをデバイス経由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、攻撃者がBFDトラフィックをドロップし、BFDセッションフラップが発生する可能性があります。BFDセッションのフラップが原因で、ルートが不安定になり、トラフィックがドロップされ、サービス拒否(DoS)状態が発生する可能性があります。この脆弱性は、IPv4トラフィックとIPv6トラフィックの両方に適用されます。

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。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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-bfd-dos-wGQXrzxn

このアドバイザリは、2022年2月の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公開の一部です。これらのアドバイザリとリンクの一覧については、以下を参照してください。シスコのイベント対応：2022年2月の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公開。

該当製品

脆弱性のある製品

この脆弱性は、次のすべての条件が満たされると、スタンドアロンNX-OSモードのCisco Nexus 9000シリーズスイッチに影響を与えます。

- デバイスで脆弱性のあるバージョンのCisco NX-OSソフトウェアが実行されている。
- デバイスでBFD機能が有効になっている（BFDはデフォルトで無効になっている）。
- デバイスにCisco Cloud Scale ASICがインストールされている。

Cisco Nexus 9200および9300プラットフォームスイッチ

Cisco Nexus 9200および9300プラットフォームスイッチは、ソフトウェアリリース7.0(3)I6(2)から7.0(3)I7(3)に対して脆弱です。 これらのプラットフォームスイッチでサポートされるCisco Cloud Scale ASIC PID [1]は次のとおりです。

- N9K-C92160YC-X
- N9K-C92300YC
- N9K-C92304QC
- N9K-C9232C
- N9K-C92348GC-X
- N9K-C9236C
- N9K-C9272Q
- N9K-C93108TC-EX
- N9K-C93108TC-FX
- N9K-C9316D-GX
- N9K-C93180LC-EX
- N9K-C93180YC2-FX
- N9K-C93180YC-EX
- N9K-C93180YC-FX
- N9K-C93216TC-FX2
- N9K-C93240YC-FX2
- N9K-C9332C
- N9K-C93360YC-FX2
- N9K-C9336C-FX2
- N9K-C9348GC-FXP
- N9K-C93600CD-GX
- N9K-C9364C
- N9K-C9364C-GX

Cisco Nexus 9500 シリーズ スイッチ ページ

Cisco Nexus 9500シリーズスイッチは、ソフトウェアリリース7.0(3)I6(2) ~ 9.3(8)に対して脆

弱です。 10.1(1)から10.2(1)へのリリースにも脆弱性が存在します。これらのプラットフォームスイッチでサポートされるCisco Cloud Scale ASIC PID [1]は次のとおりです。

- N9K-X97160YC-EX
- N9K-X97284YC-FX
- N9K-X9732C-EX
- N9K-X9732C-FX
- N9K-X9736C-EX
- N9K-X9736C-FX
- N9K-X9788TC-FX

1. Cisco Cloud Scale ASICのPIDリストは、公開時点では正確でした。PIDに関する具体的な質問がある場合は、Cisco Technical Assistance Center(TAC)にお問い合わせください。

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。

脆弱性のあるハードウェアの判別

管理者はshow module CLIコマンドを発行してPIDを表示できます。次の例では、PIDがN9K-C93108TC-FXであるため、デバイスに脆弱性が存在します。

```
nxos# show module
Mod Ports               Module-Type                 Model              Status
--- ----- ------------------------------------ --------------------- ---------
1 54 48x1/10GT + 6x40G/100G Ethernet Modul N9K-C93108TC-FX      active *
```

BFD設定の判別

ステップ 1：BFD機能は有効になっていますか。

この脆弱性が不正利用されるのは、デバイスでBFD機能が有効になっている場合だけです。管理者はshow feature | include bfd CLIコマンドを使用して、BFD機能の状態を確認します。BFDがenabledと表示されている場合、その機能はデバイスで有効になります。

```
nxos# show feature | include bfd
bfd 1 enabled
```

ステップ 2：アクティブなBFDセッションがありますか。

この脆弱性は、デバイスにアクティブなBFDセッションが少なくとも1つ存在する限り、不正利用される可能性があります。管理者はshow bfd session CLIコマンドを発行して、BFDセッションの状態を確認できます。BFDセッションがUP状態の場合、デバイスは脆弱であると見なされます。

```
nxos# show bfd session
Interface           Dest Addr           Local det time(int*mult)      State
```

```
---------------- -------------- --------------- --------------- ----------
Te0/0/1/0 10.10.20.1 300ms(100ms*3) 6s(2s*3) UP
```

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
- VMware vSphere 向け Nexus 1000 Virtual Edge
- Nexus 1000V Switch for Microsoft Hyper-V
- Nexus 1000V Switch for VMware vSphere
- 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
- Nexus 9000 シリーズ ファブリック スイッチ（アプリケーション セントリック インフラストラクチャ（ACI）モード）
- UCS 6200 シリーズ ファブリック インターコネクト
- 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

セキュリティ侵害の痕跡

デバイスでこの脆弱性が不正利用されているかどうかを確認するには、管理者がCLIで**show hardware rate-limiter bfdコマンドを発行**し、過剰な量の廃棄されたBFDフレームを確認します。

BFDがパケットをドロップする原因となる可能性がある他のネットワークイベントがあります。BFDドロップされたパケットの増加が一貫して高い割合で観察される場合は、Cisco TACに連絡して、この脆弱性がデバイスで積極的に不正利用されているかどうかを確認してください。

nxos# **show hardware rate-limiter bfd**				
kilo bits per second				
:1				
R-L	config		Dropped	
+—+—+—+—+—+—+—+—+				
bfd	10,000	640840	**5484530000**	5485170840

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 Cisco Support and Downloads 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。

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 Cisco Service Contract 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 POS から入手できない場合は、Cisco TAC に連絡してアップグレードを入手してください。

https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

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、シスコでは Cisco Software Checker を提供しています。このツールにより、特定の Cisco NX-OS ソフトウェアリリースに該当するシスコ セキュリティアドバイザリ、および各アドバイザリで説明されている脆弱性が修正された最初のリリース（「First Fixed」）を特定できます。 また該当する場合、そのリリースに関するすべてのアドバイザリ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。

お客様は、Cisco Software Checker を使用して次の方法でアドバイザリを検索できます。

- ソフトウェア、プラットフォーム、および 1 つ以上のリリースを選択する
- 特定のリリースのリストを含む .txt ファイルをアップロードする
- **show version コマンドの出力を入力する**

検索を開始した後で、すべてのシスコ セキュリティ アドバイザリまたは 1 つ以上の特定のアドバイザリが含まれるように検索をカスタマイズできます。

また、次のフォームを使用して、Cisco NX-OS ソフトウェアとプラットフォームを選択、およびリリースを入力することで（例：Cisco Nexus 3000 シリーズ スイッチの **7.0(3)I7(5)**、**ACI モードの Cisco NX-OS ソフトウェアの 14.0(1h)**）、**シスコ セキュリティ アドバイザリの対象となるリリースであるかを判断することもできます。**

デフォルトでは、Cisco Software Checker の結果には、Security Impact Rating（SIR）が「重大」または「高」の脆弱性だけが含まれます。 「中間」の SIR 脆弱性の結果を含めるには、Cisco Software Checker を使用して、検索をカスタマイズするときに [影響の評価（Impact Rating）] **ドロップダウンリストの [中間（Medium）]** チェックボックスをオンにします。

Cisco Nexus 9000 シリーズ スイッチの SMU

シスコはこの脆弱性に対処する次の SMU もリリースしています。SMUは、Cisco.comの Software Centerからダウンロードできます。

Cisco NX-OS ソフトウェア リリース	Platform	SMU 名
7.0(3)I7(10)	Nexus 9000 シリーズ スイッチ	nxos.CSCvx75912-n9k_ALL-1.0.0-7.0.3.I7.10.lib32_n9000.rpm

9.3(8)	Nexus 9000 シリーズ スイッチ	nxos.CSCvx75912-n9k_ALL-1.0.0-9.3.8.lib32_n9000.rpm

Cisco Nexus 9000シリーズスイッチ用Cisco NX-OSソフトウェアでのSMUのダウンロードとインストールの詳細については、Cisco NX-OSシステム管理設定ガイドCisco Nexus 9000シリーズスイッチの「ソフトウェアメンテナンスアップグレードの実行」を参照してください。

その他のリソース

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
Vmware スイッチ向け Cisco Nexus 1000V
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

この脆弱性は Cisco TAC サポートケースの解決中に発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-bfd-dos-wGQXrzxn

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	「該当製品」セクションの機密データを削除。	該当製品	最終版	2022年2月23日
1.0	初回公開リリース	—	最終版	2022年2月23日

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 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。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、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。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。