スタンドアロン NX-OS モードで動作する Cisco Nexus 9000 シリーズ スイッチの Fibre Channel over Ethernet NPV におけるサービス妨害に関する脆弱性

High

アドバイザリーID : cisco-sa-20190306-nxos-npv-dos

初公開日 : 2019-03-06 16:00

バージョン 1.0 : Final

CVSSスコア : 7.4

回避策 : No workarounds available

Cisco バグ ID : CSCvk44504

CVE-2019-1617

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 NX-OS ソフトウェアの Fibre Channel over Ethernet（FCoE）N ポート仮想化（NPV）プロトコル実装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サービス妨害（DoS）状態を引き起こせるようになります。

この脆弱性は、fcoe-npv 機能のアンインストール時に FCoE パケットが正しく処理されないことに起因しています。 攻撃者が、隣接ホストから該当デバイスに FCoE フレームを次々と送信することにより、この脆弱性をエクスプロイトする可能性があります。 攻撃者が、エクスプロイトによってパケットを増幅できるようになり、その結果インターフェイスが飽和して DoS 状態が引き起こされることがあります。

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ました。 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-20190306-nxos-npv-dos

このアドバイザリは、2019 年 3 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。このバンドルの中には、26 件の脆弱性に関する 25 件のシスコ セキュリティ アドバイザリが含まれています。 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： 2019 年 3 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。

該当製品

脆弱性のある製品

本脆弱性は、Cisco NX-OS ソフトウェアの脆弱性のあるリリースを実行する次のシスコ製品に影響を与えます。

- スタンドアロン NX-OS モードの Nexus 9000 シリーズ スイッチ

脆弱性が存在するのは、次の Nexus 9000 シリーズの PID のみです。

- N9K-C92160YC-X
- N9K-C9272Q
- N9K-C9236C
- N9K-C93180YC-EX
- N9K-X9732C-EX
- N9K-C93180LC-EX
- N9K-C93180YC-FX
- N9K-X9736C-FX

システムの PID を表示するには、**show inventory** CLI コマンドを使用します。

```
9K-A# show inventory
NAME: "Chassis", DESCR: "Nexus9000 C93128TX Chassis"
PID: N9K-C93128TX          ,  VID: V02 ,  SN: SAL1822TF13

NAME: "Slot 1", DESCR: "1/10G-T Ethernet Module"
PID: N9K-C93128TX , VID: V02 , SN: SAL1822TF13

NAME: "Slot 2", DESCR: "40G Ethernet Expansion Module"
PID: N9K-M12PQ , VID: V01 , SN: SAL1910AMHD
```

注: この脆弱性は、次の条件のすべてが満たされた場合に発生します。

- 該当デバイスが vPC ピア スイッチとして設定されている。
- fcoe-npv 機能をアンインストールする。

詳細については、「詳細」を参照してください。

脆弱性が存在する Cisco NX-OS 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」の項を参照してください。

Cisco NX-OS ソフトウェア リリースの判別

管理者は、デバイスの CLI で **show version コマンド**を使用することによって、デバイスで実行されている Cisco NX-OS ソフトウェアのリリースをチェックできます。 デバイスが Cisco NX-OS ソフトウェア リリース **7.0(3)I5(1)** を実行している場合、コマンドの出力例は次のようになります。

```
9K-A# show inventory
NAME: "Chassis", DESCR: "Nexus9000 C93128TX Chassis"
PID: N9K-C93128TX          ,  VID: V02 ,  SN: SAL1822TF13

NAME: "Slot 1", DESCR: "1/10G-T Ethernet Module"
PID: N9K-C93128TX , VID: V02 , SN: SAL1822TF13

NAME: "Slot 2", DESCR: "40G Ethernet Expansion Module"
PID: N9K-M12PQ , VID: V01 , SN: SAL1910AMHD
```

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が存在する製品のセクションにリストされている製品だけ既知この脆弱性によって影響されるためにである。

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 2100 シリーズ
- Firepower 4100 シリーズ次世代ファイアウォール
- 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 1000V Switch for Microsoft Hyper-V
- Nexus 1000V Switch for VMware vSphere
- Nexus 2000 シリーズ ファブリック エクステンダ
- Nexus 3000 シリーズ スイッチ
- Nexus 3500 プラットフォーム スイッチ
- Nexus 3600 プラットフォーム 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 7700 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)
- Nexus 9500 R シリーズ ラインカードおよびファブリック モジュール
- 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

詳細

該当デバイスは、「脆弱性が存在する製品」の項に概説されている設定の場合に脆弱になります。 これらの状態を特定するにあたっては、次のコマンドが役に立ちます。

vPC 設定のステータスを確認するには、**show vpc brief** CLI コマンドを使用します。

```
9K-A# show vpc brief
Legend:
(*) - local vPC is down, forwarding via vPC peer-link

vPC domain id : 10
Peer status : peer adjacency formed ok
vPC keep-alive status : peer is alive
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 inconsistency reason : Consistency Check Not Performed
vPC role : primary
Number of vPCs configured : 1
Peer Gateway : Enabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status : Disabled
Delay-restore status : Timer is off.(timeout = 30s)
Delay-restore SVI status : Timer is off.(timeout = 10s)

vPC Peer-link status
---------------------------------------------------------------------
id Port Status Active vlans
-- ---- ------ --------------------------------------------------
1 Po1 up 1

vPC status
----------------------------------------------------------------------
id Port Status Consistency Reason Active vlans
-- ---- ------ ----------- ------ ------------
10 Po10 up success success 1
```

fcoe-npv 機能のステータスを確認するには、**show feature-set** CLI コマンドを使用します。

```
9K-A# show feature-set
Feature Set Name      ID        State  -------------------  --------  --------
fex                    3          uninstalled mpls                  4          uninstalled
fabric                 7          uninstalled
fcoe-npv               8          uninstalled
```

セキュリティ侵害の痕跡

デバイスが「脆弱性が存在する製品」の項に概説されている設定になっている場合、vPC ピア リンク以外の Rx 入力レートが比較的低く、該当の Nexus 9000 シリーズ スイッチの vPC ペアで有効になっているすべてのインターフェイスの Tx レートが高いと、侵害が発生している可能性があります。

インターフェイスのスループットの統計情報を確認するには、**show interface counter table** CLI コマンドを使用します（egrep -v "0.0 0.0% 0.0 0.0%"、Rx および Tx 列の統計情報がないインターフェイスを除く）。

```
9K-A# show feature-set
Feature Set Name      ID        State  --------------------  --------  --------
fex                    3          uninstalled mpls                 4          uninstalled
fabric                 7          uninstalled
fcoe-npv              8         uninstalled
```

```
9K-A# show feature-set
Feature Set Name      ID        State  --------------------  --------  --------
fex                    3          uninstalled mpls                 4          uninstalled
fabric                 7          uninstalled
fcoe-npv              8         uninstalled
```

```
9K-A# show feature-set
Feature Set Name      ID        State  --------------------  --------  --------
fex                    3          uninstalled mpls                 4          uninstalled
fabric                 7          uninstalled
fcoe-npv              8         uninstalled
```

```
9K-A# show feature-set
Feature Set Name      ID        State  --------------------  --------  --------
fex                    3          uninstalled mpls                 4          uninstalled
fabric                 7          uninstalled
fcoe-npv              8         uninstalled
```

侵害が発生している可能性を示すもう 1 つの状態としては、出力破棄が挙げられます。 出力破棄を確認するには、**show interface counter errors non-zero** CLI コマンドを使用します。

```
9K-A# show feature-set
Feature Set Name      ID        State  --------------------  --------  --------
fex                    3          uninstalled mpls                 4          uninstalled
fabric                 7          uninstalled
fcoe-npv              8         uninstalled
```

デバイスの出力、または上記の情報に関して不明な点がある場合は、Cisco TAC までお問い合わせください。
https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

```
9K-A# show feature-set
Feature Set Name      ID        State  --------------------  --------  --------
fex                    3          uninstalled mpls                 4          uninstalled
fabric                 7          uninstalled
fcoe-npv              8         uninstalled
```

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 アップデートを提

供しています。 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、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、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。

ソフトウェアのアップグレードを検討する際には、Cisco Security Advisories and Alerts 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は新規リリースでも継続して適切なサポートが受けられることを確認してください。 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 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。

修正済みリリース

この項の該当する表に示すように、適切なリリースにアップグレードすることをお勧めします。
完全なアップグレード ソリューションを確認するにあたっては、このアドバイザリが、公開されたバンドルの一部であることを考慮する必要があります。 バンドル アドバイザリの完全なリストは、次のページにあります。 シスコのイベント レスポンス： 2019 年 3 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。

次の表では、左の列に Cisco FXOS ソフトウェアまたは Cisco NX-OS ソフトウェアのリリースを示しています。 中央の列は、リリースがこのアドバイザリに記載されている脆弱性に該当するか

どうか、および、この脆弱性に対する修正を含む最初のリリースを示しています。 右の列では、今回のアドバイザリ バンドルに記載された脆弱性全体に対する最初の修正リリースを、影響を受けるソフトウェア リリースごとに記載しています。

各表の右の列に記載されているリリースには、脆弱性に対する修正が含まれていますが、Cisco NX-OS ソフトウェア イメージの署名検証に関する脆弱性に関連する修正については、ソフトウェア アップグレードの一部として BIOS をアップグレードする必要があります。 以下に示すいずれかの製品のソフトウェアをアップグレードする場合は、このアドバイザリに記載されている BIOS アップグレードと、該当製品の ID および BIOS バージョンの詳細を参照することをお勧めします。

- Nexus 3000 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
- スタンドアロン NX-OS モードの Nexus 9000 シリーズ スイッチ
- Nexus 9500 R シリーズ ラインカードおよびファブリック モジュール

スタンドアロン NX-OS モードの Nexus 9000 シリーズ スイッチ： CSCvk44504

Cisco NX-OS ソフトウェア リリース	この脆弱性に対する最初の修正リリース	アドバイザリ バンドルに記載されている脆弱性全体に対する最初の修正リリース
7.0(3)I4 よりも前	脆弱性なし	7.0(3)I7(6)
7.0(3)I4	脆弱性なし	7.0(3)I7(6)
7.0(3)I5	7.0(3)I7(5)	7.0(3)I7(6)
7.0(3)I6	7.0(3)I7(5)	7.0(3)I7(6)
7.0(3)I7	7.0(3)I7(5)	7.0(3)I7(6)
9.2	9.2(2)	9.2(2)

関連情報

Cisco Nexus スイッチに最適な Cisco NX-OS ソフトウェア リリースの確認に関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 向け Cisco Nexus 1000V スイッチ
Cisco Nexus 3000 シリーズおよび 3500 シリーズ スイッチ
Cisco Nexus 5000 シリーズ スイッチ
Cisco Nexus 5500 プラットフォーム スイッチ
Cisco Nexus 6000 Series Switches

Cisco Nexus 7000 シリーズ スイッチ
Cisco Nexus 9000 シリーズ スイッチ
ACI モードの Cisco Nexus 9000 シリーズ スイッチ

Cisco UCS に最適な Cisco NX-OS ソフトウェア リリースの確認に関してサポートが必要な場合は、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）では、本アドバイザリに記載されている脆弱性のエクスプロイト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 のサポート 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-20190306-nxos-npv-dos

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.0	初回公開リリース		最終版	2019 年 3 月 6 日

利用規約