Cisco IOS および IOS XE ソフトウェアの双方向フォワーディング検出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-20180328-bfd

初公開日 : 2018-03-28 16:00

最終更新日 : 2018-07-09 15:04

バージョン 1.1 : Final

CVSSスコア : 8.6

回避策 : No workarounds available

Cisco バグ ID : CSCvc40729

CVE-2018-0155

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 Catalyst 4500 シリーズ スイッチおよび Cisco Catalyst 4500-X シリーズ スイッチの双方向フォワーディング検出（BFD）オフロード実装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 *iosd* 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、BFD パケットの BFD ヘッダーが不完全な場合のエラー処理が不十分であることに起因します。 攻撃者は、該当スイッチに（またはスイッチを通過する）巧妙に細工された BFD メッセージを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。 不正利用に成功すると、攻撃者はシステムのリロードを引き起こす可能性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。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-20180328-bfd
このアドバイザリは、2018 年 3 月 28 日 発行の Cisco IOS および IOS XE ソフトウェア Security Advisory Bundled Publication の一部であり、22 の脆弱性を説明する 20 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。Cisco Event Response: March 2018 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication。

該当製品

脆弱性のある製品

本脆弱性は、BFD 機能が有効化され、脆弱性が存在する Cisco IOS ソフトウェア リリースまたは Cisco IOS XE ソフトウェア リリースを実行する以下のシスコ製品に影響を与えます。

- Catalyst 4500 Supervisor Engine 6-E（K5）
- Catalyst 4500 Supervisor Engine 6L-E（K10）
- Catalyst 4500 Supervisor Engine 7-E（K10）
- Catalyst 4500 Supervisor Engine 7L-E（K10）
- Catalyst 4500E Supervisor Engine 8-E（K10）
- Catalyst 4500E Supervisor Engine 8L-E（K10）
- Catalyst 4500E Supervisor Engine 9-E（K10）
- Catalyst 4500-X シリーズ スイッチ（K10）
- Catalyst 4900M スイッチ（K5）
- Catalyst 4948E イーサネット スイッチ（K5）

本脆弱性は、影響を受けるデバイスで BFD 機能が有効になっている場合にのみ不正利用される可能性があります。 Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアでは、ソフトウェアが IP Base（*ipbase*）パッケージ ライセンスまたはそれ以上のライセンスを実行している場合、BFD 機能がデフォルトで有効化されています。 BFD 機能は LAN Base（*lanbase*）パッケージ ライセンスではサポートされません。 詳細については、LAN Base、IP Base、およびエンタープライズ サービス イメージのサポートをご確認ください。

脆弱性が存在する Cisco IOS ソフトウェアおよび IOS XE ソフトウェアの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。

BFD 機能が有効かどうかの確認

BFD 機能が有効になっているか確認するには、管理者権限で **show running-config | | include feature bfd** コマンドを特権 EXEC モードで実行します。 次に、 IPv4 ヘルパー アドレスが設定されたデバイス上の **show running-config |** 次の例は、**show running-config | include feature bfd** コマンドを BFD 機能が無効になっている Cisco Catalyst スイッチで実行した場合です。

```
switch# show running-config | include feature bfd

platform module all feature bfd disable
platform module feature bfd disable
platform feature bfd disable
feature bfd disable
```

show running-config | | include feature bfd コマンドからの出力がない場合は、BFD 機能が有効になっていることを示します。

有効になっているパッケージ ライセンスの確認

デバイスでどのパッケージ ライセンスが有効化されているかについては、管理者が CLI で **show license feature** コマンドを使用して確認できます。 下記の例は、IP Base (*ipbase*) パッケージ ライセンスが有効化されている Cisco Catalyst スイッチで**show license feature** コマンドを実行した場合の出力を示しています。

```
C4500# show license feature

Feature name  Enforcement  Evaluation  Clear Allowed  Enabled  Right... ----------------------------
------------------------------------------------ entservices true true true false true ipbase
true          false        true            true       false
lanbase             false         false        true            false      false
internal_service    true          false        true            false      false
```

ソフトウェア リリースが **show license feature** コマンドをサポートしていない場合、管理者はデバイスで現在実行中のソフトウェア イメージのタイプを特定することで、デバイスで有効化されているパッケージ ライセンスを確認できます。 デバイスで実行中のソフトウェア イメージのタイプについては、管理者が特権 EXEC モードで **show version | include image** コマンドを使用することで確認できます。 下記の例は、LAN Base (**lanbase**) パッケージ ライセンスが有効化されているソフトウェア イメージを実行している Cisco Catalyst スイッチで **|** *show version* **include image** コマンドを実行した場合の出力を示しています。

```
C4948E# show version | include image

System image file is "bootflash:cat4500e-lanbasek9-mz.151-2.SG3.bin"
```

Cisco IOS ソフトウェア リリースの判別

デバイス上で実行されている Cisco IOS ソフトウェア リリースは、管理者がデバイスにログインして、CLI で **show version** コマンドを使用し、表示されるシステム バナーを参照することにより確認できます。 デバイスが Cisco IOS ソフトウェアを実行している場合、システム バナーに「*Cisco Internetwork Operating System Software*」や「*Cisco IOS Software*」などのテキストが表示されます。 バナーにはインストールされたイメージ名もカッコ内に表示されます。その後ろには Cisco IOS ソフトウェアのリリース番号とリリース名も表示されます。 一部のシスコ デバイスでは、**show version** コマンドをサポートしていなかったり、別の出力が表示されたりすることがあります。

次に、Cisco IOS ソフトウェア リリース 15.5(2)T1 が実行されていて、インストールされているイメージ名が *C2951-UNIVERSALK9-M* であるデバイスでのコマンド出力例を示します。

```
Router> show version

Cisco IOS Software, C2951 Software (C2951-UNIVERSALK9-M), Version 15.5(2)T1, RELEASE SOFTWARE
(fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
```

```
Compiled Mon 22-Jun-15 09:32 by prod_rel_team
.
.
.
```

Cisco IOS ソフトウェア リリースの命名と番号付けの規則に関する詳細は、『Cisco IOS and NX-OS Software Reference Guide』を参照してください。

Cisco IOS XE ソフトウェア リリースの判別

デバイス上で実行されている Cisco IOS XE ソフトウェア リリースは、管理者がデバイスにログインして、CLI で **show version コマンド**を実行し、表示されるシステム バナーを参照することにより確認できます。 デバイスが Cisco IOS XE ソフトウェアを実行している場合、システム バナーに「*Cisco IOS Software*」、「*Cisco IOS XE Software*」などのテキストが表示されます。

次に、Cisco IOS XR ソフトウェア リリース 16.2.1 が実行されていて、インストールされているイメージ名が *CAT3K_CAA-UNIVERSALK9-M* であるデバイスでのコマンドの出力例を示します。

```
ios-xe-device# show version

Cisco IOS Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version Denali
16.2.1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Sun 27-Mar-16 21:47 by mcpre
.
.
.
```

Cisco IOS XE ソフトウェア リリースの命名と番号付けの規則に関する詳細は、『Cisco IOS and NX-OS Software Reference Guide』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

他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

シスコでは、本脆弱性が Cisco Catalyst 4500 シリーズ Supervisor Engine V-10GE（K2）または Cisco Catalyst 4948 スイッチ（K2）には影響しないことを確認しています。

また、本脆弱性が Cisco IOS XR ソフトウェア、Cisco NX-OS ソフトウェアには影響を与えないことも確認しました。

セキュリティ侵害の痕跡

本アドバイザリで説明されている脆弱性の不正利用によってリロードされた後に、**show version** CLI コマンドを実行すると、出力には以下のように直前のリロード理由が表示されます。

```
ios-xe-device# show version

Cisco IOS Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version Denali
16.2.1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Sun 27-Mar-16 21:47 by mcpre
.
.
.
```

また、ログにはリロードされる前に次の例のようなメッセージが表示されます。

```
ios-xe-device# show version

Cisco IOS Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version Denali
16.2.1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Sun 27-Mar-16 21:47 by mcpre
.
.
.
```

この脆弱性が不正利用されると、該当デバイスがリロードされ、crashinfo ファイルが生成されます。 **show tech-support** CLI コマンドの出力結果および *crashinfo* ファイルを確認してデバイスに本脆弱性の不正利用が発生しているかどうかを確認するには、Cisco Technical Assistance Center（TAC）までご連絡ください。

回避策

この脆弱性に対処する回避策はありません。

自環境内で BFD 機能を使用しない場合は、グローバル コンフィギュレーション モードで **feature bfd disable** コマンドを使用すると機能を無効化できます。 **feature bfd disable** コマンドは、Cisco IOS ソフトウェア リリース 15.2(1)E 以降および Cisco IOS XE ソフトウェア リリース 3.5.0E 以降で利用できます。

自環境で BFD 機能を使用する場合は、コントロール プレーン ポリシング（CoPP）を実装して、既知の BFD ピアからの BFD パケットのみを処理し、他のすべての BFD トラフィックを破棄することで、不正アクセスを抑制することができます。

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 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 IOS および IOS XE ソフトウェア

Cisco IOS ソフトウェアおよび IOS XE 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 IOS Software Checker ツールを提供しています。このツールにより、特定のソフトウェア 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、すべてのアドバイザリに記載された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。

このツールを使用して次のタスクを実行できます。

- ドロップダウン リストからリリース（複数可）を選択するか、分析対象となるローカル システムからファイルをアップロードして、検索を開始する
- **show version** コマンドの出力をツールで解析する
- カスタマイズした検索（過去に公開されたすべてのシスコ セキュリティ アドバイザリを検索対象に含めたり、特定のアドバイザリのみ、または最新のバンドル資料から全アドバイザリ

を含めるなど）を作成する

リリースが、公開されたシスコ セキュリティ アドバイザリのいずれかに該当するかどうかを確認するには、Cisco.com の Cisco IOS Software Checker を使用するか、以下のフィールドに Cisco IOS ソフトウェアまたは Cisco IOS XE ソフトウェア リリース（たとえば、**15.1(4)M2**、**3.13.8S** など）を入力します。

Cisco IOS XE ソフトウェア リリースと Cisco IOS ソフトウェア リリースのマッピングについては、Cisco IOS XE ソフトウェアのリリースに応じて「Cisco IOS XE 2 Release Notes」、「Cisco IOS XE 3S Release Notes」、または「Cisco IOS XE 3SG Release Notes」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-20180328-bfd

改訂履歴

Version	Description	Section	Status	日付
1.1	BFD 機能のライセンス要件を明確化。「feature bfd disable」コマンドを利用できるリリースを明確化。	「脆弱性のある製品」および「回避策」	Final	2018年7月9日
1.0	初回公開リリース		Final	2018年3月28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。