Cisco IOS および IOS XE ソフトウェアの QoS においてリモートでコードが実行される脆弱性

Critical

アドバイザリーID : cisco-sa-20180328-qos

初公開日 : 2018-03-28 16:00

最終更新日 : 2018-04-27 21:15

バージョン 1.4 : Final

CVSSスコア : 9.8

回避策 : Yes

Cisco バグ ID : CSCvf73881

CVE-2018-0151

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 IOS ソフトウェア、Cisco IOS XE ソフトウェアの Quality of Service（QoS）サブシステムにおける脆弱性により、認証されていないリモート攻撃者がサービス妨害（DoS）状態を引き起こしたり、権限を昇格させて任意のコードを実行したりする可能性があります。

本脆弱性は、影響を受けるデバイスの UDP ポート 18999 を宛先とするパケットにおいて、特定の値に対する境界チェックが正しく行われないことに起因するものです。 攻撃者は、悪意のあるパケットを該当デバイスに送信することによって、本脆弱性を不正利用する可能性があります。 パケットを処理する際に、バッファ オーバーフローが攻撃に利用できる状態で発生する場合があります。 不正利用が成功すると、攻撃者は該当デバイスにおいて、権限を昇格させた上で任意のコードを実行できる可能性があります。 本脆弱性によりデバイスがリロードされ、デバイスのリロード中に一時的な DoS 状態が引き起こされる可能性があります。

なお、条件として、悪意のあるパケットが該当デバイス宛に送信され、そこで処理される必要があります。 デバイスを通過するトラフィックでは、本脆弱性は生じません。

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。該当するシスコ製品のほとんどには、この脆弱性に対処する回避策があります。

このアドバイザリは、次のリンクより確認できます。
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-qos
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

この脆弱性は、Cisco IOS ソフトウェアまたは Cisco IOS XE ソフトウェアの脆弱性のあるリリースを実行しているシスコ デバイスに影響を与えます。

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。

デバイスの確認

Cisco IOS ソフトウェアまたは Cisco IOS XE ソフトウェアを実行しているデバイスが本脆弱性の影響を受けるかどうかを確認するには、管理者がデバイスにログインして CLI で **show udp** コマンドを使用します。 show udp コマンドをサポートしていないデバイスでは、代替として show ip sockets コマンドを使用可能です。

show udp コマンドで次の例のような出力が返される場合には、デバイスがこの脆弱性の影響を受ける可能性があります。

```
Router> show udp

Proto  Remote    Port    Local    Port  In Out  Stat TTY OutputIF
17     0.0.0.0   0     --any--  18999  0   0     11   0
```

Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアにおける Dynamic Multipoint VPN（DMVPN）機能用の適応型 QoS では、UDP ポート 18999 が使用されており、同機能が影響を受けないプラットフォーム上でプロビジョニングされていることから、ポート 18888 がオープンになっている場合があります。 UDP ポート 18999 がデバイスのリスニング ポートにバインドされている場合は、Cisco IOS Software Checker を使用して、デバイスが脆弱性の存在するソフトウェア リリースを実行しているか確認します。

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。

シスコは、この脆弱性が Cisco IOS XR ソフトウェアまたは Cisco NX-OS ソフトウェアには影響を与えないことを確認しました。

回避策

次の回避策は、コントロール プレーン ポリシング（CoPP）の構成可能な着信ポートをサポートするデバイスに適用されます。 Cisco ASR 900 シリーズなど、シスコ デバイスのいくつかのファミリは、特定のポートおよびプロトコルでのみ CoPP をサポートします。 これらのプラットフォームでは利用可能な回避策がないため、修正済みのソフトウェア バージョンにアップグレードする必要があります。

DMVPN 機能用の適応型 QoS を使用しない場合は、下記に類似した CoPP ポリシーを使用することで、該当デバイスの UDP ポート 18999 宛てのすべてのトラフィックを拒否できます。

```
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
.
.
.
```

ポリシー マップ内で drop キーワードをサポートしていないプラットフォームでは、代替として下記に類似したポリシーを使用することを検討してください。

```
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
.
.
.
```

DMVPN 機能用の適応型 QoS を後で設定する場合は、デバイスを Cisco IOS ソフトウェアまたは Cisco IOS XE ソフトウェアの影響を受けないリリースにアップグレードし、CoPP ポリシーを削除する必要があります。

この回避策を自身の環境に統合するお客様には、適合性について導入前にテストすること、および次のリンクにある CoPP ベスト プラクティス ドキュメントを参照することが推奨されます。
https://www.cisco.com/c/en/us/about/security-center/copp-best-practices.html

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

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-qos

改訂履歴

Version	Description	Section	Status	日付
1.4	いくつかのシスコ プラットフォームにはこの脆弱性に対処する回避策の実装に必要な機能が含まれていない可能性があることを明示するように更新。 リスニング ポートを識別するための代替コマンドを追加。 スペルミスを修正。	要約、デバイスの評価、および回避策	Final	2018年4月27日
1.3	メタデータが更新されました。	â	Fina	20

			l	18年4月26日
1.2	回避策セクションの誤記を修正。 アクセス コントロール リストの役割について説明するコメントを追加。	回避策	Final	2018年4月13日
1.1	回避策のセクションを更新：フラグメント化されたパケットに対処するための追加のアクセスリスト エントリを含む CoPP ポリシーを更新（既存の CoPP ポリシーに統合する際に問題を起こしていた可能性があったため）。 deny キーワードをサポートしないプラットフォーム用の代替ポリシー マップを追加。	回避策	Final	2018年4月12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。