第 2 世代シスコサービス統合型ルータの Cisco IOS ソフトウェアにおける Denial of Service の脆弱性

アドバイザリーID : cisco-sa-20170927-rbip-dos
CVE-2017-12232
初公開日 : 2017-09-27 16:00
最終更新日 : 2022-12-17 04:17
バージョン 1.1 : Final
CVSSスコア : 7.4
回避策 : No workarounds available
Cisco バグ ID : CSCvc03809

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ソフトウェアを実行する第2世代シスコサービス統合型ルータ(ISR G2)の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該当デバイスのリロードを引き起こし、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、イーサネット フレームの誤った分類に起因するものです。攻撃者が、該当するデバイスに巧妙に細工されたイーサネット フレームを送信することで、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、攻撃者は該当デバイスのリロードを引き起こし、その結果 DoS 状態が発生する可能性があります。

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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-rbip-dos

このアドバイザリは、2017年9月27日に公開された13件の脆弱性に関する12件のシスコセキュリティアドバイザリを含むCisco IOSソフトウェアおよびIOS XEソフトウェアリリース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: September 2017 Semiannual Cisco IOS and IOS XE 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、Cisco IOS ソフトウェアの脆弱なリリースを実行している第 2 世代シスコ サービス統合型ルータ（ISR G2）に影響を及ぼします。

脆弱性が存在する Cisco IOS 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。

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、その後ろに、Cisco IOS ソフトウェアのリリース番号とリリース名が表示されます。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します。

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。

```
<#root>

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、『White Paper: 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 XE ソフトウェア、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を確認しました。

詳細

Cisco IOS ソフトウェアでは、Cisco ISR G2 ルータにおいて、内部使用のみを目的に設計されたカスタム プロトコルを使用します。同プロトコルは、ネットワーク モジュールなどのルータやサービス ブレード間でのメッセージの伝達に使用されます。同プロトコルはイーサネット フレームの上で構成され、ルータによるサービス ブレードへの処理や設定、内部的にはルータへの処理や設定を行えるようにします。同プロトコルは、外部で使用されることは想定されておらず、通常は、このプロトコルによるフレームが通常のネットワーク セグメントでみられることはありません。

この脆弱性は、イーサネット フレームの誤った分類により、ルータのインターフェイスの 1 つにそのフレームが到達することに起因します。特定の条件下においては、このようなフレームがプロトコルの一部として扱われる可能性があります。そして、このようなフレームがプロトコルに沿って不正に加工される場合、該当するルータでリロードを引き起こす可能性があります。

セキュリティ侵害の痕跡

この脆弱性の不正利用に成功すると、該当するデバイスでリロードと crashinfo ファイルの生成が起こり、誤ったアクセス エラー メッセージが出力されます。

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、デバイスのスタック トレースをデコードして、スタック トレースとこの問題との関連性を判別します。

プロセスがクラッシュしている場合は、デバイスのログか crashinfo ファイルに、次の例と同様のエラーメッセージが含まれます。

```
Unexpected exception to CPU: vector 1400, PC = 0x43BB03C , LR = 0x43BB038
```

crashinfo ファイルを確認し、デバイスにこの脆弱性の不正利用が発生していないかを判別するには、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。

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。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。

ソフトウェアのアップグレードを検討する際には、[シスコのセキュリティアドバイザリおよびアラート（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 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 IOS ソフトウェア

お客様が Cisco IOS 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 Cisco IOS 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。

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 メニューからリリース（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入れたり、特定のアドバイザリのみ、または最新のバンドル資料のすべての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ソフトウェアリリース(たとえば、15.1(4)M2)を入力します。

	オン

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）は、2022 年 3 月に、この脆弱性のさらなるエクスプロイトが試みられたことを認識しました。これらの脆弱性が修正済みのソフトウェアリリースにアップグレードすることを、引き続き強くお勧めします。

出典

この脆弱性はサポート ケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-rbip-dos

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	エクスプロイトに関する情報を更新。	不正利用事例と公式発表	Final	2022 年 12 月 16 日
1.0	初回公開リリース	—	Final	2017年9月27日

利用規約

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。

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。