

Cisco IOS XEソフトウェアのIPフラグメントリアセンブリにおけるDoS脆弱性



アドバイザリーID : cisco-sa-20160928-frag [CVE-2016-](#)

初公開日 : 2016-09-28 16:00

[6386](#)

バージョン 1.0 : Final

CVSSスコア : [7.8](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCux66005](#)

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 XEソフトウェアのIPv4フラグメントリアセンブリ機能の脆弱性により、認証されていないリモートの攻撃者が該当デバイスのリロードを引き起こす可能性があります。

この脆弱性は、影響を受けるソフトウェアがIPv4パケットを再構成する際に発生する内部データ構造の破損に起因します。攻撃者は、巧妙に細工されたIPv4フラグメントを該当デバイスに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、攻撃者は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) 状態に陥る危険性があります。

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。

このアドバイザリーは、次のリンクより確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-frag>

このアドバイザリーは、2016年9月28日に公開された11件の脆弱性に関する10件のシスコセキュリティアドバイザリーを含む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ーバンドルの一部です。このすべての脆弱性はセキュリティへの影響が「高」と評価されています。アドバイザリーとリンクの一覧については、『[Cisco Event Response: September 2016 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、64ビットCisco IOS XEプラットフォームでCisco IOS XEソフトウェアの脆弱性が存在するリリースを実行し、1つ以上のインターフェイスにIPv4アドレスが設定されているシスコデバイスに影響を与えます。

64ビットCisco IOS XEプラットフォームの例は次のとおりです。

- Cisco 4000 シリーズ サービス統合型ルータ
- Cisco ASR 900 シリーズ アグリゲーション サービス ルータ
- ルートプロセッサ2(RP2)またはルートプロセッサ3(RP3)を搭載したCisco ASR 1000シリーズアグリゲーションサービスルータ
- Cisco cBR-8コンバージドブロードバンドルータ

脆弱性が存在する Cisco IOS XE 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。

プラットフォームのバージョンの確認

ルータでCisco IOS XEソフトウェアの64ビットバージョンが実行されているかどうかを確認するには、管理者がshow version | i X86_64コマンドを使用します。

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 | i X86_64コマンドを、64ビットバージョンのCisco IOS XEソフトウェアを実行しているルータで実行した場合の出力を示します。

```
<#root>
```

```
Router#
```

```
show version | i X86_64
```

```
Cisco IOS Software, ASR1000 Software (X86_64_LINUX_IOSD-ADVENTERPRISEK9-M), Version 15.3(3)S8, RELEASED FOR SERVICE  
Router#
```

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 XE Software」などのテキストが表示されます。

次に、Cisco IOS XE ソフトウェア リリース 3.16.1aS が実行されているデバイスでの show version コマンドの出力例を示します。

```
<#root>
```

```
Router>
```

```
show version
```

```
Cisco IOS XE Software, Version 03.16.01a.S - Extended Support Release  
Cisco IOS Software, ASR1000 Software (PPC_LINUX_IOSD-ADVENTERPRISEK9-M), Version 15.5(3)S1a, RELEASE  
Technical Support: http://www.cisco.com/techsupport  
Copyright (c) 1986-2015 by Cisco Systems, Inc.  
Compiled Wed 04-Nov-15 17:40 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、『[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 ソフトウェア、Cisco IOS XR ソフトウェア、および 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

この脆弱性は、パケット再構成プロセスで使用される内部データ構造の破損によって引き起こされます。この破損は、メモリ内の構造のアライメントの問題に起因し、該当するソフトウェアが 64ビットCisco IOS XEプラットフォームで実行されている場合にのみ発生します。特定の状況では、データ構造の破損がポインタに影響を与え、その後ポインタにアクセスするとデバイスがリロードされます。

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。

<http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN.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です。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 Technical Assistance Center (TAC) に連絡してアップグレードを入手してください。

http://www.cisco.com/c/ja_jp/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

お客様が 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するため、シスコは Cisco IOS Software Checker ツールを提供しています。このツールを使用すると、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、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

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リリースであるかどうかを確認するには、Cisco.com の [Cisco IOS ソフトウェアチェッカー](#) 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 ソフトウェアのリリース番号 (たとえば、15.1(4)M2、3.1.4S など) を入力します。

Cisco IOSソフトウェアリリースへのCisco IOS XE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。

推奨事項

\$propertyAndFields.get("recommendations")

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-20160928-frag>

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2016 年 9 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。

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、単独の転載や意識を施した場合、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。