Cisco IOS XE ソフトウェア IP断片再組立てサービス拒否の脆弱性

High

アドバイザリーID : cisco-sa-20160928-frag

初公開日 : 2016-09-28 16:00

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

CVE-2016-6386

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 フラグメント再構成 機能の脆弱性はリモート攻撃者非認証により影響を受けたデバイスはリロードしますする可能性があります。

脆弱性は影響を受けたソフトウェアが IPv4 パケットを再構成すると発生する内部データ構造の破損が原因です。 攻撃者は影響を受けたデバイスへ巧妙に細工された IPv4 フラグメントを送信 することによってこの脆弱性を不正利用する可能性があります。 正常なエクスプロイトは攻撃者によりデバイスはサービス拒否（DoS）状態に終って、リロードしますことを可能にする可能性があります。

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。
928-frag

このアドバイザリは、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。 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。 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： Cisco IOS および IOS XE ソフトウェアに関するセキュリティ アドバイザリ公開資料（半年刊、2016 年 9 月）

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 プラットフォームの Cisco IOS XE ソフトウェアの脆弱なリリースを実行して、1つ以上のインターフェイスのために設定される IPv4 アドレスがあるCisco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下記のものを含んでいます:

- 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）との 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 はブロードバンドルータ コンバージしました

Cisco IOS XE ソフトウェアがリリースする情報に関しては脆弱で、見ますこの状況報告の修正済みソフトウェアのセクションをであって下さい。

プラットフォームのバージョンの判別

ルータが Cisco IOS XE ソフトウェアの 64 ビット バージョンを実行しているかどうか判別するために、管理者は **show version** の出力をチェックできます **| I X86_64** コマンド。

次の例は **show version** の出力を示したものです **| I** Cisco IOS XE ソフトウェアの 64 ビット バージョンを実行しているルータの **X86_64** コマンド:

```
Router# show version | i X86_64
Cisco IOS Software, ASR1000 Software (X86_64_LINUX_IOSD-ADVENTERPRISEK9-M), Version 15.3(3)S8,
RELEASE SOFTWARE (fc1)
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。

```
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 SOFTWARE (fc1)
```

```
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ついては、以下を参照してください。[ホワイト ペーパー： Cisco IOS および NX-OS ソフトウェア リファレンス ガイド]

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組み立て プロセスで使用する内部データ構造の破損によって引き起こされます。 破損はメモリの構造のためのアラインメントの問題が原因であり、影響を受けたソフトウェアが 64 ビット Cisco IOS XE プラットフォームで動作するときだけ発生します。 特別な場合に、データ構造の破損はポインタに影響を与え、ポインタへのそれに続くアクセスによりデバイスはリロードします。

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。
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 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/en/US/support/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 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**、**3.1.4S** 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

この脆弱性はサポート ケースの解決中に発見されました。

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-frag

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2016 年 9 月 28 日

利用規約