Cisco ASR 900 シリーズ アグリゲーション サービス ルータ バッファオーバーフローの脆弱性

Critical

アドバイザリーID : cisco-sa-20161102-tl1

初公開日 : 2016-11-02 16:00

バージョン 1.0 : Final

CVSSスコア : 10.0

回避策 : Yes

Cisco バグ ID : CSCuy15175

CVE-2016-6441

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 ASR 900 シリーズ ルータのトランザクション言語 1(TL1) コードの脆弱性は非認証により、リモート攻撃者 リロードをの引き起こすようにする可能性がありますまたはリモートでコードを、影響を受けたシステム実行して下さい。

影響を受けたソフトウェアが不完全な境界を行うので存在 する脆弱性は入力 データでチェックします。 攻撃者はデバイスがリロードします可能性がある TL1 ポートへ悪意のある要求を送信 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。 エクスプロイトは攻撃者が任意 のコードを実行し、システムの完全 な 制御を得るか、または影響を受けたシステムのリロードを引き起こ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。本脆弱性に対処する回避策がいくつかあります。

このアドバイザリは、次のリンクより確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161102-tl1

該当製品

脆弱性のある製品

この脆弱性は Cisco ASR 900 シリーズ アグリゲーション サービス ルータ（ASR902、ASR903 および ASR907）に影響を与えます Cisco IOS XE ソフトウェアの次のリリースを実行している:

- 3.17.0S
- 3.17.1S
- 3.17.2S
- 3.18.0S
- 3.18.1S

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。

次の例は Cisco IOS XE ソフトウェア リリース 3.17.01.S を実行しているデバイスの **show version コマンド**の出力を示したものです:

```
Router>show version

Cisco IOS XE Software, Version 03.17.01.S - Standard Support Release
Cisco IOS Software, ASR903 Software (PPC_LINUX_IOSD-UNIVERSALK9_NPE-M), Version 15.6(1)S1,
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Wed 09-Mar-16 06:34 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2016 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.
```

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、この脆弱性が以下の製品には影響を与えないことを確認しました。

- Cisco ASR 901 シリーズ アグリゲーション サービス ルータ
- Cisco ASR 901 10G シリーズ アグリゲーション サービス ルータ
- Cisco ASR 901S シリーズ アグリゲーション サービス ルータ

- Cisco ASR 920 シリーズ アグリゲーション サービス ルータ

詳細

セキュリティ侵害の痕跡

この脆弱性の不正利用によりデバイスの潜在的なリモート コード 実行かリロードを引き起こす可能性があります。 エクスプロイトは示すスタック トレースのデコードによってことを *TL1 助手プロセス*でクラッシュしたデバイス確認できます。 次の例と同じようなエラーメッセージはデバイスログで見つけることができます:

```
Router>show version

Cisco IOS XE Software, Version 03.17.01.S - Standard Support Release
Cisco IOS Software, ASR903 Software (PPC_LINUX_IOSD-UNIVERSALK9_NPE-M), Version 15.6(1)S1,
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Wed 09-Mar-16 06:34 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2016 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.
```

回避策

この脆弱性のための回避策があります。 次の軽減は Cisco IOS XE ソフトウェアの修正済み バージョンへのアップグレードがスケジュールすることができるまでインフラストラクチャの保護を助けるかもしれません:

インフラストラクチャ アクセス コントロール リスト

インフラストラクチャ デバイスを保護し、リスクを、直接インフラストラクチャ不正侵入の影響最小限に抑えるためにおよび効果は、管理者 インフラストラクチャ機器に送信 される トラフィックのポリシー施行を行うためにインフラストラクチャ アクセスコントロール アクセス・コントロール・リスト（iACLs）を展開するように助言されます。 iACL は、既存のセキュリティ ポリシーと設定に基づいて、インフラストラクチャ デバイス宛ての正当なトラフィックのみを明示的に許可することによって構築されます。 インフラストラクチャ デバイスの保護を最大にするには、IP アドレスが設定されているすべてのインターフェイスの入力方向で配備済みの iACL を適用する必要があります。 iACL 回避策はこの脆弱性に対して攻撃が信頼されたソース ソース・アドレスから起きるとき完全な保護を提供できません。

iACL ポリシーは影響を受けたデバイスに送信 される TCP および UDP ポート 3082 および 3083 の不正 な TL1 パケットを拒否します。 影響を受けたデバイスによって使用する、192.168.100.1 のホストは影響を受けたデバイスにアクセスを必要とする信頼されたソースとみなされます次の例では、192.168.60.0/24 は IPアドレス空間であり。 許可されないすべてのトラフィックを拒否する前に、ルーティングおよび管理アクセスに必要なトラフィックを許可するように注意する必要があります。 インフラストラクチャのアドレス レンジは、できるだけユーザおよびサービス セグメントに使用されるアドレス レンジとは別個にする必要があります。 このようにアドレスを設定することで、iACL の構築と配備が容易になります。

```
Router>show version

Cisco IOS XE Software, Version 03.17.01.S - Standard Support Release
Cisco IOS Software, ASR903 Software (PPC_LINUX_IOSD-UNIVERSALK9_NPE-M), Version 15.6(1)S1,
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Wed 09-Mar-16 06:34 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2016 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.
```

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。

修正済みリリース

この脆弱性は該当製品で動作する 3.17S および 3.18S リリース トレインに影響を与えます。

Cisco IOS XE 主要な該当するリリース	First Fixed Release（修正された最初のリリース）
3.17S	3.17.3S; 第 30 のために 11月スケジュールされる
3.18S	3.18.2S

Cisco IOS XE ソフトウェアの脆弱性への公開を判別するのをさらに顧客が助けるために Cisco はツールを、特定の Cisco IOS XE ソフトウェア リリースおよび以前のリリースに影響を与える Cisco Security Advisory を識別する Cisco IOSソフトウェア チェッカー提供します、各アドバイザリに説明がある脆弱性を解決する（「最初に」固定される）。 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

リリースがあらゆる公開された Cisco Security Advisory から影響を受けするかどうか判別するために、Cisco.com の Cisco IOSソフトウェア チェッカーを使用するか、または—次のフィールドで… Cisco IOS XE ソフトウェア リリースを—たとえば、**3.17.0S** 入力して下さい:

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

この脆弱性は弊社販売代理店 要求を処理するとき検出されました。

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161102-tl1

改訂履歴

Version	Description	Section	Status	日付
1.0	初版リリース		Final	2016-November-02

利用規約