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

アドバイザリーID : cisco-sa-20161102-tl1 CVE-2016-6441
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

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Transaction Language 1(TL1)コードに脆弱性が存在するため、認証されていないリモートの攻撃者によって該当システムのリロードが引き起こされたり、リモートからコードが実行されたりする可能性があります。

この脆弱性は、影響を受けるソフトウェアが入力データに対して不完全な境界チェックを実行するために存在します。攻撃者は、この脆弱性を不正利用してTL1ポートに悪意のある要求を送信し、デバイスをリロードさせる可能性があります。この不正利用により、攻撃者は任意のコードを実行してシステムのフルコントロールを取得したり、該当システムのリロードを引き起こしたり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。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。
https://sec.cloudapps.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、次のCisco IOS XEソフトウェアリリースを実行する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。

- 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。

次に、Cisco IOS XEソフトウェアリリース3.17.01.S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 03.17.01.S - Standard Support Release
Cisco IOS Software, ASR903 Software (PPC_LINUX_IOSD-UNIVERSALK9_NPE-M), Version 15.6(1)S1, RELEASE SO
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

セキュリティ侵害の痕跡

この脆弱性が不正利用されると、リモートコードが実行されたり、デバイスがリロードされたりする可能性があります。スタックトレースのデコードによって、デバイスが TL1ヘルパープロセスでクラッシュしたことが示されることで、不正利用が確認される可能性があります。デバイスログには、次の例のようなエラーメッセージが記録されています。

```
Exception to IOS Thread:
Frame pointer 0x348D3D18, PC = 0x150255E4

UNIX-EXT-SIGNAL: Segmentation fault(11), Process = TL1 Helper Process
-Traceback= 1#c2f8cd10bbd769d41be54f5792c0ec33  :10000000+50255E4 :10000000+33DEED0
:10000000+33DEED0 :10000000+33D6718 :10000000+33D5444
```

回避策

この脆弱性には回避策があります。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をスケジュールできるまで、インフラストラクチャを保護するには、次の緩和策が有効です。

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、インフラストラクチャへの直接攻撃によるリスクと影響を最小限に抑えるには、インフラストラクチャアクセスコントロールリスト(iACL)を配備して、インフラストラクチャ機器に送信されたトラフィックに対してポリシーを適用することが推奨されます。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の回避策では、信頼できる送信元アドレスから攻撃が発信された場合は、この脆弱性に対する完全な保護を提供できません。

iACLポリシーにより、該当する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パケットが拒否されます。次の例では、192.168.60.0/24が該当するデバイスによって使用されるIPアドレスレンジであり、192.168.100.1にあるホストは該当するデバイスへのアクセスを必要とする信頼された送信元であると見なされます。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。

```
ip access-list extended Infrastructure-ACL-Policy

 remark - permit trusted TL1 traffic - won't prevent exploitation from these hosts.
 remark - The exploit has only been seen on TCP port 3083, others are included for completeness.
 remark - Do not use these four lines if not using TL1 feature.
 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 3082
 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 3083
 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 3082
 permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 3083

!-- The following vulnerability-specific access control entry
!-- (ACE) can aid in identification of attacks.

 remark deny all other traffic to TL1 port.
 deny tcp any 192.168.60.0 0.0.0.255 eq 3082 log
 deny tcp any 192.168.60.0 0.0.0.255 eq 3083 log
 deny udp any 192.168.60.0 0.0.0.255 eq 3082 log
 deny udp any 192.168.60.0 0.0.0.255 eq 3083 log

!-- Permit or deny all other Layer 3 and Layer 4 traffic in accordance
!-- with existing security policies and configurations
!-- Apply iACL to interfaces in the ingress direction

 permit ip any any

interface GigabitEthernet0
 ip access-group Infrastructure-ACL-Policy in
```

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。

修正済みリリース

この脆弱性は、該当する製品で実行されている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の影響を受けるメジャーリリース	First Fixed Release（修正された最初のリリース）
3.17秒	3.17.3S（11月30日に予定）
3.18秒	3.18.2S

さらに、Cisco 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に、シスコではCisco IOS Software Checkerツールを提供しています。このツールは、特定のCisco IOS XEソフトウェアリリースに影響を与え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に記載された脆弱性を修正する最初のリリース（「初回修正」）を特定します。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 XEソフトウェアリリース(たとえば、3.17.0S)を入力します。

	オン

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、お客様からのお問い合わせへの対応の際に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161102-tl1

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	初版リリース	—	Final	2016年11月2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。

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。