

Cisco ASR 920 シリーズ ルータのための Cisco IOS XE ソフトウェア ゼロの接触プロビジョニング サービス拒否の脆弱性

High アドバイザリーID : cisco-sa-20170322-ztp [CVE-2017-3859](#)
初公開日 : 2017-03-22 16:00
バージョン 1.0 : Final
CVSSスコア : [8.6](#)
回避策 : No workarounds available
Cisco バグ ID : [CSCuy56385](#)

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 920 シリーズ アグリゲーション サービス ルータのゼロ接触提供機能のための DHCP コード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。

脆弱性はゼロ タッチ プロビジョニングのための巧妙に細工された DHCPパケットを処理するとき書式指定文字列脆弱性が原因です。 攻撃者は影響を受けたデバイスへ特に巧妙に細工された DHCPパケットを送信 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。 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。

このアドバイザリーは、次のリンクより確認できます。

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170322-ztp>

この状況報告は、5 脆弱性を記述する 5 Cisco Security Advisory を含む Cisco IOS および IOS XE ソフトウェア Security Advisory によって組み込まれる書のリリースの 2017 年 3月 22 日一部です。すべての脆弱性に最高のセキュリティへの影響定格があります。これらのアドバイザリー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： 行進 2017 半年ごと Cisco IOS および IOS XE ソフトウェア Security Advisory によって組み込まれる書。](#)

該当製品

脆弱性のある製品

この脆弱性は Cisco IOS XE ソフトウェアの該当するリリースを実行して、DHCPサーバ ポートで受信している Cisco ASR 920 シリーズ アグリゲーション サービス ルータに影響を及ぼします。デフォルトで、デバイスは DHCPサーバ ポートで受信しません。

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。

デバイスが DHCPサーバ ポートで受信しているかどうか判別するために、デバイスの **show ip sockets** privileged exec コマンドを使用して下さい。次の例は DHCPサーバや DHCP リレー エージェントで設定される Cisco IOS XE デバイスの **show ip sockets** コマンドの出力を示したものです。デバイスが DHCPサーバ パケットを聞き取っていることを出力されるポート 67 は確認します:

```
ASR920# show ip sockets
Proto Remote Port Local Port In Out Stat TTY OutputIF 17 0.0.0.0 0 192.168.0.1 18999 0 0 11 0
17 0.0.0.0 0 --any-- 67 0 0 22211 0 ASR920#
```

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 (fcl)
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。

セキュリティ侵害の痕跡

この脆弱性の不正利用により影響を受けたデバイスは crashinfo ファイルをリロードし、生成します。ファイルを検討し、デバイスがこの脆弱性の不正利用によって妥協されたかどうか判断するために Cisco Technical Assistance Center (TAC) に連絡して下さい。デバイスは次のメッセージとクラッシュするかもしれません:

```
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
```

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、[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 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、本アドバイザーの 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ー、および各アドバイザー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ー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ーを検索対象に含めたり、特定のアドバイザーのみ、または最新のバンドル資料から全アドバイザーを含めるなど) 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ー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

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170322-ztp>

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2017-March-22

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。