

Cisco IOS および IOS XE ソフトウェア自律型ネットワーク インフラストラクチャにおける Denial Of Service (DoS) の脆弱性

High アドバイザリーID : cisco-sa-20170726-anidos [CVE-2017-6663](#)
初公開日 : 2017-07-26 16:00
バージョン 1.0 : Final
CVSSスコア : [7.4](#)
回避策 : No workarounds available
Cisco バグ ID : [CSCvd88936](#)

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 ソフトウェアと Cisco IOS XE ソフトウェアの自律型ネットワーク機能における脆弱性により、隣接するネットワーク内の (未認証の) 攻撃者が自律ノードをリロードさせ、サービス妨害 (DoS) 状態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の自律型ネットワーク コードの状態に起因しています (ただし問題の状態については未解明です)。キャプチャしたパケットをリプレイし、Autonomic Control Plane (ACP) チャンネルがリセットされると、この脆弱性がエクスプロイトされる危険性があります。エクスプロイトに成功すると、ACP チャンネルがリセットされ、影響を受けるデバイスがリロードされ、DoS 状態が引き起こされる可能性があります。

シスコでは、本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せん。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-20170726-anidos>

該当製品

脆弱性のある製品

この脆弱性は、自律型ネットワークをサポートして自律型ネットワークを使用するように設定されている、Cisco IOS または Cisco IOS XE ソフトウェアのいずれかのリリースが

稼働するデバイスに影響します。

脆弱性が存在する Cisco IOS ソフトウェアおよび IOS XE ソフトウェアのリリースについての詳細は、このアドバイザリの「[修正済みソフトウェア](#)」の項を参照してください。

自律型ネットワークの設定の評価

管理者は `show running-config` コマンドを使用することで、特定デバイスが自律型ネットワークを使用するように設定されているかどうかを判別できます。| CLI の `include ^autonomic` コマンド。次に、Cisco IOS Software が実行され、自律型ネットワークを使用するように設定されているデバイスでのコマンドの出力例を示します。

```
Router# show running-config | include ^autonomic
```

```
autonomic
```

```
Router#
```

そのデバイスが自律型ネットワークを使用するように設定されていない場合、このコマンドは出力を返しません。

Cisco IOS 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 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` コマンドを使用し、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 ソフトウェアを実行している場合、システム バナーに「*Cisco Internetwork Operating System Software*」や「*Cisco IOS Software*」などのテキストが表示されます。バナーにはインストールされたイメージ名もカッコ内に表示されます。その後ろには Cisco IOS ソフトウェアのリリース番号とリリース名も表示されます。一部のシスコデバイスでは、`show version` コマンドをサポートしていなかったり、別の出力が表示されたりすることがあります。

次の例は、Cisco IOS ソフトウェア リリースが 15.5(2)T1 で、インストールされたイメージ名が *C2951-UNIVERSALK9-M* であるシスコ製品を示しています。

```
Router> show version
```

```
Cisco IOS Software, C2951 Software (C2951-UNIVERSALK9-M), Version 15.5(2)T1, RELEASE SOFTWARE (fc1)
```

```
Technical Support: http://www.cisco.com/techsupport
```

```
Copyright (c) 1986-2015 by Cisco Systems, Inc.
```

```
Compiled Mon 22-Jun-15 09:32 by prod_rel_team
```

```
.  
. .  
.
```

Cisco IOS 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](#)

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 XR ソフトウェアまたは 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。

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ソフトウェア アップデートを提供していません。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、本アドバイザリの URL をご用意ください。

修正済みリリース

本アドバイザリは以下のアドバイザリを含むコレクションの一部です。お客様におかれましては、これらも考慮した上で、アップグレード ソリューション全体をご確認ください。

- [cisco-sa-20170726-aniacp](#): Cisco IOS および IOS XE ソフトウェア自律型コントロールプレーン チャネルにおける情報漏えいの脆弱性
- [cisco-sa-20170726-anicrl](#): Cisco IOS XE ソフトウェア自律型ネットワークング インフラストラクチャ証明書失効による脆弱性
- [cisco-sa-20170726-anidos](#): Cisco IOS および IOS XE ソフトウェア自律型ネットワークング インフラストラクチャにおける Denial Of Service (DoS) の脆弱性

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。

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は確認していません。この脆弱性は、Black Hat USA 2017 カンファレンスで ERNW の Omar Eissa 氏によって発表されました。

出典

この脆弱性は、ERNW の Omar Eissa 氏によってシスコに報告されました。

URL

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170726-anidos>

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2017-July-26

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。