

# Cisco IOS ソフトウェアおよび IOS XE ソフトウェアの Autonomic Networking Infrastructure における複数の脆弱性

<b>Critical</b>	アドバイザーID : cisco-sa-20150325-ani	<a href="#">CVE-2015-0637</a>
	初公開日 : 2015-03-25 16:00	<a href="#">0637</a>
	最終更新日 : 2016-01-14 17:11	<a href="#">CVE-2015-0635</a>
	バージョン 1.2 : Final	<a href="#">0635</a>
	CVSSスコア : <a href="#">9.0</a>	<a href="#">CVE-2015-0636</a>
	回避策 : <a href="#">Yes</a>	<a href="#">0636</a>
	Cisco バグ ID : <a href="#">CSCup62191</a> , <a href="#">CSCup62315</a> , <a href="#">CSCup62293</a>	

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 ソフトウェアおよび IOS XE ソフトウェアの Autonomic Networking Infrastructure ( ANI ) 機能に複数の脆弱性が存在するため、認証されていないリモート攻撃者によりサービス妨害 ( DoS ) 状態が引き起こされたり、デバイスに対する一部のコマンド アンド コントロールが取得されたりする可能性があります。

- Autonomic Networking Registration Authority スプーフィングの脆弱性
- Autonomic Networking Infrastructure のスプーフィングされた自律ネットワーキング メッセージ サービス妨害 ( DoS ) の脆弱性
- Autonomic Networking Infrastructure のデバイスのリロードとサービス妨害 ( DoS ) の脆弱性

シスコはこれらの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す。

このアドバイザーは、次のリンクより確認できます。

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150325-ani>

注: 2015 年 3月 25 日、Cisco IOS 及び XE ソフトウェアは Security Advisory によって組み込まれる書 7 Cisco Security Advisory が含まれています。アドバイザーは Cisco IOSソフトウェアおよび Cisco IOS XE ソフトウェアの脆弱性に対処します。個々のパブリケーション リンクは Cisco イベント応答にあります: 半年ごと Cisco IOS 及び XE ソフトウェアは次のリンクで Security Advisory パブリケーションを組み込みました:

## 影響を受ける製品

自律ネットワーキング サポートを使用する以下の Cisco IOS デバイスは、これらの脆弱性に該当します。

- Cisco ASR 901、901S、および 903 シリーズ アグリゲーション サービス ルータ
- Cisco ME 3600、3600X、および 3800X シリーズ イーサネット アクセス スイッチ

## 脆弱性が存在する製品

影響を受ける Cisco IOS ソフトウェアおよび IOS XE ソフトウェアを実行するデバイスは、Autonomic Networking Infrastructure 機能が有効にされている場合、脆弱性が存在します。

デバイスが自律ネットワーキングを実行しているかどうか確認するために、管理者は 自治コマンドがあるように実行コンフィギュレーションを確認できます。

`show run | 自治を含んで下さい`

出力がないか、または 自治コマンドがなければ場合、デバイスは脆弱ではないこと。

## 脆弱性が存在しない製品

Cisco IOS XR ソフトウェアは、これらの脆弱性の影響を受けません。

Cisco IOS NX-OS ソフトウェアは、これらの脆弱性の影響を受けません。

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。

## 細部

Autonomic Networking Infrastructure ( ANI ) は Cisco IOS 機能であり、ネットワーク オペレータのネットワーク管理を簡素化する自己管理の概念を導入することにより、インテリジェントな自動デバイス管理を可能にします。Autonomic Networking Infrastructure 機能により、準備段階が不要になり、ネットワークのブートストラップ機能が簡素化されます。これにより、デバイスを安全にドメインへ参加させて設定することができます。

### Autonomic Networking Registration Authority スプーフィングの脆弱性

Cisco IOS ソフトウェアおよび IOS XE ソフトウェアの Autonomic Networking Infrastructure ( ANI ) の脆弱性により、認証されていないリモート攻撃者が Autonomic Networking Registration Authority ( ANRA ) 応答をスプーフィングする可能性があります。

この脆弱性は、Autonomic Networking ( AN ) 応答メッセージの検証が不十分であることに起因し

ます。攻撃者は、巧妙に細工された AN メッセージ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。不正利用が成功すると、攻撃者は信頼されていない自律ドメインにデバイスをブートストラップし、AN ノードに対する一部のコマンドアンドコントロールを取得し、サービス妨害 (DoS) 状態を引き起こし、正当な自律ドメインへのアクセスを阻害する可能性があります。

この脆弱性 Cisco バグ ID [CSCup62191](#) ( [登録ユーザのみ](#) ) で文書化されています、よくある脆弱性および公開 ( CVE ) ID CVE-2015-0635 は割り当てられました。

## Autonomic Networking Infrastructure のスプーフィングされた自律ネットワークングメッセージサービス妨害 ( 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 Autonomic Networking Infrastructure ( ANI ) 機能の脆弱性により、認証されていないリモート攻撃者がサービス妨害 ( DoS ) 状態を引き起こし、特定の Autonomic Networking ( AN ) ノードから自律ドメインへのアクセスを阻害する可能性があります。

この脆弱性は、有限状態マシンをリセットすることができるオーバーロードされた AN メッセージに起因します。攻撃者は、既存の AN ノードをスプーフィングするように巧妙に細工された AN メッセージ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。エクスプロイトにより、攻撃者はスプーフィングされたノードから自律ドメインへのアクセスを阻害する可能性があります。

この脆弱性は Cisco バグ ID [CSCup62293](#) ( [登録ユーザのみ](#) ) で文書化されています、CVE ID CVE-2015-0636 を割り当てられました。

## Autonomic Networking Infrastructure のデバイスのリロードとサービス妨害 ( 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 Autonomic Networking Infrastructure ( ANI ) の脆弱性により、認証されていないリモート攻撃者が該当デバイスをリロードする可能性があります。

この脆弱性は、受信した Autonomic Networking ( AN ) メッセージの検証が不十分であることに起因します。攻撃者は、ターゲットデバイスをスプーフィングするように巧妙に細工された AN メッセージ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。エクスプロイトにより、攻撃者は該当システムをリロードさせ、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 Cisco バグ ID [CSCup62315](#) ( [登録ユーザのみ](#) ) で文書化されています、CVE ID CVE-2015-0637 を割り当てられました。

## 回避策

このアドバイザリに記載されている脆弱性に対して利用可能な回避策や軽減措置はありません。

## 固定ソフトウェア

ソフトウェアアップグレードを検討するとき、顧客は Cisco Security Advisory、応答およびアラートアーカイブを <http://www.cisco.com/go/psirt> で参照し、公開および完全なアップグレードソリューションを判別するためにそれに続くアドバイザリを検討するように勧告されます。

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。

## Cisco IOS ソフトウェア

シスコでは、Cisco IOS ソフトウェアの脆弱性にさらされているかどうかを判断するためのツールを提供しています。 [Cisco IOSソフトウェアチェッカー](#)は顧客が次のタスクを行うことを可能にします:

- ドロップダウンメニューからリリースを選択するか、ローカルシステムからファイルをアップロードすることによって、検索を開始する
- 解析するためにツールのための `show version` コマンド出力を入力して下さい
- 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、特定の資料のみ、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

このツールを使うことで、そのソフトウェアリリースに関連するすべてのシスコセキュリティアドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース ( "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。 [Cisco IOSソフトウェアチェッカー](#)を参照するか、または次のフィールドでリリースがあらゆる公開された Cisco IOSソフトウェアアドバイザリから影響を受けるとどう判別するために Cisco IOS ソフトウェアリリースを入力して下さい。

( 入力例 : 15.1(4)M2 )

## Cisco IOS XE ソフトウェア

Cisco IOS XE ソフトウェアは、この資料で情報開示された脆弱性の影響を受けます。

Cisco IOS XE ソ フト ウェア アリ	First Fixed Release ( 修正され た最初のリリース )	2015 年 3 月の Cisco IOS ソフトウェアセキュリテ ィアドバイザリバンドル パブリケーションのすべ てのアドバイザリに対す る First Fixed Release ( 修正
---	---	---

リリース		された最初のリリース)
2.5.x	脆弱性なし	脆弱性あり; 3.12.3S 以降へ移行
2.6.x	脆弱性なし	脆弱性あり; 3.12.3S 以降へ移行
3.1.xS	脆弱性なし	脆弱性あり; 3.12.3S 以降へ移行
3.1.xS G	脆弱性なし	脆弱性なし
3.2.xS	脆弱性なし	脆弱性あり; 3.12.3S 以降へ移行
3.2.xS E	脆弱性なし	脆弱性あり; migrate to 3.7.1E or later.
3.2.xS G	脆弱性なし	脆弱性なし
3.2.xX O	脆弱性なし	脆弱性なし
3.2.xS Q	脆弱性なし	脆弱性なし
3.3.xS	脆弱性なし	脆弱性あり; 3.12.3S 以降へ移行
3.3.xS E	脆弱性なし	脆弱性あり; migrate to 3.7.1E or later.
3.3.xS G	脆弱性なし	脆弱性あり; migrate to 3.7.1E or later.
3.3.xX O	脆弱性なし	脆弱性あり; migrate to 3.7.1E or later.
3.3.xS Q	脆弱性なし	脆弱性なし
3.4.xS	脆弱性なし	脆弱性あり; 3.12.3S 以降へ移行
3.4.xS G	脆弱性なし	脆弱性あり; migrate to 3.7.1E or later.
3.4.xS Q	脆弱性なし	脆弱性なし
3.5.xS	脆弱性なし	脆弱性あり; 3.12.3S 以降へ移行
3.5.xE	脆弱性なし	脆弱性あり; migrate to 3.7.1E or later.
3.6.xS	脆弱性なし	脆弱性あり; 3.12.3S 以降へ移行
3.6.xE	脆弱性なし	脆弱性あり; migrate to 3.7.1E or later.
3.7.xS	脆弱性なし	脆弱性あり; 3.12.3S 以降へ移行
3.7.xE	脆弱性なし	3.7.1E

3.8.xS	脆弱性なし	脆弱性あり; 3.12.3S 以降へ移行
3.9.xS	脆弱性なし	脆弱性あり; 3.12.3S 以降へ移行
3.10.xS	脆弱性あり; 3.13.1S 以降へ移行	脆弱性あり; 3.12.3S 以降へ移行
3.11.xS	脆弱性あり; 3.13.1S 以降へ移行	脆弱性あり; 3.12.3S 以降へ移行
3.12.xS	脆弱性あり; 3.13.1S 以降へ移行	脆弱性あり; 3.12.3S 以降へ移行
3.13.xS	3.13.1S	3.13.2S
3.14.xS	脆弱性なし	脆弱性なし
3.15.xS	脆弱性なし	脆弱性なし

## Cisco IOS XR ソフトウェア

Cisco IOS XR ソフトウェアは、2015 年 3 月の Cisco IOS ソフトウェア セキュリティ アドバイザリバンドルに含まれている脆弱性の影響を受けません。

### 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。

### ソース

### URL

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150325-ani>

### 改訂履歴

Version	Description	Section	Status	Date
1.2	過去に公開されたすべてのCisco IOSソフトウェア セキュリティ アドバイザリを照会できる Cisco IOS Checker ソフトウェアの Checker フォームを更新しました。			2016 年 1 月 14 日
1.1	2015 年 3 月の Cisco IOS ソフトウェア セキュリティ アドバイザリバンドル パブリケーションのすべてのアドバイザリにおいて First Fixed Release (修正した最初のリリース) の箇所を更新しました。			2015 年 3 月 25 日

1.0	Initial public release.			2015 年 3 月 25 日
-----	-------------------------	--	--	--------------------------

## 利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザー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。