Cisco IOS および IOS XE ソフトウェア IPv6 サービス拒否の脆弱性

High

アドバイザリーID : cisco-sa-20170320-aniipv6

初公開日 : 2017-03-20 16:00

バージョン 1.0 : Final

CVSSスコア : 8.6

回避策 : Yes

Cisco バグ ID : CSCvc42729

CVE-2017-3850

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 Cisco IOS XE ソフトウェアの自治ネットワーキングインフラストラクチャ（ANI）機能の脆弱性はリモート攻撃者非認証によりサービス拒否（DoS）状態を引き起こすようにする可能性があります。

脆弱性はある特定の巧妙に細工されたパケットの不完全な入力の検証が原因です。 攻撃者は ANI 機能をサポートする Cisco IOS XE ソフトウェア リリースをまたは Cisco IOSソフトウェア実行しているデバイスへ巧妙に細工された IPv6 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。

デバイスはこの脆弱性が影響を受ける 2 つの条件を満たす必要があります:

- デバイスは ANI が設定されるかどうかに関係なく ANI をサポートする Cisco IOS XE ソフトウェアまたは Cisco IOSソフトウェアのバージョンを実行したにちがいありません（ ）
- デバイスは到達可能 IPv6 インターフェイスを備えなければなりません

エクスプロイトは攻撃者により影響を受けたデバイスは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。

このアドバイザリは、次のリンクより確認できます。
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170320-aniipv6

注: また自治レジストラで設定される影響を受けたデバイスについては関連アドバイザリを参照して下さい: Cisco IOS および IOS XE ソフトウェア自治ネットワーキングインフラストラクチャ レジストラ サービス拒否の脆弱性。

該当製品

脆弱性のある製品

この脆弱性は ANI 機能をサポートする Cisco IOSソフトウェアおよび Cisco IOS XE ソフトウェア デバイスに影響を与えます。 デバイスはこの脆弱性が影響を受ける 2 つの条件を満たす必要があります:

- デバイスは ANI が設定されるかどうかに関係なく ANI をサポートする Cisco IOS XE ソフトウェアまたは Cisco IOSソフトウェアのバージョンを実行したにちがいありません（ ）
- デバイスは到達可能 IPv6 インターフェイスを備えなければなりません

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。

インターフェイスに割り当てられた IPv6 アドレスがあるかどうか判別します

管理者は CLI で **show ipv6 interface brief** コマンドを使用することによって IPv6 アドレスを割り当てたインターフェイスを識別できます。 次の例は有効に なる IPv6 のデバイスのコマンドの出力を示したものです:

```
router# show ipv6 interface brief
.
.
.
GigabitEthernet0/0/0 [Up/Up]
 fe80::212:daff:fe62:c150
 2001:DB8::1
```

IPv6 がデバイスで動作しているソフトウェア リリースによってサポートされなければ、**show ipv6 interface brief** コマンドの使用はエラーメッセージを表示します。 デバイスで IPv6 が有効化されていない場合に、**show ipv6 interface brief** コマンドを使用すると、IPv6 アドレスを使用するインターフェイスは表示されません。 どちらのシナリオでも、デバイスはこの脆弱性の影響を受けません。

判別しますかどうか Cisco IOS か IOS XE ソフトウェアのリリースサポート ANI

お客様が 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するため、シスコは Cisco IOS Software Checker ツールを提供しています。このツールを使用すると、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。

ANI をサポートする Cisco IOS および Cisco IOS XE ソフトウェア トレインの概要ビューは次の テーブルにあります。 ただし、顧客はこのアドバイザリの修正済みソフトウェアのセクションに記述されているようにリリースを、チェックするのに Cisco IOSソフトウェア チェッカーを使用するように勧められます。

ANI をサポートする一連のCisco IOSソフトウェア

一連のCisco IOSソフトウェア	コメント
15.2E	15.2(1)E および 15.2(2)E トレインは影響を受けていません
15.2EA	15.2(2)EA トレインは影響を受けていません
15.3S	15.3(1)S および 15.3(2)S トレインは影響を受けていません
15.4S	
15.5S	
15.5SN	
15.6M	
15.6S	
15.6SN	
15.6SP	
15.6T	

ANI をサポートする Cisco IOS XE ソフトウェア トレイン

Cisco IOS XE ソフトウェア トレイン
3.7E
3.8E
3.9E
3.10S およびそれ以降トレイン
16 つのトレイン

判別しますかどうかハードウェアプラットフォームサポート ANI

デバイスが該当するソフトウェア リリースを実行する場合確認する、管理者はかどうかハードウェアプラットフォームサポート ANI CLI で**提示自治デバイス コマンドを**使用するように助言されます。 次の例は ANI をサポートするデバイスのこのコマンドの出力を示します:

ANI を示すコマンド 出力の例はサポートされます

```
Router> show autonomic device

        UDI                             PID:CSR1000V SN:XXXXXXXXXXX
        Domain Cert is Not Valid

Router>
```

ANI を示すコマンド 出力の追加例はサポートされます

```
Router> show autonomic device

Router>
```

ANI がデバイスで動作しているソフトウェア リリースによってサポートされなければ、**提示自治デバイス コマンド**の使用は次の例に示すように**エラーメッセージを表示します**:

ANI を示すコマンド 出力の例はサポートされません

```
Router> show autonomic device
                  ^
% Invalid input detected at '^' marker.

Router>
```

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 (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
.
.
.
```

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。

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影響を受けたデバイスはリロードします。 不正利用はデバイスのためのスタック トレースをデコードし、プロセスがクラッシュしたかどうか判別することによって確認することができます。 プロセスがクラッシュした場合、デバイスログは次の例と同じようなエラーメッセージが含まれています:

```
%Software-forced reload


Exception to IOS Thread:
Frame pointer 0x7F7A1225B3F8, PC = 0x7F7AE51201F7

UNIX-EXT-SIGNAL: Aborted(6), Process = AN
.
.
.
%SYS-3-OVERRUN: Block overrun at ...
```

回避策

この脆弱性に対処する回避策はありません。 回避策は UDP ポート 8888 または UDP ポート 4936 のデバイスに送信される IPv6 パケットをフィルタリングするのに Access Control List （ACL）の使用でデバイスが ANI のために設定されないとき構成されています。 ANI を使用するためにデバイスが設定される場合この回避策は適用されないし、顧客はデバイスのソフトウェア

をアップデートするように勧告されます。

以下は ACL 回避策の例です:

```
%Software-forced reload


Exception to IOS Thread:
Frame pointer 0x7F7A1225B3F8, PC = 0x7F7AE51201F7

UNIX-EXT-SIGNAL: Aborted(6), Process = AN
.
.
.
%SYS-3-OVERRUN: Block overrun at ...
```

前述の例では、 *<mydeviceaddress> は* IPv6 アドレスです。 ACL は設定されるすべての IPv6 アドレスおよびすべてのインターフェイスに適用する必要があります。 インターフェイスに設定される複数の IPv6 アドレスがある場合すべてのアドレスは ACL によってカバーする必要があります。 これには各インターフェイスのためのすべてのループバックおよびリンク ローカル アドレスが含まれています。

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 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。

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。

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製品 のセキュリティ上の問題に対する回答チーム（PSIRT）はこのアドバイザリに説明がある脆弱性の不正利用に気づいていません。 ERNW のオマール Eissa は行進 2017 のドイツの TROOPERS17 会議でこの脆弱性を表わしました。

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-20170320-aniipv6

改訂履歴

Version	Description	Section	Status	日付
1.0	Initial public release.		Final	2017-March-20

利用規約