Cisco IOSおよびIOS XEソフトウェアのIPv6におけるDoS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)状態を引き起こす可能性があります。

この脆弱性は、特定の巧妙に細工されたパケットに対する不完全な入力検証に起因します。攻撃者は、ANI機能をサポートするCisco IOSソフトウェアまたはCisco IOS XEソフトウェアリリースを実行しているデバイスに、巧妙に細工されたIPv6パケットを送信することで、この脆弱性を不正利用する可能性があります。

デバイスがこの脆弱性の影響を受けるには、次の2つの条件を満たす必要があります。

- デバイスは、ANIをサポートするCisco IOSソフトウェアまたはCisco IOS XEソフトウェアのバージョンを実行している必要があります（ANIが設定されているかどうかに関係なく）
- デバイスには到達可能なIPv6インターフェイスが必要です

この不正利用により、攻撃者は該当デバイスをリロードさせ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。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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170320-aniipv6

注：Autonomic Registrarとして設定されている該当デバイスに関するアドバイザリも参照してください(Cisco IOSおよびIOS XEソフトウェアAutonomic Networking Infrastructure Registrarのサービス妨害(DoS)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。デバイスがこの脆弱性の影響を受けるには、次の2つの条件を満たす必要があります。

- デバイスは、（ANIが設定されているかどうかに関係なく）ANIをサポートするCisco IOSソフトウェアまたはCisco IOS XEソフトウェアのバージョンを実行している必要があります
- デバイスには到達可能なIPv6インターフェイスが必要です

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IPv6アドレスが割り当てられているかどうかの確認

管理者は、CLI で show ipv6 interface brief コマンドを使用して、IPv6 アドレスを割り当てたインターフェイスを特定できます。次の例は、IPv6 が有効になっているデバイスでのコマンドの出力を示しています。

<#root>

```
router#
show ipv6 interface brief

.
.
.
GigabitEthernet0/0/0 [Up/Up]
 fe80::212:daff:fe62:c150
 2001:DB8::1
```

デバイスで実行されているソフトウェアリリースでIPv6がサポートされていない場合、show ipv6 interface briefコマンドを使用するとエラーメッセージが表示されます。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。

Cisco IOSまたはIOS XEソフトウェアリリースがANIをサポートしているかどうかの確認

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要約を次の表に示します。ただし、このアドバイザリの「修正済みソフトウェア」セクションで説明されているように、Cisco IOS Software Checkerを使用してリリースをチェックすることをお勧めします。

ANIをサポートするCisco IOSソフトウェアトレイン

Cisco IOSソフトウェアトレイン	注釈
15.2E	15.2(1)Eおよび15.2(2)Eトレインは影響を受けません
15.2EA	15.2(2)EAトレインは該当しません
15.3秒	15.3(1)Sおよび15.3(2)Sトレインは影響を受けません
15.4秒	
15.5秒	
15.5SN	
1560万	
15.6秒	
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以降のトレイン
16列車

ハードウェアプラットフォームがANIをサポートしているかどうかの確認

デバイスで該当ソフトウェアリリースが実行されている場合、管理者はCLIでshow autonomic deviceコマンドを使用して、ハードウェアプラットフォームがANIをサポートしているかどうかを確認することをお勧めします。次の例は、ANIをサポートするデバイスにおけるこのコマンドの出力を示しています。

ANIがサポートされていることを示すコマンド出力例

```
<#root>

Router>

show autonomic device


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

Router>
```

ANIがサポートされていることを示すその他のコマンド出力例

```
<#root>

Router>

show autonomic device


Router>
```

デバイスで実行されているソフトウェアリリースでANIがサポートされていない場合にshow autonomic deviceコマンドを使用すると、次の例に示すようなエラーメッセージが表示されます。

ANIがサポートされていないことを示すコマンド出力例

```
<#root>

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、その後ろに、Cisco IOS ソフトウェアのリリース番号とリリース名が表示されます。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します。

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。

<#root>

```
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。

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。

```
<#root>

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
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 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。

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、該当するデバイスがリロードされます。この脆弱性は、デバイスのスタックトレースをデコードし、ANプロセスがクラッシュしたかどうかを確認することで確認できます。プロセスがクラッシュした場合、デバイスログには次の例のようなエラーメッセージが含まれます。

```
<#root>

%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、アクセスコントロールリスト(ACL)を使用して、UDPポート8888またはUDPポート4936のデバイスがANI用に設定 されていない場合に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ことです。デバイスがANIを使用するように設定されている場合、この回避策は適用されず、デバイスのソフトウェアをアップデートすることをお勧めします。

ACLの回避策の例を次に示します。

```
!
interface GigabitEthernet0/0/0
 no ip address
 ipv6 enable
 ipv6 traffic-filter drop_ANI_IPv6 in
!
ipv6 access-list drop_ANI_IPv6
 deny udp any host <mydeviceaddress> eq 4936 log
 deny udp any host <mydeviceaddress> eq 8888 log
 permit any any
!
```

前記の例では、 <mydeviceaddress>はIPv6アドレスです。ACLは、設定されているすべてのインターフェイスとすべてのIPv6アドレスに適用する必要があります。インターフェイスに複数のIPv6アドレスが設定されている場合は、すべてのアドレスがACLの対象である必要があります。これには、各インターフェイスのすべてのループバックアドレスとリンクローカルアドレスが含まれます。

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 Cisco Service Contract 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 POS 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/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。

Cisco IOS および IOS XE ソフトウェア

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。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

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リリースであるかどうかを確認するには、Cisco.com の Cisco IOS ソフトウェアチェッカーを使用するか、以下のフィールドに Cisco IOS ソフトウェアまたは Cisco IOS XE ソフトウェアのリリース番号（たとえば、

15.1(4)M2、3.1.4S など) を入力します。

Check

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。

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)では、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は確認しておりません。ERNWのOmar Eissaは、2017年3月にドイツで開催されたTROOPERS17会議でこの脆弱性を公開しました。

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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170320-aniipv6

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	初回公開リリース	—	Final	2017-3-20

利用規約

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。