シスコ製品における細工された Ipv6 ネイバー探索パケットによるサービス妨害（DoS）脆弱性

High

アドバイザリーID： cisco-sa-20160525-ipv6

初公開日： 2016-05-25 16:00

最終更新日： 2016-09-14 13:02

バージョン 1.15： Interim

CVSSスコア： 5.0

回避策： No workarounds available

Cisco バグ ID： CSCva94139 CSCva21637 CSCva39982 CSCuz66542 CSCuz80276 CSCuz83883 CSCuz80281 CSCuz81292 CSCuz89940 CSCva61877 CSCva33531 CSCuz79330 CSCuz96600

CVE-2016-1409

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

複数のシスコ製品における IP バージョン 6（IPv6）パケット処理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該当デバイスの IPv6 トラフィック処理を停止し、デバイスにサービス妨害（DoS）状態を発生させる可能性があります。

この脆弱性は、該当デバイスに送信される巧妙に細工された IPv6 パケットの不十分な処理ロジックに起因します。 攻撃者は、巧妙に細工した IPv6 ネイバー探索（ND）パケットを該当デバイスに送信することで、この脆弱性を不正利用する可能性があります。 この不正利用により、攻撃者は IPv6 トラフィック処理を停止して、デバイスで DoS 状態を引き起こす可能性があります。

これはシスコ特有の脆弱性ではありません。 細工されたパケットを処理パスやハードウェアで早期にドロップする機能のない IPv6 処理ユニットは、この脆弱性の影響を受けます。

シスコでは、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する予定です。

このアドバイザリは、次のリンクより確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160525-ipv6

該当製品

シスコでは現在、この脆弱性の影響を受ける製品とそれらの製品への各影響を特定するために、製品ラインを調査中です。 調査の進捗に応じて、シスコは該当する各製品の Cisco Bug ID など、本アドバイザリ内の情報を更新します。 Cisco Bug Search Tool を使用するとバグを検索でき、利用可能な回避策や修正されたソフトウェア リリースなど、プラットフォーム固有の追加情報を入手できます。

脆弱性のある製品

シスコは Cisco IOS XR ソフトウェア、Cisco IOS ソフトウェア、Cisco IOS XE ソフトウェア、Cisco NX-OS ソフトウェア、Cisco ASA ソフトウェア、Cisco StarOS ソフトウェアが、このアドバイザリに記載された脆弱性の影響を受けることを確認しました。

注: 少なくとも 1 つのインターフェイスでグローバル IPv6 アドレスが設定され、トラフィックを処理する該当デバイスは、リモート攻撃者により不正利用される可能性があります。 インターフェイスにリンクローカル アドレスのみが設定され、IPv6 トラフィックを処理している該当デバイスは、レイヤ 2 隣接攻撃者によってのみ、巧妙に細工されたパケットを使用して不正利用される可能性があります。

該当するソフトウェア 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。

Cisco IOS XR ソフトウェア

次のシスコ製品は、該当リリースの Cisco IOS XR ソフトウェアを実行し、少なくとも 1 つのインターフェイスで IPv6 が有効にされている場合に、この脆弱性の影響を受けます。

- Cisco 12000 シリーズ ルータ
- Cisco ASR 9000 シリーズ アグリゲーション サービス ルータ
- Cisco Carrier Routing System
- Cisco Network Convergence System 4000 シリーズ
- Cisco Network Convergence System 6000 シリーズ ルータ

これらのプラットフォームのすべてのタイプのライン カードが、この脆弱性の影響を受けます。

デバイスが該当リリースの Cisco IOS XR ソフトウェアを実行していて、IPv6 が有効にされている場合、管理者はコマンドライン インターフェイス（CLI）で **show ipv6 interface brief** コマンドを使用することで、IPv6 アドレスが割り当てられたインターフェイスを特定できます。次に、Cisco IOS XR ソフトウェアが実行され、IPv6 が有効化されているデバイスでのコマンドの出力例を示します。

```
RP/0/RP0/CPU0:router# show ipv6 interface brief

 <!output omitted>
 GigabitEthernet0/2/0/0 [Up/Up]
 fe80::212:daff:fe62:c150
 202::1
```

IPv6 が有効化されている場合、設定に **ipv6 enable** インターフェイス コンフィギュレーション コマンドが存在します。 次に、脆弱性の存在するコンフィギュレーションの出力例を示します。

```
RP/0/RP0/CPU0:router# show ipv6 interface brief

 <!output omitted>
 GigabitEthernet0/2/0/0 [Up/Up]
 fe80::212:daff:fe62:c150
 202::1
```

デバイスで実行されている Cisco IOS XR 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 メッセージが生成されます。 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 ソフトウェア

該当リリースの Cisco IOS ソフトウェアを実行していて、1 つ以上のインターフェイスで IPv6 が有効にされているシスコ製品は、この脆弱性の影響を受けます。 デフォルトでは、IPv6 は有効化されていません。

IPv6 が 1 つ以上のインターフェイスで有効になっているかどうかは、管理者が CLI で **show running-config | include ipv6.(enable|address)**特権 EXEC コマンドを使用することにより確認できます。 IPv6 が有効化されている場合、コマンドの出力に *ipv6 enable* および *ipv6 address* が表示されます。

以下に、 **show running-config | include ipv6.(enable|address)**コマンドを、IPv6 が設定された Cisco IOS XE ソフトウェアを実行しているデバイスで実行した場合の出力例を示します。

```
Router# show running-config | include ipv6.(enable|address)
 ipv6 enable
 ipv6 address dhcp rapid-commit
 ipv6 address autoconfig   ipv6 address MANAGEMENT ::1FFF:0:0:0:3560/128
 ipv6 address 2001:DB8::1/64
```

Cisco IOS XE ソフトウェア

次の製品は、該当リリースの Cisco IOS XE ソフトウェアを実行し、トラフィック処理を行うインターフェイスの少なくとも 1 つで IPv6 が有効になっている場合、この脆弱性の影響を受けます。

- Cisco 4300 シリーズ サービス統合型ルータ
- Cisco 4400 シリーズ サービス統合型ルータ
- Cisco ASR 900 シリーズ アグリゲーション サービス ルータ
- Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ
- シスコ クラウド サービス ルータ 1000V シリーズ
- Cisco IOS XE ソフトウェアを実行するスイッチ

デフォルトでは、IPv6 は有効化されていません。

この脆弱性は、シャーシに設置された Embedded Services Processor（ESP）とルート プロセッサ（RP）の特定の組み合わせには依存しません。 シャーシに設置された ESP と RP がどのような組み合わせでも、この脆弱性の影響を受けます。

IPv6 が 1 つ以上のインターフェイスで有効になっているかどうかは、管理者が CLI で **show running-config | include ipv6.(enable|address)**特権 EXEC コマンドを使用することにより確認できます。 IPv6 が有効化されている場合、コマンドの出力に「 *ipv6 enable*」または「 *ipv6 address*」が表示されます。

以下に、 **show running-config | include ipv6.(enable|address)**コマンドを、IPv6 が設定された Cisco IOS XE ソフトウェアを実行しているデバイスで実行した場合の出力例を示します。

```
Router# show running-config | include ipv6.(enable|address)
 ipv6 enable
 ipv6 address dhcp rapid-commit
 ipv6 address autoconfig   ipv6 address MANAGEMENT ::1FFF:0:0:0:3560/128
 ipv6 address 2001:DB8::1/64
```

Cisco NX-OS ソフトウェア

Cisco NX-OS ソフトウェアを実行するすべてのシスコ製品は、トラフィックを処理する 1 つ以上のインターフェイスで IPv6 が有効にされている場合に、この脆弱性の影響を受けます。 デフォルトでは、IPv6 は有効化されていません。

IPv6 が 1 つ以上のインターフェイスで有効になっているかどうかは、管理者が CLI で **show running-config | include ipv6.address** 特権 EXEC コマンドを使用することにより確認できます。 IPv6 が有効化されている場合、コマンドの出力に「 *ipv6 address*」が表示されます。

以下に、 **show running-config | include ipv6.address** コマンドを、IPv6 を有効にした Cisco NX-OS ソフトウェアを実行しているデバイスで実行した場合の出力例を示します。

```
Router# show running-config | include ipv6.address
 ipv6 address 2001:DB8::1/64
```

Cisco ASA ソフトウェア

IPv6 は、デフォルトでは有効化されていません。 Cisco ASA または Cisco ASASM で IPv6 を有効にするには、IPv6 が正しく動作するため少なくともリンクローカル アドレスが設定されている必要があります。 グローバル アドレスを設定すると、リンクローカル アドレスは各インターフェイスで自動的に設定されます。

Cisco ASA または Cisco ASASM で IPv6 が有効化されていることは、管理者が CLI で **show ipv6 interface** コマンドを使用して、出力が返されることによって確認できます。 以下に、2 つのインターフェイス (内部および外部) が設定され、IPv6 が有効化された Cisco ASA の出力例を示します。

```
ciscoasa# show ipv6 interface
outside is up, line protocol is up
  IPv6 is enabled, link-local address is fe80::219:2fff:fe83:4f42
  No global unicast address is configured
  Joined group address(es):
    ff02::1
    ff02::1:ff83:4f42
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses.
inside is up, line protocol is up
  IPv6 is enabled, link-local address is fe80::219:2fff:fe83:4f43
  No global unicast address is configured
  Joined group address(es):
    ff02::1
    ff02::1:ff83:4f43
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses.
```

Cisco StarOS ソフトウェア

Cisco StarOS ソフトウェアを実行する Cisco ASR 5000 シリーズ デバイスは、トラフィック処理を行う 1 つ以上のインターフェイスで IPv6 が有効にされている場合に、この脆弱性の影響を受けます。 デフォルトでは、IPv6 は有効化されていません。

IPv6 が 1 つ以上のインターフェイスで有効になっているかどうかは、管理者が CLI で **show ipv6 interface summary** 特権 EXEC コマンドを使用することにより確認できます。 IPv6 が有効化されている場合、コマンドの出力に IPv6 アドレスが表示されます。

次に、Cisco StarOS ソフトウェアが実行され、IPv6 が有効化されているデバイスでの **show ipv6 interface summary** コマンドの出力例を示します。

```
[local]router# show ipv6 interface summary
Friday February 21 09:00:07 UTC 2014
Interface Name                 Address/Mask        Port                Status
============================== ================== ================== ======
int1_test_v6                    2001:db8::1/64 20/1 vlan 122     UP
int2_test_v6                    2001:db8::2/64 21/1 vlan 122     UP
int3_test_v6                    2001:db8::3/64 22/1 vlan 122     UP
int4_test_v6                    2001:db8::4/64 23/1 vlan 130     UP
```

Cisco IOS XR 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 XR ソフトウェア リリースとそれを実行しているデバイスの名前は、管理者がデバイスにログインして、CLI で **show version** コマンドを使用することにより確認できます。 デバイスが Cisco IOS XR 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 XR Software* 」などのテキストが表示されます。 デバイスで現在実行しているシステム イメージ ファイルの場所と名前は、「 *System image file is*」の横に表示されます。 ハードウェア製品の名前はシステム イメージ ファイル名の次の行に表示されます。

次に、Cisco IOS XR ソフトウェア リリース 4.1.0 が実行されていて、インストールされているイメージ名が *mbihfr-rp.vm* であるデバイスでの **show version** コマンドの出力例を示します。

```
RP/0/RP0/CPU0:router# show version
 Mon May 31 02:14:12.722 DST

 Cisco IOS XR Software, Version 4.1.0
 Copyright (c) 2010 by Cisco Systems, Inc.

 ROM: System Bootstrap, Version 2.100(20100129:213223) [CRS-1 ROMMON],

 router uptime is 1 week, 6 days, 4 hours, 22 minutes
 System image file is "bootflash:disk0/hfr-os-mbi-4.1.0/mbihfr-rp.vm"

 cisco CRS-8/S (7457) processor with 4194304K bytes of memory.
 7457 processor at 1197Mhz, Revision 1.2
```

Cisco IOS ソフトウェア リリースの判別

シスコ製品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。 カッコ内にイメージ名が表示され、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、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 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** コマンドを使用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 3.6.2S (Cisco IOS ソフトウェア リリース 15.2(2)S2 にマッピング) 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 Software, IOS-XE Software (PPC_LINUX_IOSD-ADVENTERPRISEK9-M), Version 15.2(2)S2,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Tue 07-Aug-12 13:40 by mcpre
```

Cisco NX-OS 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 NX-OS 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** コマンドを使用することにより確認できます。 デバイスが Cisco NX-OS ソフトウェアを実行している場合、システム バナーに「 *Cisco Nexus Operating System (NX-OS) Software*」などのテキストが表示されます。

次に、Cisco NX-OS ソフトウェア リリース 7.1(1)N1(1) を実行している Cisco Nexus 5000 シリーズ スイッチでの **show version** コマンドの出力例を示します。

```
# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Documents: http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html
Copyright (c) 2002-2012, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

Software
BIOS:      version 3.6.0
```

```
loader:    version N/A
kickstart: version 7.1(1)N1(1)
system:    version 7.1(1)N1(1)
```

Cisco ASA ソフトウェア リリースの判別

脆弱性のあるバージョンの Cisco ASA ソフトウェアがアプライアンスで実行されているかどうかを知るには、 **show version** コマンドを発行します。 Cisco ASA ソフトウェア リリース 8.4(1) が実行されているデバイスの例を以下に示します。

```
ciscoasa#show version | include Version
Cisco Adaptive Security Appliance Software Version 8.4(1)
Device Manager Version 6.4(1)
```

Cisco ASDM を使用してデバイスを管理している場合は、ログイン ウィンドウ、または Cisco ASDM ウィンドウの左上にソフトウェアのリリースが表示されます。

Cisco StarOS ソフトウェア リリースの判別

シスコ製品上で実行されている Cisco StarOS 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。 各ソフトウェア イメージはリリース バージョンとビルド番号によって特定できます。

次の例は、Cisco StarOS ソフトウェア リリース 15.0 (49328) が実行されているシスコ製品を示しています。

```
[local<host_name># show version
Active Software:
 Image Version: 15.0 (49328)
 Image Branch Version: 015.000(001)
 Image Description: Production_Build
 Image Date: Tue Apr 23 00:45:12 EDT 2013
 Boot Image: Unknown
```

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。

セキュリティ侵害の痕跡

この脆弱性の不正利用により、該当プラットフォームで CPU の使用量が高くなる可能性があります。 また、該当デバイスで IPv6 トラフィックの処理が停止される可能性があります。 一部のデバイスでは、この脆弱性が不正利用されると、IPv6 トラフィックに加えて、デバイスで終端するトラフィックのサービスが一時的に中断される可能性があります。

回避策

回避策は利用可能になり次第、Cisco Bugs に記載されます。バグは Cisco Bug Search Tool で検索できます。

また、インターネット エッジ ルータにアクセス コントロール リスト（ACL）を配置して IPv6 ND パケットを拒否することでルータ背後のインフラストラクチャ デバイスを保護するなど、緩和策を講じる必要があります。 インフラストラクチャを保護するため、IPv6 ND パケットはローカル リンクに限定してエッジでドロップする必要があります。 インターネット エッジでこれらのパケットをドロップする手段は、一般にベスト プラクティスとして受け入れられています。 または、可能な限りスタティック IPv6 ネイバーを設定し、すべての IPv6 ND パケットをエッジで拒否することにより、この脆弱性を軽減します。

修正済みソフトウェア

Cisco IOS XR ソフトウェア、Cisco IOS ソフトウェア、Cisco IOS XE ソフトウェア、Cisco NX-OS ソフトウェアのすべてのリリースが、このアドバイザリに記載された脆弱性の影響を受けます。

すべてのハードウェア プラットフォームが同様に影響を受けるわけではありません。 ソフトウェアへの修正を適用できる場合、利用可能になった時点で該当ソフトウェア リリースの更新プログラムが公開され、それらの更新に関する情報は Cisco Bugs に記載されます。 Cisco Bug Search Tool を使用してアクセスできます。 ソフトウェア アップデートが適用できない場合、各 Cisco Bug リリース ノートにガイダンスが記載されます。

ソフトウェアのアップグレードを検討する場合は、 http://www.cisco.com/go/psirt の Cisco Security Advisories and Responses アーカイブや後続のアドバイザリを参照して、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は新規リリースでも継続して適切なサポートが受けられることを確認してください。 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。

不正利用事例と公式発表

2016 年 5 月 26 日時点で、Cisco Product Security Incident Response Team（PSIRT）は該当プラットフォームを実行している一部のお客様の業務の中断を確認しました。

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

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160525-ipv6

改訂履歴

Version	Description	Section	Status	日付
1.15	Cisco bug CSCva94139、 CSCva61877 を追加	Cisco Bug ID	Interim	2016年9月14日
1.14	Cisco bug CSCva3353 を追加	Cisco Bug ID	Interim	2016年8月9日
1.13	Cisco bug CSCva39982 を追加	Cisco Bug ID	Interim	2016年7月12日
1.12	潜在的な緩和策に関する情報を含むため概要および回避策を更新。	概要、回避策	Interim	2016年7月6日
1.11	調査中の製品および修正済みソフトウェアに関する情報を更新。	該当製品、修正済みソフトウェア	Interim	2016年7月1日
1.10	修正済みソフトウェアに関する情報を更新。	修正済みソフトウェア	Interim	2016年6月20日
1.9	修正済みソフトウェアに関する情報を更新。	修正済みソフトウェア	Interim	2016年

				6月16日
1.8	調査中の製品および脆弱性が存在する製品に関する情報を更新。	該当製品	Interim	2016年6月13日
1.7	修正済みソフトウェアに関する情報を更新。	修正済みソフトウェア	Interim	2016年6月10日
1.6	調査中の製品に関する情報を更新。	該当製品	Interim	2016年6月8日
1.5	修正済みソフトウェアに関する情報を更新。	修正済みソフトウェア	Interim	2016年6月6日
1.4	調査中の製品および脆弱性が存在する製品に関する情報を更新。	該当製品	Interim	2016年6月3日
1.3	潜在的な緩和策に関する情報を含むため概要および回避策を更新。	概要、回避策	Interim	2016月6月1日
1.2	調査中の製品および脆弱性が存在する製品に関する情報を更新。 侵入痕跡の疑い、およびサービス中断に関する情報を追加。	該当製品	Interim	2016月5月

				31日
1.1	調査中の製品および脆弱性が存在する製品に関する情報を更新。 侵入痕跡の疑い、およびサービス中断に関する情報を追加。	該当製品、侵入の痕跡、不正利用事例と公式発表	Interim	2016年5月26日
1.0	初回公開リリース		Interim	2016年5月25日

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、単独の転載や意訳を施した場合、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。