Cisco IOS および IOS XE ソフトウェア IPv6 First Hop Security（FHS）サービス拒否の脆弱性

High

アドバイザリーID : cisco-sa-20150923-fhs

初公開日 : 2015-09-23 16:00

最終更新日 : 2016-12-08 15:19

バージョン 1.2 : Final

CVSSスコア : 7.8

回避策 : No workarounds available

Cisco バグ ID : CSCus19794 CSCuo04400

CVE-2015-6278

CVE-2015-6279

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

IPv6 の 2 脆弱性は最初にセキュリティ機能 Cisco IOS のホップし、IOS XE ソフトウェアはリモート攻撃者非認証により影響を受けたデバイスはリロードしますする可能性があります。

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。 これらの脆弱性を軽減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。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150923-fhs

注: 2015 年 9月 23 日、Cisco IOS および IOS XE ソフトウェア Security Advisory によって組み込まれる書のリリースは 3 Cisco Security Advisory が含まれています。 すべてのアドバイザリは 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。 個々の公表資料へのリンクは、次のリンクにある「*シスコのイベント対応*： *9月 2015 年半年ごと Cisco IOS および IOS 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:*

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep15.html

該当製品

これらの脆弱性は Cisco IOS か Cisco IOS XE ソフトウェアを実行する製品に影響を及ぼします

。ソフトウェアの影響を受けたバージョンに関する詳細についてはこの Security Advisory の「ソフトウェア バージョン および 修正」セクションを参照して下さい。

脆弱性のある製品

実行するデバイスは両方の脆弱性から Cisco IOS の脆弱なバージョンか Cisco IOS XE ソフトウェア 最初のホップ セキュリティ機能からの IPv6 スヌーピング機能が設定される場合影響を受けます。
IPv6 スヌーピング機能が設定されるかどうか判別するために、**show running config を**使用して下さい **| スヌーピングする IPv6 を含んで下さい|interface コマンドは**スヌーピングする IPv6 がインターフェイスで設定される確認しましたり、または**提示 IPv6 スヌーピング ポリシー** コマンドをことを使用し。

次の例は GigabitEthernet0/0/1 インターフェイスで設定される IPV6 スヌーピングのルータのこれらのコマンドの出力を示します:

```
router#show running-config | include ipv6 snooping|interface
...
interface GigabitEthernet0/0/1
ipv6 snooping
...
router#show ipv6 snooping policies
Target               Type  Policy               Feature        Target range
Gi0/0/1              PORT  default              Snooping       vlan all
```

、管理者はデバイスにログインどの Cisco IOS ソフトウェア リリースが Cisco製品で動作しているか判別し、システムバナーを表示する **show version コマンドを**発行するためにできます。 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続きます。 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 *C2951-UNIVERSALK9-M* のインストール済みイメージ名前と Cisco IOS ソフトウェア リリース 15.2(4)T1 を実行している Cisco製品を指定したものです:

```
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
!--- output truncated
```

Cisco IOSソフトウェアのための指名および番号付与規則についての情報に関しては、白書を参照して下さい: 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

Cisco IOS XR はこれらの脆弱性から影響を受けません。
Cisco NX-OS は、これらの脆弱性の影響を受けません。
Ciscoワイヤレス LAN コントローラ（WLC）はこれらの脆弱性から影響を受けません。

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。

詳細

セキュリティおよびスケーラビリティを提供するために、IPv6 スヌーピング機能は IPv6 Neighbor Discovery（ND）インスペクション、IPv6 デバイス トラッキング、IPv6 アドレスを含む複数のレイヤ2 IPv6 最初のホップ セキュリティ機能を、グリーニングおよび IPv6 バインディング テーブル リカバリ組み込みます。 IPv6 ND インスペクションはレイヤ2 で、またはレイヤ2 とレイヤ3 の間でセキュリティおよびスケーラビリティを IPv6 機能に与えるために動作します。

Cisco IOS および IPv6 スヌーピング機能を使用するために設定される IOS XE ソフトウェアは次の 2 脆弱性から影響を受けます:

Cisco IOS および IOS XE ソフトウェア IPv6 スヌーピング サービス拒否の脆弱性
Cisco IOS および IOS XE ソフトウェアの最初のホップ セキュリティ機能からの IPv6 スヌーピング機能の脆弱性はリモート攻撃者非認証により影響を受けたデバイスはリロードしますする可能性があります。

脆弱性は暗号に生成アドレス（CGA）オプションを使用する IPv6 ND パケットの不十分な検証が原因です。 攻撃者は IPv6 スヌーピング機能が有効に なる影響を受けたデバイスへ不正 な 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。

この脆弱性 Cisco バグ ID CSCuo04400 （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-2015-6279 は割り当てられました。

Cisco IOS および IOS XE ソフトウェア IPv6 スヌーピング セキュア ネットワーク開発 サービス拒否の脆弱性
Cisco IOS および IOS XE ソフトウェアの最初のホップ セキュリティ機能からの IPv6 スヌーピング機能の脆弱性はリモート攻撃者非認証により影響を受けたデバイスはリロードしますする可能性があります。

脆弱性は特定の IPv6 ND パケットに対して不十分なコントロール プレーン 保護（CPPr）が原因です。 攻撃者は特定の IPv6 ND パケットで構成されている IPv6 スヌーピング機能が設定される影響を受けたデバイスへトラフィックのフラッドを送信 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。

この脆弱性 Cisco バグ ID CSCus19794 （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-2015-6278 は割り当てられました

回避策

これらの脆弱性に対する回避策はありません。

管理者はデバイスが nonvulnerable リリースにアップグレードされるまで影響を受けたデバイスの IPv6 スヌーピング機能を無効に するかもしれません。

IPv6 スヌーピング使用を無効に するため機能が設定された各インターフェイスにおけるインターフェイス設定モードの **IPv6 スヌーピング** コマンド無し。

機能が無効に なったことを確認するために、**show running-config を**使用して下さい **| IPv6 スヌーピング** コマンドか**提示 IPv6 スヌーピング ポリシー** コマンドを**含んで下さい。**

次の例は無効に なる IPv6 スヌーピングの Cisco IOSデバイスを示したものです:

```
router#show ipv6 snooping policies
Target               Type  Policy               Feature        Target range
router#
```

修正済みソフトウェア

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, Responses, and Alerts アーカイブや、後続のアドバイザリを参照して侵害の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。

Cisco IOS ソフトウェア

シスコでは、お客様が 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 Software Checker により、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
- **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 Software Checker を参照するか、次のフィールドに Cisco IOS ソフトウェア リリースを入力して、いずれかの公開された Cisco IOS ソフトウェア アドバイザリに該当するかどうかを判断できます。

(入力例： 15.1(4)M2)

Cisco IOS ソフトウェア リリースへの Cisco IOS XE ソフトウェア リリースのマッピングについては、「Cisco IOS XE 2 Release Notes」、「Cisco IOS XE 3S Release Notes」、および「Cisco IOS XE 3SG Release Notes」を参照してください。

Cisco IOS XE ソフトウェア

Cisco IOS XE ソフトウェアはこのアドバイザリに説明がある脆弱性から影響を受けます。

Cisco IOS XE ソフトウェア リリース群	First Fixed Release for このアドバイザリ	First Fixed Release for のすべてのアドバイザリ 9月 2015 年の Cisco IOS および IOS XE ソフトウェア Security Advisory 組み込まれたパブリケーション
2.6	脆弱性なし	Vulnerable; 3.10.6S またはそれ以降への移行する。
3.1S	脆弱性なし	Vulnerable; 3.10.6S またはそれ以降への移行する。
3.1SG	脆弱性なし	脆弱性なし
3.2S	脆弱性なし	Vulnerable; 3.10.6S またはそれ以降への移行する。
3.2SE	Vulnerable; 3.6.3E またはそれ以降への移行する。	Vulnerable; 3.6.3E またはそれ以降への移行する。
3.2SG	脆弱性なし	脆弱性なし
3.2SQ	脆弱性なし	脆弱性なし
3.2XO	脆弱性なし	脆弱性なし
3.3S	脆弱性なし	Vulnerable; 3.10.6S またはそれ以降への移行する。
3.3SE	Vulnerable; 3.6.3E またはそれ以降への移行する。	Vulnerable; 3.6.3E またはそれ以降への移行する。
3.3SG	脆弱性なし	脆弱性なし
3.3SQ	脆弱性なし	脆弱性なし
3.3XO	Vulnerable; 3.6.3E またはそれ以降への移行する。	Vulnerable; 3.6.3E またはそれ以降への移行する。

3.4S	脆弱性なし	Vulnerable; 3.10.6S またはそれ以降への移行する。
3.4SG	Vulnerable; 3.6.3E またはそれ以降への移行する。	Vulnerable; 3.6.3E またはそれ以降への移行する。
3.4SQ	脆弱性なし	脆弱性なし
3.5E	Vulnerable; 3.6.3E またはそれ以降への移行する。	Vulnerable; 3.6.3E またはそれ以降への移行する。
3.5S	脆弱性なし	Vulnerable; 3.10.6S またはそれ以降への移行する。
3.5SQ	脆弱性なし	脆弱性なし
3.6E	3.6.3E	3.6.3E
3.6S	脆弱性なし	Vulnerable; 3.10.6S またはそれ以降への移行する。
3.7E	3.7.2E	3.7.2E
3.7S	脆弱性なし	Vulnerable; 3.10.6S またはそれ以降への移行する。
3.8S	脆弱性なし	Vulnerable; 3.10.6S またはそれ以降への移行する。
3.9S	Vulnerable; 3.10.6S またはそれ以降への移行する。	Vulnerable; 3.10.6S またはそれ以降への移行する。
3.10S	3.10.6S	3.10.6S
3.11S	3.11.4S	Vulnerable; 3.13.3S またはそれ以降への移行する。
3.12S	Vulnerable; 3.13.3S またはそれ以降への移行する。	Vulnerable; 3.13.3S またはそれ以降への移行する。
3.13S	3.13.3S	3.13.3S
3.14S	3.14.2S	Vulnerable; 3.15.1S またはそれ以降への移行する。
3.15S	脆弱性なし	3.15.1S
3.16S	脆弱性なし	脆弱性なし

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とその公表は確認しておりません。

これらの脆弱性は内部テストで発見されました。

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150923-fhs

改訂履歴

バージョン	説明	セクション	ステータス	Date

1.2	更新済楕円形定義は利用できます。			2016-December-08
1.1	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
1.0	初回公開リリース			2015-September-23

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。