Cisco IOSソフトウェア DHCP バージョン 6 サービス拒否の脆弱性

High

アドバイザリーID : cisco-sa-20140924-dhcpv6

初公開日 : 2014-09-24 16:00

バージョン 1.0 : Final

CVSSスコア : 7.8

回避策 : No Workarounds available

Cisco バグ ID : CSCum90081

CVE-2014-3359

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 DHCP バージョン 6 （DHCPv6）サーバ実装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。

脆弱性は形式が間違った DHCPv6 パケットの不適当な解析が原因です。 攻撃者は影響を受けたデバイスが処理される形式が間違った DHCPv6 パケットの送信によってこの脆弱性を不正利用する可能性があります。 エクスプロイトは攻撃者により影響を受けたデバイスのメモリリークおよび終局リロードを引き起こ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-20140924-dhcpv6

注: 2014 年 9月 24 日、Cisco IOSソフトウェア Security Advisory によって組み込まれる書は 6 Cisco Security Advisory が含まれています。 すべての状況報告は Cisco IOS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：半年ごと Cisco IOSソフトウェア Security Advisory は次のリンクで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_sep14.html

該当製品

脆弱性のある製品

DHCPv6 サーバ 機能がイネーブルの状態で影響を受けた Cisco IOSソフトウェアか Cisco IOS XE ソフトウェアを実行している Ciscoデバイスは脆弱です。 DHCPv6 サーバ 機能はデフォルトでイネーブルになっていません。 DHCPv6 クライアントかリレー エージェントで設定される Ciscoデバイスはこの脆弱性から影響を受けません。

Cisco IOSデバイスまたは Cisco IOS XE デバイスが DHCPv6 サーバで設定されるかどうか判別するために、 **提示 IPv6 dhcp interface コマンドを**発行して下さい。

次の例は DHCPv6 サーバで設定されないので脆弱ではない Cisco IOSデバイスを示したものです:

```
Router#show ipv6 dhcp interface
Router#
```

次の例はこの脆弱性から影響を受ける Cisco IOSデバイスを示したものです。 デバイスは DHCPv6 サーバ 機能が FastEthernet0/0 インターフェイスに加えられ、DHCPv6 がサーバ プール DHCPv6-stateful 使用されるので脆弱です:

```
Router#show ipv6 dhcp interface
FastEthernet0/0 is in server mode
 Using pool: DHCPv6-stateful
 Preference value: 0
 Hint from client: ignored
 Rapid-Commit: disabled
Router#
```

次の例はこの脆弱性から影響を受ける Cisco IOSデバイスを示したものです。 デバイスは DHCPv6 サーバ 機能が FastEthernet0/0 および FastEthernet0/1 インターフェイスに加えられるので脆弱です:

```
Router#show ipv6 dhcp interface
FastEthernet0/0 is in server mode
 Using pool: DHCPv6-stateful
 Preference value: 0
 Hint from client: ignored
 Rapid-Commit: disabled
Router#
```

シスコ製品上で動作している Cisco IOS ソフトウェア リリースについては、管理者がデバイスにログインして **show version** コマンドを発行し、システム バナーを表示することで判別できます。 "Internetwork Operating System Software"、"Cisco IOS Software" あるいはこれらに類似するシステム バナーによってデバイスで Cisco IOS ソフトウェアが稼働していることを確認できます。 その後ろにイメージ名が括弧の間に表示され、続いて "Version" と Cisco IOS ソフトウエア リリース名が表示されます。 他のシスコ デバイスでは、**show version** コマンドが存在しなかったり、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 15.2(4)M5、インストールされたイメージ名が C3900-UNIVERSALK9-M であるシスコ製品を示しています。

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), 15.2(4)M5, RELEASE SOFTWARE
(fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Fri 13-Sep-13 16:44 by prod_rel_team
```

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), 15.2(4)M5, RELEASE SOFTWARE
(fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Fri 13-Sep-13 16:44 by prod_rel_team
```

Cisco IOS ソフトウェア リリースの命名規則については、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

Cisco IOS XR ソフトウェアはこ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

Cisco IOSソフトウェアおよび Cisco IOS XE ソフトウェアの DHCPv6 サーバ 機能は特定のアドレス プールから DHCPv6 クライアントに IPv6 アドレス、プレフィックスおよび他の情報を割り当て、管理する DHCPv6 サーバ実装です。

Cisco IOSソフトウェアおよび Cisco IOS XE ソフトウェアの DHCP バージョン 6 （ DHCPv6 ）サーバ実装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。

脆弱性は形式が間違った DHCPv6 パケットの不適当な解析が原因です。 攻撃者は影響を受けたデバイスが処理される形式が間違った DHCPv6 パケットの送信によってこの脆弱性を不正利用する可能性があります。 エクスプロイトは攻撃者により影響を受けたデバイスのメモリリークおよび終局リロードを引き起こすことを可能にする可能性があります。

脆弱性は影響を受けた Cisco IOS または Cisco IOS XE デバイスが巧妙に細工された DHCPv6 パケットを処理するように試みるとき引き起こされます。 有効な DHCPv6 パケットはこの脆弱性を誘発しません。 Cisco IOSデバイスが転送する DHCPv6 パケットは（ たとえば、中継 DHCPv6 トラフィック ）この脆弱性を誘発しません。

パケットは両方ともリンク スコープ内のマルチキャスト アドレス ff02::1:2 （ All_DHCP_Relay_Agents_and_Servers に ）送信 し、DHCPv6 サーバのインターフェイス IPv6 ユニキャスト アドレスはこの脆弱性を誘発します。

この脆弱性は形式が間違った IPv6 パケットによってしか不正利用することができません。 IPバージョン 4 （IPv4）の DHCP バージョン 4 （DHCP）サーバで設定される Cisco IOSデバイスはこの脆弱性から影響を受けません。

この脆弱性は Cisco バグ ID CSCum90081 （ 登録ユーザのみ ）で文書化されています。 この脆弱性よくある脆弱性および公開（CVE） ID CVE-2014-3359 は割り当てられました。

回避策

この脆弱性に対する回避策はありません。

修正済みソフトウェア

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、応答および表記アーカイブを 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状況報告を検討するように勧告されます。

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。

Cisco IOS ソフトウェア

Cisco は顧客が Cisco IOSソフトウェアの脆弱性への公開を判別するのを助けるようにツールを提供しました。 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
- 2015 年 9 月組み込まれた書にすべての以前に公開された Cisco Security Advisory、特定のパブリケーション、またはすべての状況報告を含めることによってカスタマイズされた検索を作成して下さい

ツールは問い合わせられたソフトウェア リリースおよび各 Cisco Security Advisory のすべての脆弱性を解決する以前のリリースに影響を与える Cisco Security Advisory を識別します（「最初に」固定される）。 該当する場合、ツールはまたすべての表示された状況報告のすべての脆弱性を解決する最も早い可能性のあるリリースを戻します（「結合される最初に」固定される）。 Cisco IOSソフトウェア チェッカーを単に参照するか、または次のフィールドでこの組み込まれたパブリケーションの状況報告の何れかから影響を受けるかどうか判別するために 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文書で表われる脆弱性から影響を受けます。

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 リリース	First Fixed Release（修正された最初のリリース）	のすべてのアドバイザリーのための最初修正済みリリース 9月 2014 年の Cisco IOSソフトウェア Security Advisory 組み込まれたパブリケーション
2.1.x	脆弱性なし	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
2.2.x	脆弱性なし	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
2.3.x	脆弱性なし	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
2.4.x	脆弱性なし	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
2.5.x	脆弱性なし	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
2.6.x	脆弱性なし	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
3.1.xS	脆弱性なし	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
3.1.xSG	脆弱性なし	脆弱性なし
3.2.xS	脆弱性なし	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
3.2.xSE	脆弱性なし	脆弱性あり; 3.3.2SE に移行して下さい
3.2.xSG	脆弱性なし	脆弱性なし
3.2.xXO	脆弱性なし	脆弱性なし
3.2.xSQ	脆弱性なし	脆弱性なし
3.3.xS	脆弱性なし	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
3.3.xSE	脆弱性なし	3.3.2SE
3.3.xSG	脆弱性なし	脆弱性あり; 3.4.4SG またはそれ以降に移行して下さい。
3.3.xXO	脆弱性なし	3.3.1XO
3.3.xSQ	脆弱性なし	脆弱性なし
3.4.xS	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
3.4.xSG	脆弱性なし	3.4.4SG
3.4.xSQ	脆弱性なし	脆弱性なし
3.5.xE	脆弱性なし	3.5.2E

3.5.xS	脆弱性あり; 3.7.4S またはそれ以降に移行して下さい。	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
3.6.xE	脆弱性なし	脆弱性なし
3.6.xS	脆弱性あり; 3.7.4S またはそれ以降に移行して下さい	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
3.7.xE	脆弱性なし	脆弱性なし
3.7.xS	3.7.6S	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
3.8.xS	脆弱性あり; 3.10.4S またはそれ以降に移行して下さい。	脆弱性あり; 3.10.4S またはそれ以降に移行して下さい。
3.9.xS	脆弱性あり; 3.10.4S またはそれ以降に移行して下さい。	脆弱性あり; 3.10.4S またはそれ以降に移行して下さい。
3.10.xS	3.10.4S	3.10.4S
3.11.xS	脆弱性あり; 3.12S またはそれ以降に移行して下さい。	脆弱性あり; 3.12S またはそれ以降に移行して下さい。
3.12.xS	脆弱性なし	脆弱性なし
3.13.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 2014 年 9 月 Cisco IOSソフトウェア Security Advisory によって組み込まれる書で表われる脆弱性の何れかから影響を受けません。

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。

この脆弱性は内部テストの間に検出されました。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140924-dhcpv6

改訂履歴

リビジョン 1.0	2014-September-24	初回公開リリース

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。