Cisco IOSソフトウェア DHCP サービス拒否の脆弱性

High

アドバイザリーID : cisco-sa-20130925-dhcp

初公開日 : 2013-09-25 16:00

バージョン 1.0 : Final

CVSSスコア : 7.8

回避策 : Yes

Cisco バグ ID : CSCug31561

CVE-2013-5475

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 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。

脆弱性は巧妙に細工された DHCP パケットの解析の間に発生します。 攻撃者は有効に なる DHCPサーバか DHCPリレー機能がある影響を受けたデバイスへ巧妙に細工された DHCP 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。 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。回避策はこの脆弱性へありません。

このアドバイザリは、次のリンクより確認できます。
925-dhcp
注： 2013 年 9月 25 日、Cisco IOSソフトウェア Security Advisory によって組み込まれる書は 8 Cisco Security Advisory が含まれています。 すべてのアドバイザリは Cisco IOSソフトウェアの脆弱性に対処します。 各 Cisco IOSソフトウェア Security Advisory は正しい 2013 年 9 月のすべての Cisco IOSソフトウェア脆弱性はパブリケーションを組み込んだことアドバイザリ、また Cisco IOS ソフトウェア リリースで詳述される脆弱性を解決する Cisco IOS ソフトウェア リリースをリストします。

"Cisco Event Response: 半年ごと Cisco IOSソフトウェア Security Advisory は次のリンクの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_sep13.html

該当製品

修正済みソフトウェア

有効に なる DHCPサーバか DHCPリレー機能と影響を受けた 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。 DHCPサーバか DHCPリレー機能はデフォルトで有効に なりません。 DHCP クライアントで設定される 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 DHCPサーバで設定されるかどうか判別するために、 **提示 ip dhcp pool コマンドを**発行して下さい。

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 DHCPサーバ 機能が有効に なり、IP アドレスを機能する設定された プールは少なくとも 1 サブネットがあるので脆弱です:

```
Router#show ip dhcp pool

Pool test :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 192.168.1.1          192.168.1.1      - 192.168.1.254         0
```

Cisco IOSデバイスまたは Cisco IOS XE デバイスが DHCP リレー エージェントで設定されるかどうか判別するために、 **show run を**発行して下さい **| helper-address コマンドを含んで下さい**。

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 DHCP リレー エージェント 機能が有効に なるので出力される **ip helper-address** に基づいて脆弱、です:

```
Router#show ip dhcp pool
```

```
Pool test :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 192.168.1.1          192.168.1.1      - 192.168.1.254         0
```

Cisco 製品で稼働している Cisco IOS ソフトウェア リリースを確認するには、機器にログインし show version コマンドを実行してシステムバナーを表示させます。 "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 Cisco 機器では、 show version コマンドがない場合や、表示が異なる場合があります。

次の例は C3900-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 15.0(1)M1 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, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod_rel_teamRouter> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod_rel_team
```

Cisco IOS ソフトウエアのリリース命名規則の追加情報は以下のリンクの "White Paper: http://www.cisco.com/web/about/security/intelligence/ios-ref.html の Cisco IOS および NX-OS ソフトウェア レファレンスガイド」。

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。

改訂履歴

リビジョン 1.0	2013-September-25	初版リリース

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。