Cisco IOS および IOS XE ソフトウェアの DHCP におけるリモート コード実行の脆弱性

アドバイザリーID : cisco-sa-20170927-dhcp
初公開日 : 2017-09-27 16:00
最終更新日 : 2022-12-17 05:51
バージョン 1.3 : Final
CVSSスコア : 9.8
回避策 : No workarounds available
Cisco バグ ID : CSCsm45390 CSCuw77959

CVE-2017-12240

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 および Cisco IOS XE ソフトウェアの DHCP リレー サブシステムには、認証されていないリモート攻撃者が任意のコードを実行し、該当システムのフル コントロールを取得する可能性がある脆弱性が存在します。また、攻撃者は該当システムのリロードを引き起こし、その結果 DoS 状態が発生する可能性があります。

この脆弱性は、影響を受けるソフトウェアにおける DHCP リレー サブシステムのバッファ オーバーフロー条件に起因し、攻撃者は、巧妙に細工されたDHCPバージョン4(DHCPv4)パケットを該当システムに送信することにより、この脆弱性を不正利用する可能性があります。エクスプロイトが成功すると、任意のコードが実行され、影響を受けるシステムのフル コントロールを取得されるか、影響を受けるシステムがリロードされ、DoS 状態が生じ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-20170927-dhcp

このアドバイザリは、2017年9月27日に公開された13件の脆弱性に関する12件のシスコセキュリティアドバイザリを含むCisco IOSソフトウェアおよびIOS XEソフトウェアリリースのセキュリティアドバイザリバンドルの一部です。アドバイザリとリンクの一覧については、『Cisco Event Response: September 2017 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication』を参照してください。

該当製品

脆弱性のある製品

この脆弱性は、DHCP リレー エージェントとして設定され、Cisco IOS ソフトウェアまたは Cisco IOS XE ソフトウェアの脆弱性が存在するリリースを実行するシスコ デバイスに影響を与えます。

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。

DHCP リレー設定の確認

デバイスが DHCP リレー エージェントとして設定されているかどうかを判別するには、管理者がデバイスにログインして show running-config | include ip helper-address コマンドを CLI で使用します。

Cisco IOS ソフトウェアを実行し、DHCP サーバ アドレス 10.10.10.1 に DHCP パケットを転送する DHCP リレー エージェントとして設定されているデバイスでのコマンド出力は次のようになります。

<#root>

```
Router#
show running-config | include ip helper-address
ip helper-address  10.10.10.1Router#
```

デバイスが DHCP リレー エージェントとして設定されていない場合、show running-config | include ip helper-address コマンドを実行しても出力が返されません。

注：ケーブルモデム終端システム(CMTS)デバイスは、CLIでcable helper-addressコマンドを使用することにより、DHCPリレーエージェントとして有効になります。CMTS デバイスが DHCP リレー エージェントとして設定されているかどうかを判別するには、管理者がデバイスにログインして show running-config コマンドを使用します。 | には、CLI の cable helper-address コマンドが含まれます。デバイスが DHCP リレー エージェントとして設定されていない場合、コマンドは出力を返しません。

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。

次に、Cisco IOS ソフトウェア リリース 15.5(2)T1 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 C2951-UNIVERSALK9-M であるデバイスでのコマンド出力例を示します。

<#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 Software」、「Cisco IOS XE Software」などのテキストが表示されます。

次に、Cisco IOS XR ソフトウェア リリース 16.2.1 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 CAT3K_CAA-UNIVERSALK9-M であるデバイスでのコマンドの出力例を示します。

<#root>

```
ios-xe-device#
```

show version

```
Cisco IOS Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version Denali 16.2.1, REL
Technical Support: http://www.cisco.com/techsupport
```

```
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Sun 27-Mar-16 21:47 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。

詳細

DHCP は、TCP/IP ネットワーク上のホストに設定情報をダイナミックに渡すフレームワークを提供します。DHCP クライアントは、DHCP を使用して IP アドレスなどの設定パラメータを取得するインターネット ホストです。DHCP サーバは、指定したアドレス プールから DHCP クライアントに IP アドレスを割り当てて管理します。

DHCP リレー エージェントとは、クライアントとサーバ間で DHCP パケットを転送するホストです。このホストは、同一の物理サブネット上にないクライアントとサーバ間で要求および応答を転送するために使用されます。リレー エージェント転送は、IP ルータの通常の転送とは異なります。通常の転送では、IP データグラムがネットワーク間である程度透過的にスイッチングされます。その一方、リレー エージェントは DHCP メッセージを受信すると、新たに DHCP メッセージを生成し、別のインターフェイスを介して送信します。リレー エージェントはゲートウェイ IP アドレスを DHCP パケットの giaddr フィールドに設定し、パケットにリレー エージェント情報のオプション（Option 82）を追加して（設定されている場合）、DHCP サーバにパケットを転送します。リレー エージェントはその後、サーバから応答を受信し、その応答内容から Option 82 を削除した後、クライアントに転送します。

本セキュリティ アドバイザリに記載されている脆弱性は、影響を受けるソフトウェアの DHCP リレー サブシステムでバッファ オーバーフロー条件に起因します。攻撃者がこの脆弱性を不正利用するには、Cisco IOS または Cisco IOS XE ソフトウェアの脆弱性が存在するリリースが実行されていて、DHCP リレー エージェントとして設定されているシステムに対し、巧妙に細工した DHCPv4 パケットを送信する必要があります。この脆弱性の不正利用が可能なのは、DHCPv4 パケットが該当システムに送信された場合のみです。DHCP バージョン 6（DHCPv6）パケットで不正利用されることはありません。

不正利用に成功すると、任意のコードが実行され、該当システムが完全に掌握される危険性があります。また、攻撃者は該当システムのリロードを引き起こし、その結果 DoS 状態が発生する可

能性があります。

回避策

この脆弱性に対処する回避策はありません。

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。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.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。
https://www.cisco.com/c/en/us/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

リリースが、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かどうかを確認するには、Cisco.comのCisco IOS Software Checker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ソフトウェアリリース(たとえば、15.1(4)M2、3.13.8S)を入力します。

オン

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ソフトウェアリリースに応じて『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。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）は、2022 年 3 月に、この脆弱性のさらなるエクスプロイトが試みられたことを認識しました。これらの脆弱性が修正済みのソフトウェアリリースにアップグレードすることを、引き続き強くお勧めします。

出典

この脆弱性は内部テストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-dhcp

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.3	エクスプロイトに関する情報を更新。	不正利用事例と公式発表	Final	2022 年 12 月 16 日
1.2	Cisco IOS ソフトウェア チェッカー、OVAL、および CVRF に関する説明に、新しい修正リリースと脆弱性対策済みリリースに関する情報を追加。	脆弱性が存在する製品	Final	2018年2月12日
1.1	OVAL 定義と脆弱性アセスメント情報が更新され、CMTS デバイスへの対応が追加されました。	ヘッダーと脆弱な製品	Final	2017-9-29
1.0	初回公開リリース	—	Final	2017-9-27

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。