Cisco IOS および Cisco IOS XE ソフトウェアの DHCP バージョン 4 リレーにおけるヒープ オーバーフローによるサービス妨害（DoS）の脆弱性

アドバイザリーID : cisco-sa-20180328-dhcpr1
初公開日 : 2018-03-28 16:00
最終更新日 : 2022-12-15 22:19
バージョン 1.1 : Final
CVSSスコア : 8.6
回避策 : No workarounds available
Cisco バグ ID : CSCvg62730

CVE-2018-0172

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 ソフトウェアにおける DHCP Option 82 のカプセル化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影響を受けるデバイスのリロードを引き起こし、その結果、サービス妨害（DoS）状態が発生する可能性があります。

この脆弱性は、該当ソフトウェアがDHCPリレーエージェントからDHCPバージョン4(DHCPv4)パケットで受信したオプション82情報の入力検証を完了していないことに起因しています。攻撃者は、巧妙に細工された DHCPv4 パケットを該当デバイスに送信することによって、本脆弱性を不正利用する可能性があります。攻撃が成功すると、該当デバイスでヒープ オーバーフロー状態が引き起こされ、その結果デバイスがリロードして DoS 状態にな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-20180328-dhcpr1

このアドバイザリは、2018年3月28日に公開された22件の脆弱性に関する20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: March 2018 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、次のすべての条件を満たすシスコ製デバイスに影響を及ぼします。

- デバイスで脆弱性が存在する Cisco IOS ソフトウェア リリースまたは Cisco IOS XE ソフトウェア リリースを実行している。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。
- デバイスのインターフェイスが、DHCP リレー エージェントとして設定されている。
- デバイスまたはデバイスのインターフェイスで、DHCP リレー エージェント情報（Option 82 情報）を DHCP パケットに挿入するように設定されている。
- デバイスまたはデバイスのインターフェイスで、他の DHCP リレー エージェントから受け取った Option 82 情報をカプセル化するように設定されている。

DHCP リレー エージェント設定の確認

デバイスのインターフェイスが 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確認するには、管理者がデバイスにログインして CLI で show running-config | include ip helper-address コマンドを使用します。 | include ip helper-address コマンドを CLI で使用します。デバイスが Cisco cBR-8 コンバージド ブロードバンド ルータである場合は、CLI で代わりに show running-config | include cable helper-address 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。

コマンドにより出力が返される場合は、デバイスの 1 つ以上のインターフェイスが DHCP リレー エージェントとして設定されています。

以下に、show running-config | 次の例は、Cisco IOS ソフトウェアを実行するデバイスでの show running-config | include ip helper-address コマンドの出力結果を示します。このデバイスには、DHCP リレー エージェントとして機能し、DHCP パケットを DHCP サーバ アドレス 10.10.10.1 に転送するように設定されたインターフェイスがあります。

```
<#root>

Router#

show running-config | include ip helper-address
```

```
ip helper-address  10.10.10.1
Router#
```

show running-config | | include ip helper-address コマンド、または show running-config | | include cable helper-address コマンドを Cisco cBR-8 ルータで実行し、出力が返されない場合は、そのデバイスに DHCP リレー エージェントとして設定されているインターフェイスはありません。

Option 82 挿入サポートの確認

デバイスまたはデバイスのインターフェイスが Option 82 情報を DHCP パケットに挿入するように設定されているかどうかを確認するには、管理者がデバイスにログインして CLI で show running-config | | include ip dhcp relay information option コマンドを使用します。

コマンド出力に以下のいずれかが含まれている場合、デバイスは Option 82 情報を DHCP パケットに挿入するように設定されています。

- ip dhcp relay information option-insert：インターフェイス設定、DHCP リレー エージェントとして設定されているインターフェイスの下に表示される
- ip dhcp relay information option server-id-override：インターフェイス設定、DHCP リレー エージェントとして設定されているインターフェイスの下に表示される
- ip dhcp relay information option：グローバル コンフィギュレーション

以下に、show running-config | 次の例は、Cisco IOS ソフトウェアを実行しているデバイスで show running-config | include ip dhcp relay information option コマンドを実行した場合の出力を示します。このデバイスは、DHCP リレー エージェントとして機能し、Option 82 情報を DHCP パケットに挿入するように設定されたインターフェイスを持っています。

<#root>

```
Router#
```

show running-config | include ip dhcp relay information option

```
ip dhcp relay information option-insert
Router#
```

show running-config | | include ip dhcp relay information option コマンドで出力が返されない場合、デバイスのどのインターフェイスも、Option 82 情報を DHCP パケットに挿入するように設定されていません。

Option 82 カプセル化サポートの確認

デバイスまたはデバイスのインターフェイスが、他の DHCP リレー エージェントから受信した DHCP Option 82 情報をカプセル化するように設定されているかどうかを確認するには、管理者がデバイスにログインして CLI で show running-config | | include ip dhcp relay information policy.* encapsulate コマンドを使用します。

コマンド出力に以下のいずれかが含まれている場合、デバイスは受信した Option 82 情報をカプセル化するように設定されています。

- ip dhcp relay information policy-action encapsulate：インターフェイス設定、DHCP リレー エージェントとして設定されているインターフェイスの下に表示される
- ip dhcp relay information policy encapsulate：グローバル コンフィギュレーション

次の例は、Cisco IOS ソフトウェアを実行しているデバイスでのコマンド出力を示しています。このデバイスは、DHCP リレー エージェントとして機能し、他の DHCP リレー エージェントから受信した Option 82 情報をカプセル化するように設定されています。

```
<#root>

Router#

show running-config | include ip dhcp relay information policy.* encapsulate


ip dhcp relay information policy encapsulate
Router#
```

show running-config | | include ip dhcp relay information policy.* encapsulate コマンドで出力が返されない場合、デバイスもデバイスのインターフェイスも Option 82 をカプセル化するように設定されていません。

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、『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、『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

本脆弱性を不正利用するには、本アドバイザリの「脆弱性のある製品」セクションに記載されているすべての設定要件を満たすインターフェイス経由で受信したパケットを利用する必要があります。

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 リストからリリース（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。

Check

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

シスコは、本脆弱性を発見し、報告いただいた Tenable 社に謝意を表します。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-dhcpr1

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	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-DEC-15
1.0	初回公開リリース	—	Final	2018年3月28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。

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。