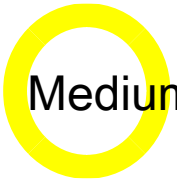
Cisco IOSおよびIOS XEソフトウェアのCisco Discovery Protocolにおける DoS脆弱性



アドバイザリーID : cisco-sa-20180926-cdp-dos
CVE-2018-15373
初公開日 : 2018-09-26 16:00
バージョン 1.0 : Final
CVSSスコア : 7.4
回避策 : No workarounds available
Cisco バグ ID : CSCvg54267

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Cisco Discovery Protocol(CDP)機能の実装における脆弱性により、認証されていない隣接する攻撃者が該当デバイスのメモリを枯渇させ、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、デバイスに送信されるCisco Discovery Protocol(CDP)パケットが高いレートで処理される際に、影響を受けるソフトウェアによる不適切なメモリ処理に起因します。攻撃者は、該当デバイスに高レートのCisco Discovery Protocolパケットを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。エクスプロイトに成功すると、攻撃者は該当デバイスのメモリを枯渇させ、DoS状態を引き起こす可能性があります。

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-20180926-cdp-dos

該当製品

脆弱性のある製品

この脆弱性は、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し、Cisco Discovery Protocolを使用するように設定されてい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。

Cisco Discovery Protocol 設定の確認

デバイスでCisco Discovery Protocolを使用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 cdp globalコマンドを使用します。デバイスがプロトコルを使用するように設定されている場合、コマンドの出力は次の例のようになります。

```
<#root>

CLI(config)#

show cdp global


Global CDP information:


CDP enabled globally

  Refresh time is 60 seconds
  Hold time is 180 seconds
  CDPv2 advertisements is enabled
  DeviceID TLV in System-Name(Default) Format
```

デバイスの特定のインターフェイスがCisco Discovery Protocolを使用するように設定されているかどうかを確認し、それらのインターフェイスに関する情報を表示するには、管理者がCLIでshow cdp interfaceコマンドを使用します。デバイスのいずれかのインターフェイスがプロトコルを使用するように設定されている場合、コマンドの出力には、プロトコルを使用するように設定されている各インターフェイスのプロトコルステータスとその他の情報が表示されます。

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

この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製品のみが、この脆弱性の影響を受けることが分かっています。

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。

セキュリティ侵害の痕跡

この脆弱性が不正利用されると、次の例に示すように、デバイスのCDPプロセスによって使用されるメモリ量が増加します。

```
<#root>

Switch#

show memory allocating totals | in CDP


0x7FF0A845688D

1045248800

  806519  CDP Protocol    (allocator: fh_fd_nd_cdp_add_notification_event)
0x7FF0A8456ADF

277598120

  806519  CDP Protocol    (allocator: fh_fd_nd_cdp_add_notification_event)
```

不正利用が停止すると、メモリは解放されます。

回避策

この脆弱性に対処する回避策はありません。ただし、管理者はデバイスによるCisco Discovery Protocolの使用を無効にすることができます。デバイスでのプロトコルの使用をグローバルに無効にするには、CLIでno cdp runコマンドを使用します。デバイスの特定のインターフェイスでのプロトコルの使用を無効にするには、CLIでno cdp enableコマンドを使用します。

管理者は、デバイスのCLIでshow cdp neighborsコマンドを使用して、デバイスでCisco Discovery Protocolの使用が有効になっているかどうかを最初に確認できます。コマンドの出力には、Cisco Discovery Protocolを使用して検出されたネイバーデバイスに関する詳細情報が表示されます。また、プロトコルの使用が無効になっている場合は、プロトコルの使用が有効になっていないことを示します。次に例を示します。

```
<#root>
```

```
Router#
show cdp neighbors

% CDP is not enabled

Router#
```

修正済みソフトウェア

該当するソフトウェアリリースと修正済みソフトウェアリリースの詳細については、Cisco IOSソフトウェアチェッカーを参照してください。

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。

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 など) を入力します。

Check

デフォルトでは、Cisco IOS ソフトウェアのチェックには、結果は、高セキュリティへの影響の評価 (サー) または重大な脆弱性にのみが含まれています。「中間」の SIR 脆弱性の結果を含めるには、Cisco.com の Cisco IOS ソフトウェア チェッカーを使用して、[Impact Rating] ドロップダウン リストの [中間 (Medium)] チェックボックスをオンにします。

不正利用事例と公式発表

Cisco Product Security Incident Response Team (PSIRT) 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やその公表を確認していません。

出典

この脆弱性は Cisco TAC サポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180926-cdp-dos

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2018 年 9 月 26 日

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。