Cisco IOS、IOS XE および IOS XR ソフトウェア Link Layer Discovery Protocol バッファオーバーフローの脆弱性

High

アドバイザリーID : cisco-sa-20180328-lldp
初公開日 : 2018-03-28 16:00
最終更新日 : 2022-12-15 22:19
バージョン 1.2 : Final
CVSSスコア : 8.8
回避策 : No workarounds available
Cisco バグ ID : CSCvd73487 CSCvd73664 CSCuo17183

CVE-2018-0175
CVE-2018-0167

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、Cisco IOS XE ソフトウェアおよび Cisco IOS XR ソフトウェアの Link Layer Discovery Protocol（LLDP）サブシステムの複数の脆弱性により、認証されていない隣接した攻撃者がサービス拒否（DoS）状態を引き起こすか、または影響を受けたデバイスの高度な特権の任意のコードを実行することを可能にする可能性があります。

これらの脆弱性の詳細については本アドバイザリの「詳細情報」セクションを参照してください。

シスコはこれら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。これら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-lldp

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

これらの脆弱性は、シスコ デバイスで Cisco IOS ソフトウェア、Cisco IOS XE ソフトウェア、Cisco IOS XR ソフトウェアの脆弱性が存在するリリースが実行され、LLDP を使用するように設定されている場合に影響をおよぼします。LLDP 機能のデフォルトでの状態は、プラットフォームおよびリリースにより異なります。

脆弱性が存在する Cisco IOS、IOS XE、IOS XR ソフトウェアのリリースについては、本アドバイザリの「修正済みソフトウェア」セクションを参照してください。

LLDP 設定の確認

デバイスが LLDP を使用するように設定されているかどうかを判断するには、管理者はデバイスにログインし、CLI で show lldp コマンドを使用します。デバイスが LLDP 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ようになります。

<#root>

```
Router>
show lldp


Global LLDP Information:
   Status: ACTIVE
   LLDP advertisements are sent every 30 seconds
   LLDP hold time advertised is 120 seconds
   LLDP interface reinitialisation delay is 2 seconds
```

LLDP がデバイスの特定のインターフェイスに対してのみ設定されている場合、管理者は CLI で show lldp interface コマンドを使用して、LLDP を使用するように設定されているインターフェイスを判別できます。

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。

Cisco IOS XR 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 XR 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 XR 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 XR Software」などのテキストが表示されます。また、システムイメージファイルには、デバイス上で実行されているシステムイメージファイルの場所と名前、ハードウェア製品の名前が表示されます。

次に、Cisco IOS XR ソフトウェア リリース 5.3.4 が実行されているデバイスでの show version コマンドの出力例を示します。

```
<#root>

RP/0/RSP0/CPU0:ASR9001#

show version

Wed Jan 24 01:32:32.751 EST

Cisco IOS XR Software, Version 5.3.4[Default]
Copyright (c) 2017 by Cisco Systems, Inc.

ROM: System Bootstrap, Version 2.04(20140227:092320) [ASR9K ROMMON],

ASR9001 uptime is 6 hours, 17 minutes
System image file is "bootflash:disk0/asr9k-os-mbi-5.3.4.sp4-1.0.0/0x100000/mbiasr9k-rp.vm"

cisco ASR9K Series (P4040) processor with 8388608K bytes of memory.
P4040 processor at 1500MHz, Revision 2.0
ASR-9001 Chassis
.
.
.
```

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、これらの脆弱性が 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

Cisco IOS ソフトウェア、Cisco IOS XE ソフトウェア、Cisco IOS XR ソフトウェアの LLDP サ

ブシステムにおける 2 件の脆弱性により、認証されていない隣接する攻撃者が DoS 状態を引き起こしたり、権限を昇格させて任意のコードを実行したりする可能性があります。

これらの脆弱性の詳細については、次のとおりです。

Link Layer Discovery Protocol バッファ オーバーフローの脆弱性

Cisco IOS ソフトウェア、Cisco IOS XE ソフトウェア、Cisco IOS XR ソフトウェアの LLDP サブシステム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 DoS 状態を引き起こしたり、権限を昇格させて任意のコードを実行したりする可能性があります。

本脆弱性は、不正な LLDP メッセージの不適切なエラー処理に起因します。影響を受けたデバイスのインターフェイスに直接接続されている攻撃者は、問題を引き起こすように設計された LLDP プロトコルデータユニット（PDU）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。成功すれば、攻撃に利用可能なバッファオーバーフロー状態が発生し、DoS 状態を引き起こしたり、攻撃者が高度な特権の任意のコードを実行する可能性があります。

この脆弱性のCommon Vulnerabilities and Exposures(CVE)IDはCVE-2018-0167です。

この脆弱性のSecurity Impact Rating(SIR)はHighです。

この脆弱性のCisco Bug IDは、CSCvd73487（Cisco IOSおよびIOS XEソフトウェア）および CSCuo17183（Cisco IOS XRソフトウェア）です。

Link Layer Discovery Protocol フォーマット文字列の脆弱性

Cisco IOS ソフトウェア、Cisco IOS XE ソフトウェアの LLDP サブシステム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 DoS 状態を引き起こしたり、権限を昇格させて任意のコードを実行したりする可能性があります。

この脆弱性は、LLDP メッセージにおける特定のフィールドの不適切な処理に起因します。攻撃者が、影響を受けるデバイスのインターフェイスに直接接続し、デバイスの不正利用の準備を意図した LLDP PDU を送信することにより、本脆弱性を不正利用する可能性があります。攻撃者は、影響を受けたデバイスの CLI で特定の show コマンドを、認証されたユーザーに受け入れられる必要があります。成功した場合、攻撃者が DoS 状態を引き起こす、または権限を昇格させて任意のコードを実行する可能性があります。

この脆弱性のCVE IDはCVE-2018-0175です。

この脆弱性のSIRはHighです。

この脆弱性のCisco Bug IDはCSCvd73664です。

回避策

これら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 XR ソフトウェア

次の表に、Cisco IOS XR ソフトウェアの主要なソフトウェア リリース トレインを示します。リリース トレインが本アドバイザリで説明されている脆弱性の影響を受けるかどうかと、影響を受ける場合の修正済みマイナー リリースの最初のものを示します。次の表に示すように、適切なリ

リースに移行する必要があります。

ソフトウェア トレイン	First Fixed Release（修正された最初のリリース）	推奨リリース
4.1	未修正 – 移行して下さい	5.3.4 への移行が必要
4.2	未修正 – 移行して下さい	5.3.4 への移行が必要
4.3	未修正 – 移行して下さい	5.3.4 への移行が必要
5.0	未修正 – 移行して下さい	5.3.4 への移行が必要
5.1	5.1.3	5.1.3
5.2	脆弱性なし	脆弱性なし
5.3	脆弱性なし	脆弱性なし
6.0	脆弱性なし	脆弱性なし
6.1	脆弱性なし	脆弱性なし

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

これらの脆弱性は、Cisco TAC のサポート案件の対応時に発見されました。

URL

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

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.2	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

バージョン	説明	セクション	ステータス	日付
1.1	複数のレガシーの Cisco IOS ソフトウェア イメージが脆弱でないことを示すようにメタデータを更新。	—	Final	2018年5月2日
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。