Cisco IOS および IOS XE ソフトウェア マルチキャストルーティング サービス拒否の脆弱性

High

アドバイザリーID : cisco-sa-20160928-msdp

初公開日 : 2016-09-28 16:00

バージョン 1.0 : Final

CVSSスコア : 7.8

回避策 : No workarounds available

Cisco バグ ID : CSCuy16399 CSCud36767

CVE-2016-6392

CVE-2016-6382

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 IOS XE ソフトウェアのマルチキャスト サブシステムの多重 脆弱点はリモート攻撃者非認証がサービス拒否（DoS）状態を作成するようにする可能性があります。 問題は IPv4 Multicast Source Discovery Protocol（MSDP）および IPv6 Protocol Independent Multicast にあります（PIM）。

最初の脆弱性（Cisco バグ ID CSCud36767（ 登録ユーザのみ ））設定された MSDP ピアから届く MSDP Source-Active（SA）メッセージの不十分なチェックが原因です。 デバイスの IPv4 アドレスにトラフィックを送信できる攻撃者は設計されているパケットの送信によって影響を受けたデバイスに問題を誘発するようにこの脆弱性を不正利用する可能性があります。 正常なエクスプロイトにより影響を受けたデバイスは再起動します可能性があります。

2つめの脆弱性（Cisco バグ ID CSCuy16399（ 登録ユーザのみ ））PIM レジスタ メッセージでカプセル化されるパケットの不十分なチェックが原因です。 PIM Rendezvous Point（RP）に形式が間違った IPv6 PIM レジスタパケットを送ることができる攻撃者は脆弱性を不正利用する可能性があります。 正常なエクスプロイトにより影響を受けたデバイスは再起動します可能性があります。

シスコはこれらの脆弱性に対処するソフトウェア アップデートを提供しています。 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。
928-msdp

このアドバイザリは、2016 年 9 月 28 日に公開された 11 件の脆弱性に関する 10 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。 このすべての脆弱性はセキュリティへの影響が「高」と評価されています。 これらのアドバイザリとリンクの一覧については、以下を参照してください。 シスコのイベント対応： Cisco IOS および IOS XE ソフトウェアに関するセキュリティ アドバイザリ公開資料 (半年刊、2016 年 9 月)

該当製品

脆弱性のある製品

これらの脆弱性は影響を受けたデバイスがドメイン間 MSDP または IPv6 マルチキャスト ルーティングのために設定されるときだけ該当する Cisco IOS および IOS XE ソフトウェア リリースを実行する Cisco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。

MSDP 機能がイネーブルになっているかどうか判別するために、 **show running-config を**使用して下さい **| ip msdp peer コマンドを含み、**出力を戻すことを確認して下さい。

次の例は MSDP がイネーブルの状態で Cisco IOSソフトウェアか Cisco IOS XE ソフトウェアを実行するデバイスを示したものです:

```
router#show running-config | include ip msdp peer
ip msdp peer 10.55.116.26
ip msdp peer 3.3.3.3 connect-source Loopback0
```

IPv6 マルチキャスト ルーティング機能がイネーブルになっているかどうか判別するために、**show running-config を**使用して下さい **| IPv6 マルチキャスト routing コマンドを含み、**出力を戻すことを確認して下さい。

次の例はイネーブルになっている IPv6 マルチキャスト ルーティングと Cisco IOSソフトウェアか Cisco IOS XE ソフトウェアを実行するデバイスを示したものです:

```
router#show running-config | include ipv6 multicast-routing
ipv6 multicast-routing
```

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、コマンドライン インターフェイス (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ます。その後ろには Cisco IOS ソフトウェアのリリース番号とリリース名も表示されます。 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することがあります。

次の例は、Cisco IOS ソフトウェア リリースが 15.5(2)T1 で、インストールされたイメージ名が *C2951-UNIVERSALK9-M* であるシスコ製品を示しています。

```
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ついては、以下を参照してください。ホワイト ペーパー： Cisco IOS および NX-OS ソフトウェア リファレンス ガイド

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 XE Software*」などのテキストが表示されます。

次に、Cisco IOS XE ソフトウェア リリース 3.16.1aS 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。

```
Router> show version
Cisco IOS XE Software, Version 03.16.01a.S - Extended Support Release
Cisco IOS Software, ASR1000 Software (PPC_LINUX_IOSD-ADVENTERPRISEK9-M), Version 15.5(3)S1a,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Wed 04-Nov-15 17:40 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ついては、以下を参照してください。ホワイト ペーパー： Cisco IOS および NX-OS ソフトウェア リファレンス ガイド

脆弱性を含んでいないことが確認された製品

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。

Cisco は Cisco IOS XR ソフトウェアおよび Cisco NX-OS ソフトウェアがこの状況報告に説明がある脆弱性から影響を受けないことを確認しました。

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 アップデートを提供しています。 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、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、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。
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.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、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シスコのサービス契約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購入先から入手できない場合は、Cisco Technical Assistance Center（TAC）に連絡してアップグレードを入手してください。
http://www.cisco.com/en/US/support/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

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できるよう、シスコでは Cisco IOS Software Checker ツールを提供しています。このツールにより、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、すべてのアドバイザリに記載されたすべて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含めたり、特定のアドバイザリのみ、または最新のバンドル資料から全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**、**3.1.4S** など）を入力します。

Cisco IOS XE ソフトウェア リリースと Cisco IOS ソフトウェア リリースのマッピングについては、Cisco IOS XE ソフトウェアのリリースに応じて「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）では、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とその公表は確認しておりません。

出典

これらの脆弱性は Cisco TAC によって顧客の例の調査の間に検出されました。

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-msdp

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2016 年 9 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。