Cisco IOS および IOS XE および Cisco Unified Communications Manager ソフトウェア Session Initiation Protocol（SIP）メモリリークの脆弱性

High

アドバイザリーID : cisco-sa-20160323-sip

初公開日 : 2016-03-23 18:30

最終更新日 : 2016-05-09 12:46

バージョン 1.1 : Final

CVSSスコア : 7.8

回避策 : No workarounds available

Cisco バグ ID : CSCuv39370 CSCuj23293

CVE-2016-1350

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、IOS XE および Cisco Unified Communications Manager ソフトウェアのセッション開始プロトコル（SIP）ゲートウェイ実装の脆弱性は非認証、リモート攻撃者により影響を受けたデバイスのメモリリークおよび終局リロードを引き起こすことを可能にする可能性があります。

脆弱性は形式が間違った SIP メッセージの不適当な処理が原因です。 攻撃者は影響を受けたデバイスが処理される形式が間違った SIP メッセージの送信によってこの脆弱性を不正利用する可能性があります。 エクスプロイトは攻撃者により影響を受けたデバイスのメモリリークおよび終局リロードを引き起こすことを可能にする可能性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。脆弱なデバイスの SIP をディセーブルにすること以外この脆弱性に対処する回避策がありません。

このアドバイザリは、次のリンクより確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160323-sip

この状況報告は、6 脆弱性を記述する 6 Cisco Security Advisory を含む Cisco IOS および IOS XE ソフトウェア Security Advisory によって組み込まれる書のリリースの 2016 年 3月 23 日一部です。 すべての脆弱性にあります「最高のセキュリティ への影響定格が」。 それらへの状況報告お

よびリンクの完全なリストに関しては、 Cisco イベント応答が表示されて下さい : 半年ごと Cisco IOS および IOS XE ソフトウェア Security Advisory によって組み込まれる書。

該当製品

SIP はインターネットのような IP ネットワークを渡る音声およびビデオ コールを管理するのに使用する普及したシグナリング プロトコルです。 SIP はコールセットアップおよび終了のすべての側面を処理します。 音声およびビデオは SIP が処理するが、プロトコルにコールセットアップおよび終了を必要とする他のアプリケーションを取り扱う柔軟性があるセッションのほとんどの一般的なタイプです。 SIP 呼出し シグナリングは根本的な転送 プロトコルとして UDP ポート 5060、TCPポート 5060、または TCPポート 5061 の Transport Layer Security （ TLS ）を使用できます。

脆弱性のある製品

この脆弱性は Cisco IOS、IOS XE、または SIP メッセージを処理するために設定される Cisco Unified Communications Manager ソフトウェアの脆弱なリリースを実行している Ciscoデバイスに影響を与えます。

Cisco IOS および IOS XE ソフトウェア リリースが脆弱である情報に関しては、この状況報告の「修正済みソフトウェア」セクションを参照して下さい。 Cisco IOS の最新のリリースおよび IOS XE ソフトウェアは SIP メッセージをデフォルトで処理しません。

次の Cisco Unified Communications Manager ソフトウェア リリースは脆弱です。 この アドバイザリに記載される 脆弱性を固定する最も早い Cisco Unified Communications ソフトウェア リリースについての情報に関しては、「修正済みソフトウェア」セクションを参照して下さい。

- Cisco Unified Communications Manager 8.x
- Cisco Unified Communications Manager 9.x
- Cisco Unified Communications Manager 10.x
- Cisco Unified Communications Manager 11.x

注: Cisco Unified Communications Manager リリース 8.x は終りのソフトウェア メンテナンス マイルストーンに 2015 年 7月 26 日達しました。 Cisco Unified Communications Manager 8.x リリースを使用している顧客は Cisco Unified Communications Manager のサポートされているリリースへのアップグレードの支援に関しては Cisco サポート チームに連絡する必要があります。

SIP が動作しているかどうか判別します

dial-peer configuration コマンドの発行によるダイヤル ピアを作成することは SIP メッセージを処理します Cisco IOSデバイスは SIP プロセスにより開始します。 さらに、Cisco Unified Communications Manager Express の複数の機能は、ephone のようなまた、自動的に設定さ

れる場合 SIP メッセージを処理し始めますデバイスは SIP プロセスにより開始します。 の例は影響を受けた Cisco IOS か IOS XE ソフトウェアコンフィギュレーション続きます:

```
!
 dial-peer voice <Voice dial-peer tag> pots
 ...
!
```

デバイスが SIP メッセージを処理します **dial peer コマンド**のために Cisco IOSデバイス設定を点検することに加えて管理者はまた **show processes を**使用できます **|** Cisco IOSソフトウェアが SIP メッセージを処理するプロセスを実行しているかどうか判別する **SIP** コマンドを **含んで下さい**。 次の例では、Cisco IOSデバイスが SIP メッセージを処理することをプロセス CCSIP_UDP_SOCKET の存在か CCSIP_TCP_SOCKET は示します:

```
Router#show processes | include SIP
149 Mwe 40F48254            4          1    400023108/24000  0 CCSIP_UDP_SOCKET
150 Mwe 40F48034            4          1    400023388/24000  0 CCSIP_TCP_SOCKET
```

注: Cisco IOSソフトウェアを実行する SIP メッセージを処理させ始めるデバイスがことができる複数の方法があるので管理者は特定の設定コマンドの存在に頼らないように助言されます。 その代り管理者が **show processes を**使用することが、推奨されます **|** デバイスが SIP メッセージを処理しているかどうか判別する **SIP** コマンドを **含んで下さい**。

この脆弱性は時 Cisco IOS、IOS XE、または Cisco Unified Communications Manager ソフトウェアプロセス形式が間違った SIP メッセージを実行しているデバイス 引き起こされます。 デバイスに向かうトラフィックだけ脆弱性を誘発できます; 中継 SIP トラフィックはエクスプロイト ベクトルではないです。 この脆弱性は IPv4 または IPv6 上の SIP と不正利用することができます。

注: SIP が TCP 転送に動作すれば、TCP 3 ウェイ ハンドシェイクはこの脆弱性を不正利用して必要です。

Cisco IOS か IOS XE ソフトウェア リリースの判別

、管理者はデバイスにログインどの Cisco IOS ソフトウェア リリースが Cisco製品で動作しているか判別し、**show version コマンドを**コマンドラインインターフェイスで使用し、次に現われるシステムバナーを参照するためにできます。 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。 カッコ内にイメージ名が表示され、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]

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。

セキュリティ侵害の痕跡

脆弱性が Cisco IOS または Cisco IOS XE ソフトウェアの脆弱なリリースを実行しているデバイスで不正利用されたかどうか判別するために、コマンドラインインターフェイスからの **show memory デバッグ リーク summary コマンドを**発行して下さい。

注: 脆弱性がずっと不正利用された on Cisco Unified Communications Manager ソフトウェアであるかどうか判別する方式がありません。

次の例はの出力に CCSIP_UDP_SOCKET に観察されたメモリリークがある脆弱な Cisco IOS をか IOS XE デバイスを示したものです:

```
Router#show memory debug leaks summary
Adding blocks for GD...

                I/O memory

Alloc PC        Size     Blocks      Bytes    What

                Processor memory

Alloc PC        Size     Blocks      Bytes    What

0x30302064 0000001024 0000000001 0000001024    *Init*
0x31931D28 0000001376 0000000001 0000001376    Connection
0x330F1E38 0000001184 0000000001 0000001184    *In-use Packet Header*
0x34F298D4 0000000040 0000000220 0000008800    CCSIP_UDP_SOCKET
0x34F298D4 0000000080 0000000106 0000008480    CCSIP_UDP_SOCKET
0x34F298D4 0000000084 0000000055 0000004620    CCSIP_UDP_SOCKET
```

```
0x34F298D4 0000000088 0000000079 0000006952    CCSIP_UDP_SOCKET
0x34F298D4 0000000092 0000000073 0000006716    CCSIP_UDP_SOCKET
```

注: show memory デバッグ リーク summary コマンドは CPU 中心であるかもしれ、慎重に使用する必要があります。

回避策

脆弱なデバイスの SIP をディセーブルにすること以外この脆弱性に対処する回避策がありません。

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場合は、http://www.cisco.com/go/psirt の Cisco Security Advisories and Responses アーカイブや後続のアドバイザリを参照して、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は新規リリースでも継続して適切なサポートが受けられることを確認してください。 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

顧客が Cisco IOS および IOS XE ソフトウェアの脆弱性への公開を判別するのを助けるために Cisco はツールを、特定のソフトウェア リリースおよび諮問それぞれに説明がある脆弱性を解決する以前のリリースに影響を与える Cisco Security Advisory を識別する Cisco IOSソフトウェア チェッカー提供します、（「最初に」固定される）。 該当する場合、ツールはまた識別されるすべての状況報告に説明があるすべての脆弱性を解決する以前のリリースを戻します（「結合される最初に」固定される）。

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

リリースがあらゆる公開された Cisco Security Advisory から影響を受けするかどうか判別するために、Cisco.com の Cisco IOSソフトウェア チェッカーを使用するか、または—次のフィールドで… Cisco IOS か IOS XE ソフトウェア リリースを—たとえば、**15.1(4)M2** か **3.01.4S** 入力して下さい:

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。

Cisco Unified Communications Manager ソフトウェア

Cisco UCM ソフトウェアメジャーリリース	First Fixed Release（修正された最初のリリース）
8.x	影響あり。 9.1(2)su4 またはそれ以降に移行して下さい
9.x	また 9.1(2.14900-14) と言われる 9.1(2)su4、
10.x	また 10.5(2.13900-12) と言われる 10.5(2)su3、
11.x	また 11.0(1.21900-11) と言われる 11.0(1)su1、

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エクスプロイト事例やその公表を確認していません。

出典

この脆弱性はサポート ケースの解決中に発見されました。

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160323-sip

改訂履歴

Version	Description	Section	Status	日付
1.1	ソフトウェアの CCO バージョンが含まれる調節された Cisco Unified Communications Manager ソフトウェア修正プログラム表。	修正済みソフトウェア	Final	2016-May-09
1.0	初回公開リリース		Interim	2016-March-23

利用規約