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 : Yes

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。

脆弱性は不正 な 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不正 な 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

このアドバイザリは、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」。 それらへのアドバイザリ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

修正済みソフトウェア

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下さい。 Cisco IOS および IOS XE ソフトウェアの最新 の リリースは 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。 影響を受けた Cisco IOS または IOS XE ソフトウェアコンフィギュレーションの例は続きます:

```
!
 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 **ダイヤルピアコマンド**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ために **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ために **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 不正 な 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引き起こすことができます; 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 転送するに動作すれば、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する場合、システムバナーは **Cisco Internetwork Operating System software** か **Cisco IOSソフトウェア**と同じようなテキストを表示する。 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。 いくつかの Ciscoデバイスは **show version コマンドを**サポートしませんし、別の出力を提供しないかもしれません。

次の例は、Cisco IOS ソフトウェア リリースが 15.5(2)T1、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 リリースのための指名および番号付与規則についての情報に関しては、白書を参照して下さい: Cisco IOS および NX-OS ソフトウェア レファレンスガイド。

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。

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	Initial public release.		Interim	2016-March-23

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。