Cisco IOSソフトウェア Session Initiation Protocol（SIP）サービス拒否の脆弱性

High

アドバイザリーID： cisco-sa-20110928-sip
初公開日： 2011-09-28 16:00
最終更新日： 2012-09-21 19:22
バージョン 1.1： Final
CVSSスコア： 7.8
回避策： Yes
Cisco バグ ID： CSCti48504 , CSCto88686 , CSCth03022

CVE-2011-2072
CVE-2011-0939
CVE-2011-3275

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

多重 脆弱点により非認証を可能にする可能性がある Cisco IOSソフトウェアのセッション開始プロトコル（SIP）実装におよび Cisco IOS XE ソフトウェア リモート攻撃者影響を受けたデバイスまたはシステム不安定な状態という結果に終るかもしれないトリガー メモリリークのリロードを引き起こすためにあります。 影響を受けたデバイスは開発可能であるためにこれらの脆弱性のための SIP メッセージを処理するように設定される必要があります。

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。 SIP を実行する必要があるデバイスのための回避策がありません; ただし、軽減は脆弱性への公開を制限して利用できます。このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-sip で掲示されます。

注: 2011 年 9月 28 日、Cisco IOSソフトウェア Security Advisory によって組み込まれる書は 10 Cisco Security Advisory が含まれています。 アドバイザリの 9 つは Cisco IOSソフトウェアの脆弱性に対処し、1 つのアドバイザリは Cisco Unified Communications Manager の脆弱性に対処します。 各アドバイザリは正しい 2011 年 9 月のすべての脆弱性はパブリケーションを組み込んだことアドバイザリ、また Cisco IOS ソフトウェア リリースで詳述される脆弱性を解決する Cisco IOS ソフトウェア リリースをリストします。

"Cisco Event Response: 半年ごと Cisco IOSソフトウェア Security Advisory は次のリンクのパブリケーションを」組み込みました:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep11.html

Cisco Unified Communications Manager はこのアドバイザリに説明がある脆弱性の 1 から影響を受けます。 別途の Cisco Security Advisory は次の位置で Cisco Unified Communications Manager に影響を与える脆弱性を表わすために公開されました:

928-cucm

該当製品

修正済みソフトウェア

Ciscoデバイスは SIP メッセージを処理するために設定される影響を受けた Cisco IOSソフトウェアおよび Cisco IOS XE ソフトウェア バージョンを実行しているとき影響を受けています。

Cisco IOSソフトウェアの最近のバージョンは SIP メッセージをデフォルトで処理しません。 **dial-peer voice** 設定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 内の複数の機能は、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。 影響を受けた設定の例は続きます:

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

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: 複数の方法があるので Cisco IOSソフトウェアを実行するデバイスはそれ推奨されますこと **show processes** SIP メッセージを処理し始めることができます **| SIP** コマンドをデバイスが特定の設定コマンドことをの存在に頼るかわりに SIP メッセージを処理しているかどうか判別するのに使用されています**含んで下さい。**

Cisco Unified Border Element イメージはまたこれらの脆弱性の 2 から影響を受けます。

注: Cisco Unified Border Element 機能（CUBE; 以前に）マルチサービスゲートウェイ プラットフォームを on Cisco 実行する特別な Cisco IOSソフトウェアイメージは Cisco マルチサービス IP-to-IP な ゲートウェイとして知られています。 それはインターワーキングに信号を送る

請求書を送ること、セキュリティ、コール アドミッション制御、Quality of Service ためにネットワーク間 インターフェイス ポイントを、および提供します。

Cisco 製品で稼働している Cisco IOS ソフトウェア リリースを確認するには、機器にログインし show version コマンドを実行してシステムバナーを表示させます。 "Internetwork Operating System Software"、"Cisco IOS Software" あるいはこれらに類似するシステム バナーによってデバイスで Cisco IOS ソフトウェアが稼働していることを確認できます。 その後ろにイメージ名が括弧の間に表示され、続いて "Version" と Cisco IOS ソフトウエア リリース名が表示されます。 他の Cisco 機器では、 show version コマンドがない場合や、表示が異なる場合があります。

次の例は C3900-UNIVERSALK9-M のインストール済みイメージ名前と Cisco IOS ソフトウェア リリース 15.0(1)M1 を実行している Cisco製品を指定したものです:

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1, RELEASE SOFTWARE
(fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod_rel_team

!--- output truncated
```

Cisco IOS ソフトウェア リリース 命名規則についてのその他の情報はで利用可能 な 白書 *Cisco IOS および NX-OS ソフトウェア レファレンスガイド*で利用できます: http://www.cisco.com/web/about/security/intelligence/ios-ref.html。

Cisco IOS XE ソフトウェアはこれらの脆弱性から影響を受けます。

注: Cisco Unified Communications Manager はこのアドバイザリに説明がある脆弱性の 1 から影響を受けます。 別途の Cisco Security Advisory は次の位置で Cisco Unified Communications Manager に影響を与える脆弱性を表わすために公開されました:

928-cucm

脆弱性を含んでいないことが確認された製品

SIP アプリケーション層ゲートウェイ（ALG）はこれらの脆弱性から、Cisco IOSソフトウェアの Cisco IOS Network Address Translation およびファイアウォール特性によって使用される、影響を受けません。

Cisco IOS XR ソフトウェアは、これらの脆弱性の影響を受けません。

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。

改訂履歴

リビジョ	2011-September-	アップデート IOS

ン 1.1	30	software 表によって組み込まれる書第 1 固定情報。
リビジョン 1.0	2011-September-28	初回公開リリース

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。