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-20120926-sip

初公開日： 2012-09-26 16:00

最終更新日： 2012-10-03 17:48

バージョン 1.1： Final

CVSSスコア： 7.8

回避策： Yes

Cisco バグ ID： CSCtj33003 , CSCtw84664 , CSCtw66721

CVE-2012-3949

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

影響を受けたデバイスをリロードするために引き起こすために非認証を可能にする可能性がある Cisco IOS XE ソフトウェアおよび Cisco IOSソフトウェアのセッション開始プロトコル（SIP）実装で存在 する脆弱性リモート攻撃者。 影響を受けたデバイスは開発可能であるためにこの脆弱性のための Session Description Protocol （SDP）のパススルーのための SIP メッセージを処理するために設定し。

シスコはこ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ました。 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、次のリンクより確認できます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-sip

注： 2012 年 9月 26 日、Cisco IOSソフトウェア Security Advisory によって組み込まれる書は 9 Cisco Security Advisory が含まれています。 アドバイザリの 8 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 Cisco IOSソフトウェア Security Advisory は正しい 2012 年 9 月のすべての Cisco IOSソフトウェア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_sep12.html

Cisco Unified Communications Manager はこのアドバイザリに記載される脆弱性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:

926-cucm

該当製品

修正済みソフトウェア

影響を受けた Cisco IOSソフトウェアを実行するか、または Cisco IOS XE ソフトウェアによってがバージョン 脆弱である 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時、そして Session Description Protocol （ SDP ）のパススルー 有効に なる時。

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。 以下は影響を受けた設定の例です:

```
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**。

デバイスは SIP が有効に なるときだけ、そして SDP パススルーがグローバル レベルかダイヤル ピア レベルで有効に なるとき影響を受けています。 グローバル レベルで、SDP パススル

ーは次の通り設定されます:

```
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
```

ダイヤル ピア レベルで、SDP パススルーは次の通り設定されます:

```
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
```

Cisco Unified Border Element（エンタープライズ）イメージはまたこの脆弱性から影響を受けます。

注: 以前に 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る Cisco Unified Border Element 機能（CUBE）は、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です。 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_teamRouter> 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
```

Cisco IOS ソフトウエアのリリース命名規則の追加情報は以下のリンクの "White Paper: http://www.cisco.com/web/about/security/intelligence/ios-ref.html の Cisco IOS および NX-OS ソフトウェア レファレンスガイド」。

Cisco IOS XE ソフトウェアはこ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記載される脆弱性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:
926-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 Unified Border Element（SP 版）はこの脆弱性から影響を受けません。
Cisco IOS XR ソフトウェアはこの脆弱性から影響を受けません。

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

リビジョン 1.1	2012-October-03	Cisco Unified Border Element（SP 版）が影響を受けていないこと明白にして下さい。
リビジョン 1.0	2012-September-26	Initial public release.

利用規約