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-20140326-sip **初公開日：** 2014-03-26 16:00 **最終更新日：** 2014-03-31 13:46 **バージョン 1.1：** Final **CVSSスコア：** 7.8 **回避策：** Yes **Cisco バグ ID：** CSCug45898	CVE-2014-2106

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ソフトウェアおよび Cisco IOS XE ソフトウェアのセッション開始プロトコル（SIP）実装の脆弱性はリモート攻撃者非認証により影響を受けたデバイスのリロードを引き起こすようにする可能性があります。 この脆弱性を不正利用するために、影響を受けたデバイスは SIP メッセージを処理するために設定する必要があります。 限られた Cisco IOSソフトウェアおよび Cisco IOS XE ソフトウェア リリースは影響を受けています。

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。

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、軽減はこの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-20140326-sip

注: 2014 年 3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 6 Cisco Security Advisory が含まれています。 すべてのアドバイザリは Cisco IOSソフトウェアの脆弱性に対処します。 各 Cisco IOSソフトウェア Security Advisory は正しい行進 2014 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。

個々のパブリケーション リンクは *Cisco イベント応答*にあります*: 半年ごと Cisco IOS*ソフトウ

エア Security Advisory は次のリンクで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_mar14.html

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ソフトウェアをか Cisco IOS XE ソフトウェアを実行しているとき影響を受けています。 次の Cisco IOSソフトウェアおよび Cisco IOS XE ソフトウェア リリースはこの脆弱性から影響を受けします:

- Cisco IOS ソフトウェア リリース 15.3(3)M および 15.3(3)M1
- Cisco IOS XE ソフトウェア リリース 3.10.0S、3.10.0aS および 3.10.1S1

Cisco IOSソフトウェアの最新 の リリースおよび Cisco 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。 **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: Cisco IOSソフトウェアか Cisco IOS XE 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それはこと **show processes** 推奨されます **| 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 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、Cisco IOS ソフトウェア リリースが 15.2(4)M5、インストールされたイメージ名が C3900-UNIVERSALK9-M であるシスコ製品を示しています。

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), 15.2(4)M5, RELEASE SOFTWARE
(fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Fri 13-Sep-13 16:44 by prod_rel_teamRouter> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), 15.2(4)M5, RELEASE SOFTWARE
(fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Fri 13-Sep-13 16:44 by prod_rel_team
```

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白書で利用できます: 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

Cisco Unified Communications Manager 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	2014-March-31	該当するリリースとして追加された Cisco IOS XE リリース 3.10.0aS。
リビジョン 1.0	2014-March-26	Initial public release.

利用規約