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-20140924-sip **初公開日 :** 2014-09-24 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 7.8 **回避策 :** No Workarounds available **Cisco バグ ID :** CSCul46586	CVE-2014-3360

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。

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-20140924-sip

注: 2014 年 9月 24 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。 すべての状況報告は Cisco IOSソフトウェアの脆弱性に対処します。 個々の公表資料へのリンクは、次のリンクにある「*シスコのイベント対応：半年ごと Cisco IOSソフトウェア 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_sep14.html

該当製品

脆弱性のある製品

Ciscoデバイスは影響を受けた Cisco IOSソフトウェアを実行するとき影響を受けていますまたは Cisco IOS XE ソフトウェアはリリースし、SIP メッセージを処理するために設定しました。 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コマンド **show udp を**使用することを推奨します **| 5060** および **show tcp 要約をすべて含んで下さい |** SIP ポートが開いているかどうか判別するために **5060|5061 を含んで下さい**。 デフォルトで、SIP は UDP か TCPポート 5060 で Transport Layer Security （ TLS ）が使用されるとき動作し、TCPポート 5061 で動作します。 コマンドの出力が空ではない場合、ポートは開いて、デバイスは次の例が説明するので、脆弱です:

```
Router# show udp | include 5060
 17     0.0.0.0             0 --any--          5060    0    0     11    0

Router# show tcp brief all | include 5060|5061
7F1277405E20  0.0.0.0.5061               *.*                          LISTEN
7F127BBE20D8  0.0.0.0.5060               *.*                          LISTEN
```

注: SIP またはセキュア SIP のためのポートが デフォルトから変更される場合、前例は使用中の新しいポートを参照する必要があります。

シスコ製品上で動作している Cisco IOS ソフトウェア リリースについては、管理者がデバイスにログインして **show version** コマンドを発行し、システム バナーを表示することで判別できます。 "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。 他のシスコ デバイスでは、**show version** コマンドが存在しなかったり、別の出力が表示されたりします。

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_team
```

```
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_team
```

Cisco IOS ソフトウェア リリースの命名規則については、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

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。

詳細

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する役割があります。 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 TLS を使用できます。

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。

脆弱性は特定の SIP メッセージの不正確な処理が原因です。 攻撃者は確立された コールの巧妙に細工された SIP メッセージを送信 するか、またはデバイスのリロードを誘発する、巧妙に細工された SIP メッセージを含むコールを開始することによってこの脆弱性を不正利用する可能性があります。 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 IPバージョン 4 （IPv4）または IP バージョン 6(IPv6) 上の SIP と通信プロトコル不正利用することができます。 この脆弱性は UDP トラフィック上の SIP か TCPトラフィック上の SIP と不正利用することができます。

この脆弱性は Cisco バグ ID CSCul46586 （ 登録ユーザのみ ）で文書化されています。 この脆弱性よくある脆弱性および公開（CVE） ID CVE-2014-3360 は割り当てられました。

回避策

Cisco IOSソフトウェアか Cisco IOS XE ソフトウェアを実行する影響を受けた Ciscoデバイスが VOIPサービスのために SIP を必要とする場合、SIP は無効である場合もないし対応策は見つかりません。 ユーザは脆弱性への公開の制限を助ける緩和技術を適用するように助言されます。 軽減は正規のデバイスだけ影響を受けたデバイスに接続するようにすることで構成されています。 効果を高めるために、軽減はネットワークエッジの antispoofing 手段とつなぐ必要があります。 SIP が転送 プロトコルとして UDP を使用できるのでこの操作が必要となります。

ネットワーク内の on Cisco 配置されたデバイスの場合もある追加軽減は次のリンクで利用可能の *Cisco IOSソフトウェア Session Initiation Protocol (SIP) 識別*する応用軽減情報ドキュメントガイドで利用でき *サービス拒否の脆弱性の軽減不正利用*、:
http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=35259

SIP リスニングポートを無効にすること

SIP がイネーブルになっているように要求しないデバイスに関しては最も簡単のおよびほとんどの有効な回避策はデバイスで処理する SIP を無効に することです。 Cisco IOSソフトウェアおよび Cisco IOS XE ソフトウェアのいくつかのリリースは管理者が次のコマンドで SIP を無効に することを可能にします:

```
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_team
```

警告： この回避策をメディア ゲートウェイ コントロール プロトコル (MGCP) または H.323 コールを処理しているデバイスに適用するとき、デバイスはアクティブ コールが処理されている間処理する SIP を停止しません。 このような状況では、この対応策はアクティブ コールが簡潔に停止することができるとき Maintenance ウィンドウの間に設定されるはずです。

show udp および **show tcp はすべての**コマンドを SIP UDP および TCP ポートがこの回避策をことを適用した後閉じることを確認するのに使用することができます **報告します。**

使用中の **show ip sockets** コマンドからの Cisco IOS ソフトウェア リリースによっては SIP がディセーブルにされるときまだ開いた SIP ポートを示すそれらへトラフィックを送信 するにより SIP プロセスは次のメッセージを表示します:

```
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_team
```

コントロール プレーン ポリシング

SIP サービスを提供する必要があるデバイスに関しては信頼できないソースからのデバイスに SIP トラフィックをブロックするのにコントロール プレーン ポリシング (CoPP) を使用することは可能性のあるです。 CoPP が特色にする Cisco IOSソフトウェアおよび Cisco IOS XE ソフトウェア リリース 12.0S、12.2SX、12.2S、12.3T、12.4、12.4T およびより新しいサポート。 デバイスに CoPP を設定して、管理プレーンとコントロール プレーンを保護し、既存のセキュリティ ポリシーおよび設定に従って、インフラストラクチャのデバイスに送信される承認されたトラフィックだけを明示的に許可することで、インフラストラクチャへの直接攻撃のリスクと効果を最小限に抑えることができます。 次の例は特定のネットワークコンフィギュレーションに適応させることができます:

```
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_team
```

注: SIP は転送 プロトコルとして UDP を使用できるので信頼された IP アドレスからのこれらのポートにアクセス制御アクセス・コントロール・リストをその割り当て通信バイパスするかもし

れない IPパケットの送信元アドレスをスプーフィングすることは可能性のあるです。 スプーフィングすることを防ぐのを助けるべき Unicast Reverse Path Forwarding についての情報は 知識 Unicast Reverse Path Forwarding で利用できます。

CoPP 先行する例では、一致する アクセス制御エントリは **割り当て**操作を用いる潜在的なエクスプロイト パケット **拒否**操作を一致するパケットはポリシーマップ **ドロップする** 機能から影響を受けないがこれらのパケットをポリシーマップ **ドロップする** 機能によって廃棄します。 CoPP 機能の設定および使用についてのその他の情報は *QoS ポリシングおよびシェーピングコンフュギュレーション ガイド*の コントロール プレーン ポリシング 実装 最良の方法および コントロール プレーン ポリシング章で利用できます。

修正済みソフトウェア

ソフトウェアアップグレードを検討するとき、顧客は Cisco Security Advisory、応答および表記アーカイブを http://www.cisco.com/go/psirt で参照し、公開および完全なアップグレード ソリューションを判別するためにそれに続く状況報告を検討するように勧告されます。

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が新規リリースで引き続き正しくサポートされていることを十分に確認してください。 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。

Cisco IOS ソフトウェア

Cisco は顧客が Cisco IOSソフトウェアの脆弱性への公開を判別するのを助けるようにツールを提供しました。 Cisco IOS Software Checker により、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を選択するか、ローカル システムからファイルをアップロードすることによって、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
- 2015 年 9 月組み込まれた書にすべての以前に公開された Cisco Security Advisory、特定のパブリケーション、またはすべての状況報告を含めることによってカスタマイズされた検索を作成して下さい

ツールは問い合わせられたソフトウェア リリースおよび各 Cisco Security Advisory のすべての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 を識別します（「最初に」固定される）。 該当する場合、ツールはまたすべての表示された状況報告のすべての脆弱性を解決する最も早い可能性のあるリリースを戻します（「結合される最初に」固定される）。 Cisco IOSソフトウェア チェッカーを単に参照するか、または次のフィールドでこの組み込まれたパブリケーションの状況報告の何れかから影響を受けるかどうか判別するために Cisco IOS ソフトウェア リリースを入力して下さい。

（入力例： 15.1(4)M2）

Cisco IOS XE ソフトウェア

Cisco IOS XE ソフトウェアはこの アドバイザリに記載される 脆弱性から影響を受けます。

Cisco IOS XE ソフトウェアリリース	First Fixed Release（修正された最初のリリース）	2014 年 9 月 Cisco IOSソフトウェア Security Advisory によって組み込まれる書のすべてのアドバイザリーのための最初修正済みリリース
2.1.x	脆弱性なし	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
2.2.x	脆弱性なし	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
2.3.x	脆弱性なし	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
2.4.x	脆弱性なし	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
2.5.x	脆弱性なし	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
2.6.x	脆弱性なし	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
3.1.xS	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
3.1.xSG	脆弱性なし	脆弱性なし
3.2.xS	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
3.2.xSE	脆弱性なし	脆弱性あり; 3.3.2SE に移行して下さい
3.2.xSG	脆弱性なし	脆弱性なし
3.2.xXO	脆弱性なし	脆弱性なし
3.2.xSQ	脆弱性なし	脆弱性なし
3.3.xS	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。

3.3.xSE	脆弱性なし	3.3.2SE
3.3.xSG	脆弱性なし	脆弱性あり; 3.4.4SG またはそれ以降に移行して下さい。
3.3.xXO	脆弱性なし	3.3.1XO
3.3.xSQ	脆弱性なし	脆弱性なし
3.4.xS	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
3.4.xSG	脆弱性なし	3.4.4SG
3.4.xSQ	脆弱性なし	脆弱性なし
3.5.xS	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
3.5.xE	脆弱性なし	3.5.2E
3.6.xS	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
3.6.xE	脆弱性なし	脆弱性なし
3.7.xS	3.7.6S	脆弱性あり; 3.7.6S またはそれ以降に移行して下さい。
3.7.xE	脆弱性なし	脆弱性なし
3.8.xS	脆弱性あり; 3.10.4S またはそれ以降に移行して下さい。	脆弱性あり; 3.10.4S またはそれ以降に移行して下さい。
3.9.xS	脆弱性あり; 3.10.4S またはそれ以降に移行して下さい。	脆弱性あり; 3.10.4S またはそれ以降に移行して下さい。
3.10.xS	3.10.4S	3.10.4S
3.11.xS	脆弱性あり; 3.12S またはそれ以降に移行して下さい。	脆弱性あり; 3.12S またはそれ以降に移行して下さい。
3.12.xS	脆弱性なし	脆弱性なし

3.13.xS	脆弱性なし	脆弱性なし

Cisco IOS ソフトウェア リリースへの Cisco IOS XE ソフトウェア リリースのマッピングについては、「 Cisco IOS XE 2 Release Notes」、「 Cisco IOS XE 3S Release Notes」、および「 Cisco IOS XE 3SG Release Notes」を参照してください。

Cisco IOS XR ソフトウェア

Cisco IOS XR ソフトウェアは 2014 年 9 月 Cisco IOSソフトウェア Security Advisory によって組み込まれる書で表われる脆弱性の何れかから影響を受けません。

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。

この脆弱性は内部 保全テストの間に検出されました。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140924-sip

改訂履歴

リビジョン 1.0	2014-September-24	初回公開リリース

利用規約