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-20090923-sip

初公開日 : 2009-09-23 16:00

バージョン 1.1 : Final

CVSSスコア : 7.8

回避策 : No Workarounds available

Cisco バグ ID : CSCsx25880

CVE-2009-2870

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 Unified Border Element 機能が有効に なる場合の非認証攻撃者が影響を受けたデバイスのサービス拒否（DoS）条件を引き起こすこと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）実装で存在 する脆弱性。

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に関しては回避策がありません; ただし、軽減は脆弱性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-20090923-sip で掲示されます。

注: 2009 年 9 月 23 日の IOS アドバイザリ バンドル公開には 11 件の Security Advisory が含まれています。 10 件のアドバイザリは Cisco IOS ソフトウェアの脆弱性に対処するもので、 1 件は Cisco Unified Communications Manager の脆弱性に対処するものです。 各アドバイザリには、そのアドバイザリで詳述された脆弱性を解決するリリースを記載しています。

"Cisco Event Response: Semiannual Cisco IOS Software Advisory Bundled Publication" の個々の公開リンクは次のリンク内に掲載されています:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep09.html

該当製品

この脆弱性は有効に なる SIP 音声 サービスを用いる実行するデバイス Cisco IOSソフトウェアだ

けに影響を与えます。

脆弱性のある製品

Cisco Unified Border Element が付いている 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 バージョンを実行する Ciscoデバイスは影響を受けています特色になります。 SIP および Cisco Unified Border Element 機能のために設定されない Cisco IOSデバイスはこの脆弱性から影響を受けません。

注: Cisco Unified Border Element 機能は（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）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 Unified Border Element 機能は **voice service voip コマンド**および許可**接続**サブコマンドを必要とします。 影響を受けた設定の例は次の通りです:

```
 voice service voip
   allow-connections from-type to to-type
...
!
```

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。コマンド **dial-peer voice 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、一度設定された ephone のようなまた、自動的にデバイスが SIP メッセージを処理し始めます SIP プロセスを開始します。 影響を受けた設定の例は次の通りです:

```
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コマンド 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 を含んで下さい。 次の例では、Cisco IOSデバイスが SIP メッセージを処理していることをプロセス **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
```

警告： 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 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。

以下の例は、Cisco 製品にて、IOSリリース 12.3(26) が稼動し、そのイメージ名が C2500-IS-L であることを示しています:

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 14:39 by dchih

!--- output truncated
```

次の例は C1841-ADVENTERPRISEK9-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 12.4(20)T 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, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE
SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

!--- output truncated
```

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: Cisco IOS Reference Guide" で確認できます: http://www.cisco.com/warp/public/620/1.html

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 NAT 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 XE ソフトウェアおよび 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。

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呼び出しを管理するのに

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 TCP （ 5060 ） ポート、または TLS （ 根本的な転送 プロトコルとして 5061 ） TCPポート UDP （ 5060 ） ポートを使用できます。

Cisco Unified Border Element は（ 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 ）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 Unified Border Element に関する詳細については次のリンクを参照して下さい:

http://www.cisco.com/en/US/products/sw/voicesw/ps5640/index.html

デバイスが Cisco Unified Border Element 機能がある Cisco IOSイメージを実行している場合の Cisco IOSソフトウェアの SIP 実装で存在 する DoS 脆弱性。 この脆弱性は一連の巧妙に細工された SIP メッセージの処理によって引き起こされます。

この脆弱性 Cisco バグ ID **CSCsx25880** （ 登録ユーザのみ ）で文書化されています、よくある脆弱性および公開（ CVE ） ID CVE-2009-2870 は割り当てられました。

回避策

影響を受けた Cisco IOS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従って、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。 軽減は正当 な デバイスだけルータ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アンチスプーフィング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ドキュメントガイド「 Cisco で利用できます加えました軽減情報を: 」次の位置で利用可能である Cisco Unified Communications Manager および Cisco IOSソフトウェアのサービス拒否の脆弱性の識別し、軽減不正利用、: http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20090923-voice。

ディセーブル SIP リスニングポート

SIP が有効に な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 をディセーブルにすることです。 次のコマンドとこれを達成する

Cisco IOSソフトウェア割り当て管理者のバージョン:

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE SOFTWARE
(fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

!--- output truncated
```

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 呼び出し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 接続、show tcp 要約すべて、および **show processes | SIP** 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**含んで下さい。**

使用中の Cisco IOS ソフトウェア バージョンによっては「show ip sockets」の出力はまだ開いた UDP ポート 5060 を示したものでがそのポートへ何かを送信 するにより SIP プロセスは次 の メッセージを出しました:

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE SOFTWARE
(fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

!--- output truncated
```

コントロール プレーン ポリシング

提供する必要があるデバイスに関しては SIP はそれをです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）を使用して可能性のある保守します。 Cisco IOS Release 12.0S、12.2SX、12.2S、12.3T、12.4、および 12.4T サポート CoPP 機能。 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。 次の例はネットワークに適応させることができます

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE SOFTWARE
(fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
```

```
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

!--- output truncated
```

警告： SIP は転送 プロトコルとして UDP を使用できるので容易に信頼された IP アドレスからのこれらのポートにアクセスコントロール アクセス· コントロール· リストをその割り当て通信敗北させるかもしれない送信側の IP 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。

CoPP 上の例では、「拒否」操作を一致するパケットは policy-map ドロップする 機能から（示されていない）影響を受けないが policy-map 「ドロップする」機能によって廃棄されるこれらのパケットの「割り当て」アクションの結果を用いる潜在的なエクスプロイト パケット一致する アクセス制御エントリ（ACE）その。 CoPP 機能の設定および使用のその他の情報は http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html および http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html で見つけることができます。

修正済みソフトウェア

ソフトウェアのアップグレードを検討する際には、http://www.cisco.com/go/psirt およびそれ以降のアドバイザリも参照して、起こりうる障害と完全なアップグレード ソリューションを判断してください

いずれの場合も、アップグレードする機器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しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。 情報に不明な点がある場合は、Cisco Technical Assistance Center（TAC）または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

Cisco IOS ソフトウェアの表（下掲）の各行には、Cisco IOS のリリース トレインが記載されています。 特定のリリース トレインに脆弱性がある場合は、修正を含む最初のリリース（および、それぞれの予想提供日）が表の「第 1 修正済みリリース」列に記載されます。 「推奨リリース」列には、このアドバイザリが作成された時点で発表されているすべての脆弱性の修正を含むリリースが記載されます。 特定の列に記されているリリースよりも古い（第 1 修正済みリリースより古い）トレインに含まれるリリースが稼働しているデバイスは脆弱であることが確認されています。 表の「推奨リリース」列に記載されているリリース、またはそれよりも新しいリリースにアップグレードすることを推奨します。

メジャー リリース	**修正済みリリースの入手可能性**	
Affected 12.0-Based Releases	First Fixed Release（修正された最初のリリース）	**推奨リリース**
該当する 12.0 基づいたリリースがありません。		
Affected 12.1-	First Fixed Release（修正された最初のリリース）	**推奨リリース**

Based Releases		
該当する 12.1 基づいたリリースがありません。		
Affected 12.2-Based Releases	**First Fixed Release（修正された最初のリリース）**	**推奨リリース**
該当する 12.2 基づいたリリースがありません。		
Affected 12.3-Based Releases	**First Fixed Release（修正された最初のリリース）**	**推奨リリース**
12.3	脆弱性なし	
12.3B	脆弱性なし	
12.3BC	脆弱性なし	
12.3BW	脆弱性なし	
12.3EU	脆弱性なし	
12.3JA	脆弱性なし	
12.3JEA	脆弱性なし	
12.3JEB	脆弱性なし	
12.3JEC	脆弱性なし	
12.3JK	脆弱性なし	
12.3JL	脆弱性なし	
12.3JX	脆弱性なし	
12.3T	脆弱性なし	
12.3TPC	脆弱性なし	
12.3VA	脆弱性なし	
12.3XA	脆弱性なし	
12.3XB	脆弱性なし	
12.3XC	脆弱性なし	
12.3XD	脆弱性なし	
12.3XE	脆弱性なし	
12.3XF	脆弱性なし	
12.3XG	脆弱性なし	
12.3XI	脆弱性なし	
12.3XJ	脆弱性なし	
12.3XK	脆弱性なし	
12.3XL	脆弱性なし	
12.3XQ	脆弱性なし	
12.3XR	脆弱性なし	
12.3XS	脆弱性なし	

12.3XU	脆弱性なし	
12.3XW	脆弱性なし	
12.3XX	脆弱性なし	
12.3XY	脆弱性なし	
12.3XZ	脆弱性なし	
12.3YA	脆弱性なし	
12.3YD	脆弱性なし	
12.3YF	脆弱性なし	
12.3YG	脆弱性なし	
12.3YH	脆弱性なし	
12.3YI	脆弱性なし	
12.3YJ	脆弱性なし	
12.3YK	Release prior to 12.3(11)YK3 are vulnerable， releases 12.3(11)YK3 and later are not vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.3YM	脆弱性なし	
12.3YQ	脆弱性なし	
12.3YS	脆弱性あり; first fixed in 12.4T 12.3(11)YS1 以前のリリースは脆弱ではないです。	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.3YT	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.3YU	脆弱性なし	

12.3YX	脆弱性なし	
12.3YZ	脆弱性なし	
12.3ZA	脆弱性なし	
Affected 12.4-Based Releases	**First Fixed Release（修正された最初のリリース）**	**推奨リリース**
12.4	脆弱性なし	
12.4GC	12.4(24)GC1	
12.4JA	脆弱性なし	
12.4JDA	脆弱性なし	
12.4JDC	脆弱性なし	
12.4JDD	脆弱性なし	
12.4JK	脆弱性なし	
12.4JL	脆弱性なし	
12.4JMA	脆弱性なし	
12.4JMB	脆弱性なし	
12.4JX	脆弱性なし	
12.4MD	脆弱性なし	
12.4MDA	脆弱性なし	
12.4MR	12.4(19)MR3	12.4(19)MR3
12.4SW	脆弱性なし	
12.4T	12.4(24)T1 12.4(15)T10 12.4(20)T3 12.4(22)T2	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009で利用可能
12.4XA	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009で利用可

		能
12.4XB	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009で利用可能
12.4XC	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009で利用可能
12.4XD	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009で利用可能
12.4XE	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009で利用可能
12.4XF	脆弱性なし	
12.4XG	脆弱性なし	
12.4XJ	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4

		12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.4XK	脆弱性なし	
12.4XL	12.4(15)XL5	
12.4XM	脆弱性あり; first fixed in 12.4T 12.4(15)XM 以前のリリースは脆弱ではないです。	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.4XN	脆弱性なし	
12.4XP	脆弱性あり; このアドバイザリの修正済みソフトウェア取得のセクションの手順ごとのサポート 組織に連絡して下さい	
12.4XQ	脆弱性なし	
12.4XR	脆弱性なし	
12.4XT	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.4XV	脆弱性あり; このアドバイザリの修正済みソフトウェア取得のセクションの手順ごとのサポート 組織に連絡して下さい	
12.4XW	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-

		OCT-2009で利用可能
12.4XY	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009で利用可能
12.4XZ	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009で利用可能
12.4YA	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009で利用可能
12.4YB	12.4(22)YB1	12.4(22)YB4
12.4YD	脆弱性なし	
12.4YE	脆弱性なし	

注: Cisco IOS XE か Cisco IOSソフトウェア モジュール性リリースはこの脆弱性から影響を受けしません。

不正利用事例と公式発表

Cisco PSIRT はこのアドバイザリに記載される脆弱性の公示か不正利用に気づいていません。

この脆弱性は内部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-20090923-sip

改訂履歴

リビジョン 1.0	2009-September-23	初版リリース

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。