

Cisco Unified Communications Manager 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-[CVE-20090923-cm](#) [CVE-2009-2864](#)
初公開日 : 2009-09-23 16:00
バージョン 1.0 : Final
CVSSスコア : [7.8](#)
回避策 : [Yes](#)
Cisco バグ ID :

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

以前 Cisco Unified CallManager だった Cisco Unified Communications Manager はセッション開始プロトコル (SIP) サービスでサービス拒否 (DoS) 脆弱性が含まれています。この脆弱性のエクスプロイトにより音声 サービスで割り込みを引き起こすかもしれません。

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。この脆弱性に対する回避策はありません。

このアドバイザリーは <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-cm> で掲示されます。

注: Cisco IOS[®] ソフトウェアはまたこのアドバイザリーに記載される脆弱性から影響を受けます。Cisco IOSソフトウェアのための関連アドバイザリーは <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-sip> で利用できます。

注: 2009 年 9 月 23 日の IOS アドバイザリー バンドル公開には 11 件の Security Advisory が含まれています。10 件のアドバイザリーは 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。各アドバイザリーには、そのアドバイザリー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

修正済みソフトウェア

次の Cisco Unified Communications Manager バージョンは影響を受けています:

- 5.1(3g) 以前の Cisco Unified Communications Manager 5.x バージョン
- Cisco Unified Communications Manager 6.x バージョン前の 6.1(4)
- 7.0(2a)su1 以前の Cisco Unified Communications Manager 7.0.x バージョン
- Cisco Unified Communications Manager 7.1.x バージョン前の 7.1(2)

Cisco Unified CallManagerのバージョン 4.x はこの脆弱性から影響を受けません。Cisco Unified Communications Manager バージョン 5.x、6.x および 7.x を稼働しているシステムの管理者は Cisco Unified Communications Manager 管理インターフェイスのメイン ページの表示によってソフトウェア バージョンを判別できます。ソフトウェア バージョンはまたコマンドラインインターフェイスによって **show version** アクティブなコマンドを実行することによって判別することができます。

SIP トランクは Cisco Unified CallManager Server が TCP および UDP ポート 5060 および TCP/5061 の SIP メッセージを聞き取り始めることができるように設定する必要があります。ただし、Cisco Unified Communications Manager バージョン 5.x および それ以降で、呼出しシグナリング プロトコルとして SIP の使用はデフォルトで有効になり、無効である場合もありません。

Cisco IOSソフトウェアはまたこの脆弱性から影響を受けますが、異なる Cisco バグ ID と関連付けられます。Cisco IOSソフトウェアのためのコンパニオン Security Advisory は利用できますで: <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-sip>

脆弱性を含んでいないことが確認された製品

Cisco Unified CallManagerのバージョン 4.x はこの脆弱性から影響を受けません。Cisco IOSソフトウェアを除いて、その他のCisco製品は現在この脆弱性から影響を受けるために知られていません。

改訂履歴

リビジョン 1.0	2009-September-23	初版リリース
--------------	-------------------	--------

利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザーの記述内容に関して情報配信の URL を省略し、単独の転載や意識を施した場合、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。