Cisco Unified Communications Manager Session Initiation ProtocolのDoS脆弱性

アドバイザリーID : cisco-sa-20080924-cucm
初公開日 : 2008-09-24 16:00
バージョン 1.1 : Final
CVSSスコア : 7.1
回避策 : No Workarounds available
Cisco バグ ID :

CVE-2008-3800

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 Communications Manager（旧Cisco Unified CallManager）には、Session Initiation Protocol(SIP)サービスに関するサービス拒否(DoS)の脆弱性が2つ存在します。これらの脆弱性の不正利用により、音声サービスの中断が引き起こされる可能性があります。

シスコは、これら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する予定です。修正済みソフトウェアが入手可能になり次第、このアドバイザリは更新されます。これらの脆弱性に対する回避策はありません。

注： Cisco IOSソフトウェアも、このアドバイザリに記載された脆弱性の影響を受けます。Cisco IOSソフトウェアに関するアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-sipで入手できます。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-cucm で公開されています。

該当製品

このドキュメントで説明されている脆弱性は、Cisco Unified Communications Managerに適用されます。

脆弱性のある製品

次のバージョンのCisco Unified Communications Managerが影響を受けます。

- 4.1.3SR8よりも前のCisco Unified CallManager 4.1バージョン
- 4.2(3)SR4bよりも前のCisco Unified CallManager 4.2バージョン
- 4.3(2)SR1aよりも前のCisco Unified CallManager 4.3バージョン
- 5.1(3d)より前のCisco Unified Communications Manager 5.xバージョン
- 6.1(2)su1より前のCisco Unified Communications Manager 6.xバージョン

Cisco Unified CallManagerバージョン4.xを実行しているシステムの管理者は、Cisco Unified Communications Manager AdministrationインターフェイスでHelp > About Cisco Unified CallManagerの順に選択し、Detailsボタンを選択することで、ソフトウェアバージョンを確認できます。

Cisco Unified Communications Managerバージョン5.xおよび6.xを実行しているシステムの管理者は、Cisco Unified Communications Manager Administrationインターフェイスのメインページを表示してソフトウェアバージョンを確認できます。ソフトウェアのバージョンは、コマンドラインインターフェイスでshow version activeコマンドを実行して確認することもできます。

Cisco Unified CallManagerバージョン4.xでは、コールシグナリングプロトコルとしてのSIPの使用はデフォルトで無効になっています。Cisco Unified CallManagerサーバがTCPおよびUDPポート5060と5061でSIPメッセージのリスニングを開始するには、SIPトランクを設定する必要があります。

Cisco Unified Communications Managerバージョン5.x以降では、コールシグナリングプロトコルとしてのSIPの使用は、Cisco Unified Communications Managerでデフォルトで有効になっており、無効にすることはできません。

Cisco IOSソフトウェアもこれらの脆弱性の影響を受けますが、別のCisco Bug IDで追跡されています。Cisco IOSソフトウェアに関するセキュリティアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-sipで入手できます。

脆弱性を含んでいないことが確認された製品

Cisco IOSソフトウェアを除き、このアドバイザリに記載された問題の脆弱性を含むシスコ製品は現在確認されていません。

Cisco Unified Communications Managerバージョン7.xはこれらの脆弱性の影響を受けません。

Cisco Unified CallManagerバージョン4.xは、SIPトランクが設定されていない場合、これらの脆弱性の影響を受けません。

詳細

Cisco Unified Communications Managerは、Cisco IP Telephonyソリューションのコール処理コン

ポーネントであり、企業のテレフォニー機能を、IP電話、メディア処理デバイス、Voice-over-IP(VoIP)ゲートウェイ、マルチメディアアプリケーションなどのパケットテレフォニーネットワークデバイスに拡張します。

SIPは、インターネットなどのIPネットワークを介した音声およびビデオコールの管理に使用される一般的なシグナリングプロトコルです。SIPは、コールのセットアップと終了のすべての側面を処理する役割を担います。SIPで処理される最も一般的なセッションタイプは音声とビデオですが、このプロトコルは、コールのセットアップと終了を必要とする他のアプリケーションにも柔軟に対応します。SIPコールシグナリングでは、基本のトランスポートプロトコルとしてUDP（ポート5060）、TCP（ポート5060）、またはTLS（TCPポート5061）を使用できます。

Cisco Unified Communications ManagerのSIP実装には、2つのDoS脆弱性が存在します。これらの脆弱性は、特定の有効なSIPメッセージの処理中にトリガーされ、Cisco Unified Communications Managerのメインプロセスのリロードにつながる可能性があります。

Cisco Unified CallManagerバージョン4.xでは、SIPトランクが設定されていない限り、SIPはデフォルトで有効になっていません。Cisco Unified Communications Managerバージョン5.x以降では、SIPがデフォルトで有効になっており、無効にすることはできません。

脆弱性は、次のCisco Bug IDで追跡されています。

- CSCsu38644(登録ユーザ専用)、CVE IDとしてCVE-2008-3800を割り当て
- CSCsm46064(登録ユーザ専用)、CVE IDとしてCVE-2008-3801を割り当て

回避策

これらの脆弱性に対する回避策はありません。

スクリーニングデバイスにフィルタリングを実装することで、脆弱性を緩和できます。Cisco Unified Communications ManagerサーバへのSIPアクセスを必要とするネットワークからのみ、ポート5060および5061へのTCP/UDPアクセスを許可します。

Cisco Unified Communications ManagerがSIPサービスを提供する必要がない場合は、Cisco Unified Communications ManagerがSIPメッセージをリッスンするポートを非標準ポートに移動できます。ポートをデフォルト値から変更するには、Cisco Unified CallManager Administration Webインターフェイスにログインし、System > Cisco Unified CMの順に選択して、適切なCisco Unified Communications Managerを見つけ、SIP Phone PortフィールドとSIP Phone Secure Portフィールドを非標準ポートに変更して、Saveをクリックします。SIP Phone Port（デフォルトでは5060）は、Cisco Unified Communications Managerが通常のSIPメッセージをリッスンするTCPポートとUDPポートを指し、SIP Phone Secure Port（デフォルトでは5061）は、Cisco Unified Communications ManagerがSIP over TLSメッセージをリッスンするTCPポートとUDPポートを指します。この手順の詳細については、『Cisco Unified Communications Managerアドミニストレーションガイド』(http://www.cisco.com/en/US/docs/voice_ip_comm/cucmbe/admin/7_0_1/ccmcfg/b02ccm.html#wp105751

「Updating a Cisco Unified Communications Manager」セクションを参照してください。

注：SIPポートの変更を有効にするには、Cisco CallManagerサービスを再起動する必要があります。これを行う方法については、
http://www.cisco.com/en/US/docs/voice_ip_comm/cucmbe/admin/7_0_1/ccmcfg/b03dpi.html#wp1075124
「Restarting the Cisco CallManager Service」を参照してください。

ネットワーク内のCiscoデバイスに適用可能な他の緩和策については、このアドバイザリに関連するCisco適用対応策速報
(https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20080924-sip)を参照してください。

修正済みソフトウェア

アップグレードを検討する場合は、http://www.cisco.com/go/psirt と後続のアドバイザリも参照して、問題の解決状況と完全なアップグレード ソリューションを確認してください。

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。

メジャー リリース	First Fixed Release（修正された最初のリリース）	推奨リリース
4.1.x	4.1(3)SR8	4.1(3)SR8a
4.2.x	4.2(3)SR4b	4.2(3)SR4b
4.3.x	4.3(2)SR1a	4.3(2)SR1b
5.1.x	5.1(3d)	5.1(3e)
6.1.x	6.1(2)SU1	6.1(3b)SU1

Cisco Unified Communications Managerソフトウェアのダウンロード

Cisco Unified Communications Managerソフトウェアをダウンロードするには、cisco.comの

Software Center(https://sec.cloudapps.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240)のVoice Software Downloadsセクションに移動し、IP Telephony > Call Control > Cisco Unified Communications Manager(CallManager)に移動して、適切なバージョンのCisco Unified Communications Managerを選択します。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco PSIRT では、本アドバイザリに記載されている脆弱性の不正利用事例やその公表は確認しておりません。

これらの脆弱性は、シスコの社内テストおよびお客様からのサービスリクエストの処理中に発見されたものです。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-cucm

改訂履歴

リビジョン 1.1	2009年4月9日	修正済みソフトウェアの表を更新し、修正済みソフトウェアの可用性と現在の推奨リリースを示しました。アドバイザリのステータスを暫定から最終に変更。
リビジョン 1.0	2008年9月24日	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。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。