Cisco Security Advisory: Cisco Unified Communications Manager Session Initiation Protocol Denial of Service Vulnerability

Advisory ID: cisco-sa-20090923-cm

http://www.cisco.com/warp/public/707/cisco-sa-20090923-cm.shtml

本翻訳は、原文の機械翻訳後に技術者が簡易レビューをしたものです。 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。

Revision 1.0

For Public Release 2009 September 23 1600 UTC (GMT)

目次

要約

Cisco Unified Communications Manager (旧名称 Cisco Unified CallManager) の Session Initiation Protocol (SIP) サービスには、サービス拒否 (DoS) 脆弱性が存在します。 こ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。

Cisco はこの脆弱性に対処する無償のソフト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。

このアドバイザリは以下に掲載されます:
http://www.cisco.com/JP/support/public/ht/security/107/1071758/cisco-sa-20090923-cm-j.shtml

注: Cisco IOS ソフトウェアもこのアドバイザリに記載される脆弱性の影響を受けます。 Cisco

IOS ソフトウェアの関連アドバイザリは、以下で参照できます:
http://www.cisco.com/warp/public/707/cisco-sa-20090923-sip.shtml

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。

個々の公開リンクは以下のリンクにある "Cisco Event Response: Semiannual Cisco IOS Software Advisory Bundled Publication" 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

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

脆弱性のある製品

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

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

Cisco Unified CallManager versions 4.x は、この脆弱性の影響を受けません。 Cisco Unified Communications Manager バージョン 5.x, 6.x および 7.x が稼動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、コマンドラインインターフェイスで **show version active** コマンドを実行することによっても判別することができます。

SIP トランクが設定され、Cisco Unified CallManager server が TCP および UDP ポート 5060 と TCP ポート 5061 をリスニングするようにしてある必要があります。 しかし、Cisco Unified Communications Manager バージョン 5.x 以降では、コールシグナリングのプロトコルとして SIP の使用がデフォルトで有効になり、無効にすることができません。

Cisco IOS ソフトウェアもこの脆弱性の影響を受けますが、異なる Cisco Bug ID と関連付けられます。 Cisco IOS ソフトウェアの 関連 Security Advisory は以下のリンクから入手できます:
http://www.cisco.com/warp/public/707/cisco-sa-20090923-sip.shtml

脆弱性が存在しない製品

Cisco Unified CallManager バージョン 4.x は、この脆弱性の影響を受けません。 Cisco IOS ソフトウェアを除いて、この脆弱性の影響を受けるその他の Cisco 製品は現在のところ確認されていません。

詳細情報

Cisco Unified Communications Manager は、IP Phone、メディア処理デバイス、voice-over-IP ゲートウェイ および マルチメディアアプリケーションのような パケットテレフォニーネットワークデバイスに、エンタープライズ テレフォニー機能を拡張する Cisco IP Telephony ソリューションの コール処理コンポーネントです。

SIP は、インターネットのような IP ネットワークを経由する音声とビデオコールを管理するのに使用される、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 が処理する最も一般的なタイプのセッションですが、SIP プロトコルは、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にも適用できる柔軟性があります。 SIP コール シグナリングは、トランスポートプロトコルとして、UDP (port 5060)、TCP (port 5060)または Transport Layer Security (TLS; TCP port 5061) を使用できます。

DoS 脆弱性が、Cisco Unified Communications Manager の SIP 実装に存在します。 この脆弱性は、Cisco Unified Communications Manager が巧妙に細工された SIP メッセージを処理する際に引き起こされます。 この脆弱性の不正利用により、Cisco Unified Communications Manager の主プロセスのリロードを引き起こすことができます。

この脆弱性は Cisco Bug ID CSCsz95423 (登録ユーザのみ) として文書化され、Common Vulnerabilities and Exposures (CVE) ID として CVE-2009-2864 が割り当てられています。

脆弱性スコア詳細

Cisco はこのアドバイザリでの脆弱性に対して Common Vulnerability Scoring System (CVSS) に基づいたスコアを提供しています。 このセキュリティアドバイザリでの CVSS スコアは CVSS version 2.0 に基づいています。

CVSSは、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する手助けとなる標準ベースの評価法です。

Cisco は基本評価スコア (Base Score) および現状評価スコア (Temporal Score) を提供いたします。 お客様はこれらを用いて環境評価スコア (Environmental Score) を算出し、 個々のネットワークにおける脆弱性の影響度を導き出すことができます。

Cisco は以下の URL にて CVSS に関する FAQ を提供しています。

http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

また Cisco は個々のネットワークにおける環境影響度を算出する CVSS 計算ツールを以下の URL にて提供しています。

http://intellishield.cisco.com/security/alertmanager/cvss

CSCsz95423 - Crafted SIP packet may cause CM process to crash Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

このアドバイザリで説明された脆弱性の不正利用に成功すると、Cisco Unified Communications Manager プロセスのリロードが発生し、結果として Voice サービスの中断が引き起こされます。

ソフトウエアバージョン及び修正

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、本アドバイザリ以降に公開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。 情報が不明確な場合は、Cisco Technical Assistance Center (TAC) もしくは契約している保守会社にお問い合せください。

次のテーブルはこの脆弱性のための最初の修正済みソフトウェアリリースが含まれています。 特定のリリースで First Fixed Version より前のバージョンを実行するデバイスには脆弱性が存在します。

Release	First Fixed Version
4.x	Not Vulnerable
5.x	5.1(3g)
6.x	6.1(4)
7.0.x	7.0(2a)su1
7.1.x	7.1(2)

回避策

こ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でフィルタリングを設定し、ポート 5060 への TCP/UDP アクセスとポート 5061への TCP アクセスの許可を、Cisco Unified Communications Manager サーバーへの SIP アクセスが必要なネットワークからのみに制限することで、この脆弱性を緩和することができます。

Cisco Unified Communications Manager が SIP サービスを提供する必要がない場合、管理者は Cisco Unified Communications Manager がリスニングする SIP メッセージのポートを非標準の値に設定できます。 ポートをデフォルト値からを変更するには、次の指示に従って下さい:

ステップ 1 Cisco Unified CallManager Administration の web インターフェイスにログインします

ステップ 2 System > Cisco Unified CM へ移動し、適切な Cisco Unified Communications Manager を選択します。

ステップ 3 SIP Phone Port と **SIP Phone Secure Port** のフィールドを非標準ポートへの変更し、**Save** をクリックします。

SIP Phone Port は、Cisco Unified Communications Manager が、標準の SIP メッセージをリスニングするTCP/UDP ポートでデフォルトは 5060、**SIP Phone Secure Port** は、Cisco Unified Communications Manager が、SIP over TLS messages をリスニングする TCP ポートでデフォルトは 5061 です。 この手順についてのその他の情報に関しては、"Cisco Unified Communications Manager Administration Guide" の "Updating a Cisco Unified Communications Manager" セクション http://www.cisco.com/en/US/docs/voice_ip_comm/cucmbe/admin/7_0_1/ccmcfg/b02ccm.html#wp1057513 を参照して下さい。

注：SIP のポートの変更を有効にするには、Cisco CallManager サービスのリスタートが必要です。 サービスをリスタートする方法の情報に関しては、"Restarting the Cisco CallManager Service" セクション http://www.cisco.com/en/US/docs/voice_ip_comm/cucmbe/admin/7_0_1/ccmcfg/b03dpi.html#wp1075124 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対応策は、このアドバイザリの付属ドキュメント "Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Denial of Service Vulnerabilities in Cisco Unified Communications Manager and Cisco IOS Software" に記載されており、以下の口ケーションから入手できます。: http://www.cisco.com/warp/public/707/cisco-amb-20090923-voice.shtml

修正済みソフトウェアの取得

Cisco はこれらの脆弱性に対応するための無償ソフトウェア アップデートを提供しています。 ソ

フトウェアの導入を行う前にお客様のメンテナンスプロバイダーにご相談いただくか、 ソフトウェアのフィーチャーセットの互換性および お客様のネットワーク環境に特有の問題に関してご確認下さい。

お客様がインストールしたり、サポートを受けたりできるのは、 ご購入いただいたフィーチャーセットに対してのみとなります。 そのようなソフトウェア アップグレードをインストール、ダウンロード、 アクセスまたはその他の方法で使用した場合、お客様は http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載の Cisco のソフトウェア ライセンスの条項または、 Cisco.com Downloads の http://www.cisco.com/public/sw-center/sw-usingswc.shtml に説明のあるその他の条項に従うことに同意したことになります。

ソフトウェアのアップグレードに関し、"psirt@cisco.com" もしくは "security-alert@cisco.com" に お問い合わせいただくことはご遠慮ください。

サービス契約をお持ちのお客様

サービス契約をお持ちのお客様は、通常のアップデート チャネルから アップグレード ソフトウェアを入手してください。 ほとんどのお客様は、Cisco のワールドワイドウェブサイト上の ソフトウェアセンターからアップグレードを入手することができます。 http://www.cisco.com

サードパーティのサポート会社をご利用のお客様

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、 サードパーティのサポート会社と以前に契約していたか、または現在契約しており、 その会社から Cisco 製品の提供または保守を受けているお客様は、 該当するサポート会社に連絡し、本脆弱性に関する適切な処置について指示と支援を受けてください。

回避策の効果は、使用製品、ネットワークトポロジー、トラフィックの性質や 組織の目的などのお客様の状況に依存します。影響製品が多種多様であるため、 回避策を実際に展開する前に、対象とするネットワークで適用する回避策が最適であるか、 お客様のサービスプロバイダーやサポート組織にご相談ください。

サービス契約をご利用でないお客様

Cisco から直接購入したが Cisco のサービス契約をご利用いただいていない場合、 また、サードパーティ ベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、 Cisco Technical Assistance Center (TAC) に連絡してアップグレードを入手してください。 TAC の連絡先は次のとおりです。

- +1 800 553 2447 (北米内からのフリー ダイヤル)
- +1 408 526 7209 (北米以外からの有料通話)
- 電子メール： tac@cisco.com

無償アップグレードの対象であることをご証明いただくために、 製品のシリアル番号と、このお知らせの URL をご用意ください。 サービス契約をご利用でないお客様に対する無償アップグレードは、 TAC 経由でご要求いただく必要があります。

さまざまな言語向けの各地の電話番号、説明、電子メール アドレスなどの、 この他の TAC の連絡先情報については、 http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html を参照してください。

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とその公表は確認しておりません。

この脆弱性は Cisco 内部でのテストによって発見されました。

この通知のステータス:FINAL

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を示唆するものでもありません。 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 Cisco Systems はいつでも本ドキュメントの変更や更新を実施する権利を有します。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して、単独の転載や意訳を実施した場合には、 事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

情報配信

本アドバイザリは、以下の Cisco のワールドワイドウェブサイト上に掲載されます。

http://www.cisco.com/warp/public/707/cisco-sa-20090923-cm.shtml

ワールドワイドのウェブ以外にも、次の電子メールおよび Usenet ニュースの受信者向けに、 この通知のテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで投稿されています。

- cust-security-announce@cisco.com
- first-teams@first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

このアドバイザリに関する今後の更新は、いかなるものも Cisco のワールドワイドウェブに掲載される予定です。 しかしながら、前述のメーリングリストもしくは ニュースグループに 対し積極的に配信されるとは限りません。 この問題に関心があるお客様は上記 URL にて最新情報をご確認いただくことをお勧めいたします。

更新履歴

Revision 1.0	2009-September-23	Initial public release

シスコセキュリティ手順

Cisco 製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関する支援、 および Cisco からセキュリティ情報を入手するための登録方法について詳しく知るには、 Cisco ワールドワイドウェブサイトの http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html にアクセスしてください。 このページには Cisco のセキュリティ通知に関してメディアが問い合わせる際の指示が掲載されています。 全ての Cisco セキュリティアドバイザリは http://www.cisco.com/go/psirt で確認することができます。