

Cisco Security Advisory: Cisco Unified Communications Manager Session Initiation Protocol Memory Leak Vulnerability

Advisory ID: cisco-sa-20110928-cucm

<http://www.cisco.com/warp/public/707/cisco-sa-20110928-cucm.shtml>

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 2011 September 28 1600 UTC (GMT)

目次

- [要約](#)
- [該当製品](#)
- [詳細](#)
- [脆弱性スコア詳細](#)
- [影響](#)
- [ソフトウェア バージョンおよび修正](#)
- [回避策](#)
- [修正済みソフトウェアの入手](#)
- [不正利用事例と公式発表](#)
- [この通知のステータス : FINAL](#)
- [情報配信](#)
- [更新履歴](#)
- [シスコ セキュリティ手順](#)

要約

Cisco Unified Communications Manager には、不正形式の Session Initiation Protocol (SIP; セッション開始プロトコル) メッセージの処理により引き起こされる、メモリ リークの脆弱性が存在します。この脆弱性が不正利用されると、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。シスコはこの脆弱性に対応するため、サポートされている Cisco Unified Communications Manager のバージョン向けに無償ソフトウェア アップデートをリリースしています。この SIP の脆弱性に対しては回避策が存在します。

このアドバイザリは次のリンクに掲載されます。 <http://www.cisco.com/warp/public/707/cisco-sa-20110928-cucm.shtml>

注：2011年9月28日のCisco IOS ソフトウェア セキュリティ アドバイザリ バンドル公開には10件のCisco Security Advisoryが含まれています。9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Cisco IOS ソフトウェア リリース、および2011年9月にバンドル公開したすべての脆弱性を解決するCisco IOS ソフトウェア リリースを記載しています。

個々の公開リンクは次のリンクにある「Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication」内に掲載されています。

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep11.html

Cisco IOS ソフトウェアは、このアドバイザリに記載されているSIPの脆弱性の影響を受けます。Cisco IOS ソフトウェアに影響する脆弱性に関しては、別途Cisco Security Advisoryが公開されています。<http://www.cisco.com/warp/public/707/cisco-sa-20110928-sip.shtml>で確認できます。

。

該当製品

脆弱性が存在する製品

次の製品は、このアドバイザリに記載されている脆弱性の影響を受けます。

- Cisco Unified Communications Manager 6.x
- Cisco Unified Communications Manager 7.x
- Cisco Unified Communications Manager 8.x

注：Cisco Unified Communications Manager バージョン 6.1 は2011年9月3日にソフトウェアメンテナン스가終了しています。Cisco Unified Communications Manager 6.x バージョンをご利用のお客様は、サポートされているCisco Unified Communications Manager のバージョンへのアップグレードに関してシスコ サポート チームにお問い合わせください。

脆弱性が存在しない製品

Cisco Unified Communications Manager バージョン 4.x は、この脆弱性の影響を受けません。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

Cisco Unified Communications Manager は、IP Phone、メディア処理デバイス、VoIP ゲートウェイ、およびマルチメディア 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 デバイスにエンタープライズ テレフォニー機能を拡張する、シスコ IP テレフォニー ソリューションのコール処理コンポーネントです。

SIP におけるメモリ リークの脆弱性

Cisco Unified Communications Manager には、SIP メッセージの処理に関する脆弱性が存在します。Cisco Unified Communications Manager では、不正な SIP メッセージの処理中に Session Control Buffer (SCB; セッション コントロール バッファ) がリークする可能性があります。この脆弱性が継続的に悪用されると、重要な処理が失敗し、結果として音声サービスの中断が発生することがあります。すべての SIP ポート (TCP ポート 5060 および 5061、UDP ポート 5060 および 5061) が影響を受けます。

この SIP の脆弱性は Cisco Bug ID [CSCti86047](#) ([登録ユーザのみ](#)) として文書化され、CVE ID として CVE identifier CVE-2011-2072 が割り当てられています。この脆弱性は、Cisco Unified Communications Manager バージョン 8.6(1)、8.5(1)su2、7.1(5b)su4 で修正されています。[注 : 修正が含まれている 6.x バージョンのソフトウェア サービス アップデートはありません。]

注 : この脆弱性は、Cisco IOS ソフトウェアにも該当します。対応する Cisco Bug ID は [CSCto88686](#) です。詳細については、別途「Cisco Security Advisory for the Cisco IOS Software」を参照してください。

脆弱性スコア詳細

シスコ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 バージョン 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。

シスコは基本評価スコア (Base Score) および現状評価スコア (Temporal Score) を提供しています。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。

シスコは次の 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、シスコ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://tools.cisco.com/security/center/cvssCalculator.x>

(customers only)					
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

本アドバイザリに記載された脆弱性の不正利用に成功した場合、攻撃者はリモートから音声サービスの中断の原因となるメモリリークを引き起こす可能性があります。Cisco Unified Communications Manager は影響を受けたプロセスを再度実行しますが、攻撃が繰り返されることによって、結果としてサービス拒否 (DoS) 状態が続く可能性があります。

ソフトウェアバージョンおよび修正

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。シスコはテーブルの「Recommended Releases」列のリリース、またはそれ以降のリリースにアップグレードすることを推奨します。

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メンテナンスプロバイダーにお問い合わせください。

また、次のリンク先にある Cisco Security Intelligence Operations (SIO) ポータルで、Cisco IOS ソフトウェアチェッカーを入手できます。

<http://tools.cisco.com/security/center/selectIOSVersion.x> このツールでは、特定の Cisco IOS ソフトウェアバージョンに影響のあるセキュリティアドバイザリを調べるための機能をいくつか提供しています。

Cisco Unified Communication Manager Version	Recommended Release
7.x	7.1(5b)su4
8.x*	8.5(1)su2, 8.6(1)

* 上記テーブルに記載した推奨リリースは、このアドバイザリの公開時に入手可能となる Cisco Unified Communications Manager のバージョンです。6.1 および 8.0 対応のソフトウェアアップデートは CSCt186047 では使用できません。これらのバージョンをご利用のお客様は、サポートされているリリースへのアップグレードに関してシスコ サポート チームにお問い合わせください。

Cisco Unified Communications Manager ソフトウェアは、次のリンク先からダウンロードできます。<http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=268439621>

回避策

各自の環境において SIP を必要としないお客様に対しては、回避策が存在します。Cisco Unified Communication Manager バージョン 6.1(4)、7.1(2)、8.0(1) では SIP 処理を無効にする機能が実装されています。SIP 処理はデフォルトで有効にされています。SIP 処理を無効にするには、次の手順に従ってください。

- **ステップ 1** : Cisco Unified CM 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] > [Service Parameters]** の順に選択し、該当する Cisco Unified Communications Manager サーバと Cisco CallManager サービスを選択します。
- **ステップ 3** : 「**SIP Interoperability Enabled**」パラメータを False に変更し、**[Save]** をクリックします。

注：SIP 処理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。サービスを再起動する方法については、次の場所にあるドキュメントの「Restarting the Cisco CallManager Service」セクションを参照してください。

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/7_1_2/ccmcfg/b03dpi.html#wp1075124

スクリーニング デバイスでフィルタリングを実装し、TCP ポート 5060 と 5061、および UDP ポート 5060 と 5061 へのアクセスを、Cisco Unified Communications Manager サーバへの 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、この脆弱性を緩和できます。

ネットワーク内のシスコ デバイスに適用可能なその他の緩和策については、次のリンクで、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 Multiple Vulnerabilities in Cisco Voice Products』にて参照できます。このドキュメントは、次のリンクで入手可能です。

<http://www.cisco.com/warp/public/707/cisco-amb-20110928-voice.shtml>

修正済みソフトウェアの入手

シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。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 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ください。

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 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 に記載のシスコのソフトウェア ライセンスの条項、または Cisco.com ダウンロード サイトの <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。

[サービス契約をご利用のお客様](#)

サービス契約をご利用のお客様は、通常のアップデート チャン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、シスコのワールドワイド Web サイト上の Software Center 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、その会社からシスコ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会社にご相談ください。

[サービス契約をご利用でないお客様](#)

シスコから直接購入したがシスコ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、シスコの社内テストおよびお客様からのサービス リクエストのトラブルシューティング中に発見されたものです。

[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。またシスコシステムズ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識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、次のシスコのワールドワイド Web サイト上に掲載されます。

<http://www.cisco.com/warp/public/707/cisco-sa-20110928-cucm.shtml>

ワールドワイド Web 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-bulletins@lists.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、いかなるものもシスコのワールドワイド Web サイト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	2011-September-28	Initial public release.
--------------	-------------------	-------------------------

シスコ セキュリティ手順

シスコ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、およびシスコ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、シスコワールドワイド Web 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、シスコ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。すべてのシスコ 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。