

Cisco Security Advisory: Cisco Unified Communications Manager Denial of Service Vulnerabilities

Advisory ID: cisco-sa-20110824-cucm

http://www.cisco.com/cisco/web/support/JP/110/1108/1108412_cisco-sa-20110824-cucm-j.html

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 1.2

Last Updated 2011 October 26 16:36 UTC (GMT)

For Public Release 2011 August 24 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、Denial of Service (DoS; サービス拒否) に対する 5 つの脆弱性が含まれています。

シスコはこれらの脆弱性に対応するため、該当する 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。SIP およびパケット キャプチャ サービスの DoS 脆弱性に対しては回避策があります。

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/cisco/web/support/JP/110/1108/1108412_cisco-sa-20110824-cucm-j.html

本アドバイザリに記載されている脆弱性のうちの 2 つは、Cisco Intercompany Media Engine にも影響を与えます。

Cisco Intercompany Media Engine 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。このアドバイザリは次のリンクに掲載されています。

http://www.cisco.com/cisco/web/support/JP/110/1108/1108411_cisco-sa-20110824-ime-j.html

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うち少なくとも 1 つの影響を受けます。

- Cisco Unified Communications Manager 4.x
- 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 5.1 は 2010 年 2 月 13 日にソフトウェアメンテナンスが終了しています。Cisco Unified Communications Manager 5.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 のすべてのバージョンが、このアドバイザリに記載されている脆弱性のうち少なくとも 1 つの影響を受けます。

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。

DoS の脆弱性

Cisco Unified Communications Manager は 5 つの DoS 脆弱性を含みます。これらは重要な処理

を失敗させ、結果として音声サービスの中断をもたらす可能性があります。

1 つ目の DoS 脆弱性は、デフォルトで有効化されているパケット キャプチャ サービスに関連するものです。パケット キャプチャ サービスがタイムアウトしなくなる、またはアイドル状態の TCP 接続をクローズできなくなります。攻撃者は、リモートから複数の接続をオープンして Cisco Unified Communications Manager のメモリを消費させることが可能で、その結果 Cisco Unified Communications Manager が再起動される場合があります。Cisco Unified Communications Manager Administration インターフェイスで、サービス パラメータを False に変更してパケット キャプチャ サービスを無効化する必要があります。この操作を有効にするには、Unified Communications Manager アプリケーションを再起動する必要があります。この脆弱性は Cisco Bug ID [CSCtf97162](#) ([登録ユーザのみ](#)) に文書化されており、Common Vulnerabilities and Exposures (CVE) ID として CVE-2011-2560 が割り当てられています。この脆弱性に該当するのは、Cisco Unified Communications Manager バージョン 4.x のみです。

2 つ目の DoS 脆弱性は、Media Termination Points (MTP) の特定のコンフィギュレーションに関係するものです。MTP を g729ar8 コーデックに設定したときにのみ、音声が一方向となる場合があります。特定の状況下において、SIP コールの Session Description Protocol (SDP) 部分の処理中にサービスの中断が発生し、Session Initiation Protocol (SIP) プロセスによってスタックトレースが生成される可能性があります。この脆弱性は Cisco Bug ID [CSCtc61990](#) ([登録ユーザのみ](#)) として文書化され、CVE ID として CVE-2011-2561 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 7.0(x) 以降のみに影響し、バージョン 7.1(5b)su4 および 8.0(1) では修正されています。

3 つ目の DoS 脆弱性は、特定の SIP INVITE メッセージの処理中のコアダンプに関連するものです。この脆弱性は Cisco Bug ID [CSCth43256](#) ([登録ユーザのみ](#)) として文書化され、CVE ID として CVE-2011-2562 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 6.x 以降に影響し、バージョン 6.1(5)su2、7.1(5b)su3、8.0(3a)su1 および 8.5(1) では修正されています。

残り 2 つの DoS 脆弱性は、Service Advertisement Framework (SAF) に関係するものです。認証されていない攻撃者は、巧妙に細工された SAF パケットを該当デバイスに送信することで、これらの脆弱性を不正利用する可能性があります。この脆弱性の不正利用に成功した場合、デバイスの再起動が発生することがあります。これらの脆弱性は、Cisco Bug ID [CSCth26669](#) ([登録ユーザのみ](#)) および [CSCth19417](#) ([登録ユーザのみ](#)) として文書化され、CVE ID として CVE-2011-2563 および CVE-2011-2564 がそれぞれ割り当てられています。これらの脆弱性は、Cisco Unified Communications Manager バージョン 8.x に影響し、バージョン 8.5(1) では修正されています。Cisco Intercompany Media Engine リリース 8.x もこれらの脆弱性の影響を受けます。Cisco Intercompany Media Engine 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。このアドバイザリは次のリンクに掲載されています。

http://www.cisco.com/cisco/web/support/JP/110/1108/1108411_cisco-sa-20110824-ime-j.html

注：SAF の脆弱性を引き起こすには、3 ウェイ ハンドシェイク手順によって TCP 接続が確立される必要があります。

[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>

CSCtf97162 - CCM Application Restarts During TCP Flood 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	
CSCtc61990 - Coredump may be experienced when processing certain SIP packets Calculate the environmental score of					
CVSS Base Score - 7.1					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None	None	None	Complete
CVSS Temporal Score - 5.9					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	
CSCth43256 - Coredump may be experienced when processing certain SIP packets 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	
CSCth26669 - CUCM may experience a reload when receiving certain UCM client msgs 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	
CSCth19417 - CUCM may experience a reload when receiving certain UCM client msgs 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

本アドバイザーに記載された脆弱性の不正利用に成功した場合、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。場合によっては、影響を受けた Cisco Unified Communications Manager プロセスが再起動されますが、攻撃が繰り返されることによって、結果として DoS 状態になることがあります。

ソフトウェア バージョンおよび修正

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。

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。

Cisco Unified Communications Manager Version	Recommended Releases
6.x	6.1(5)SU3
7.x	7.1(5b)SU4
8.0	8.0(3a)SU2
8.5	8.5(1)SU2, 8.6(1)

回避策

SIP DoS の脆弱性に対しては回避策があります。Cisco Unified Communications 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 処理を必要としないお客様は次の手順に従って SIP 処理を無効にすることができます。

- **ステップ 1** : Cisco Unified Communications Manager Administration の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行し、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。

Cisco Communications Manager バージョン 4.x における、パケット キャプチャ サービスに関連する DoS 脆弱性に対しては回避策があります。パケット キャプチャ サービスによるトラブルシューティングを必要としないお客様は、次の手順に従ってこのサービスを無効にすることができます。

- **ステップ 1** : Cisco Unified Communications Manager 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 サーバとパケット キャプチャ サービスを選択します。
- **ステップ 3** : 「Packet Capture Enabled」パラメータを False に変更し、[Save] をクリックします。

注 : パケット キャプチャ サービス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/service/4_2_3/ccmsrvs/sscontrl.html

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、次のリンクの、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 Unified Communications Manager』にて参照できます。

<http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110824-cucm-ime>

[修正済みソフトウェアの入手](#)

シスコ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 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 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、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、その他の 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/cisco/web/support/JP/110/1108/1108412_cisco-sa-20110824-cucm-j.html

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 1.2	2011-October-26	Revision table updated
Revision 1.1	2011-October-21	Updated URL

Revision 1.0	2011-August-24	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。