Multiple Vulnerabilities in Cisco Unity Connection

Advisory ID: cisco-sa-20150401-cuc

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150401-cuc

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 2015 April 1 16:00 UTC (GMT)

目次

要約

Cisco Unity Connection には、Session Initiation Protocol（SIP）トランクとの統合を実行した場合に複数の脆弱性が存在します。このアドバイザリに記載されている脆弱性はすべてサービス拒否の脆弱性であり、SIP メッセージを処理する際の Cisco Unity Connection の可用性に影響します。

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。これらの脆弱性を軽減する回避策はありません。

このアドバイザリは、次のリンクで確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150401-cuc

該当製品

Cisco Unity Connection は、SIP と統合されている場合、このアドバイザリに記載されているすべての脆弱性の影響を受けます。

Skinny Call Control Protocol（SCCP）との統合を実装している場合は、このアドバイザリに記載

されている脆弱性の影響は受けません。

IPv4 または IPv6 による統合が影響を受けます。

脆弱性が認められる製品

次の表に、それぞれの脆弱性の影響を受ける Cisco Unity Connection のメジャー バージョンを示しています。

Major Version	Major Train Affected by Vulnerability				
	CSCul28089	CSCul26267	CSCul20444	CSCuh25062	CSCul69819
Prior to 8.5	Y	Y	Y	Y	Y
8.5	Y	Y	Y	Y	Y
8.6	Y	Y	Y	Y	Y
9.0	Y	Y	Y	Y	Y
9.1	Y	Y	Y	Y	Y
10.0	Y	Y	Y	N	N
10.5	N	N	N	N	N

各脆弱性は互いに独立していますが、すべてが SIP 通信に影響するため、5 つすべての脆弱性向けの修正が含まれたバージョンにアップグレードすることを推奨します。

注：バージョン 8.5 より前の Cisco Unity Connection はソフトウェア メンテナンスが終了しています。8.5 より前のバージョンを使用している場合は、サポートされている Cisco Unity Connection 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。

Cisco Business Edition に関する情報

Cisco Business Edition 7000 および Cisco Business Edition 6000 は、このセキュリティ アドバイザリの「脆弱性が認められる製品」セクションの表に記載された該当バージョンの Cisco Unity Connection を使用している場合に、これらの脆弱性の影響を受けます。

ソフトウェア バージョンの確認

アプライアンスで実行されている Cisco Unity Connection ソフトウェアのバージョンを確認するには、Cisco Unity Connection Web インターフェイスにアクセスし、右上にある [About] リンクをクリックします。または、コマンドライン インターフェイスにログインして、メイン メニューにアクセスします。ソフトウェアのバージョンは、 **show version active** コマンドを使用して確認できます。次の例は、バージョン 8.6.2 が実行されている Cisco Unity Connection を示しています。

```
Welcome to the Platform Command Line Interface

admin:show version active
Active Master Version: 8.6.2.10000-30
```

脆弱性が認められない製品

次の製品はこの脆弱性の影響を受けません。

- SIP を実装した Cisco IOS ソフトウェア

- Cisco Unified Communications Manager
- Cisco Unity Express

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 Unity Connection は、豊富な機能を持つボイスメッセージング プラットフォームで、Cisco Unified Communications Manager と同じ Linux ベースの Cisco Unified Communications オペレーティング システムを使用しています。Cisco Unity Connection は、10 万ユーザまでのエンタープライズ企業をサポートします。

Cisco Unity Connection は、SIP または SCCP を使用して音声インフラストラクチャに統合できます。SIP での統合のみが、次の脆弱性による影響を受けます。

注： 次の脆弱性のすべては、IPv4 通信または IPv6 通信によって不正利用される可能性があります。

Cisco Unity Connection の SIP トランク統合におけるポート UDP 5060 の DoS 脆弱性

Cisco Unity Connection の Connection Conversation Manager（CuCsMgr）のプロセスに存在する脆弱性により、認証されていないリモートの攻撃者が該当デバイスの SIP ネットワーク ポート UDP 5060 を閉じる可能性があります。

この脆弱性は、特定の UDP パケットの不適切な処理に起因します。攻撃者は、該当デバイスの構成済み SIP トランクに特定の UDP パケットを送信することで、この脆弱性を不正利用する可能性があります。この不正利用によって攻撃者は SIP ポートを閉じることができ、Cisco Unity Connection はコールを処理できなくなります。

UDP ポート 5060 は Unity Connection で CuCsMgr のプロセス用にバインドされており、特定の UDP パケットを受信することで永続的に閉じることになります。この脆弱性は、市販されているスキャナを使用して不正利用できることがわかっています。

この脆弱性を不正利用できるのは、UDP パケットを使用する場合だけです。

この脆弱性が不正利用された場合、管理者は Cisco Unity Connection の CuCsMgr プロセスを再起動する必要があります。

この脆弱性は、Cisco Bug ID CSCuh25062（ 登録ユーザ専用 ）として文書化され、Common Vulnerabilities and Exposures（CVE）ID として CVE-2015-0612 が割り当てられています。

Cisco Unity Connection の SIP トランク統合における巧妙に細工された UDP INVITE メッセージによる DoS 脆弱性

Cisco Unity Connection の Connection Conversation Manager（CuCsMgr）プロセスに存在する脆弱性により、認証されていないリモートの攻撃者が CuCsMgr プロセスをコア ダンプし、再起動させる可能性があります。

この脆弱性は、巧妙に細工された SIP INVITE メッセージの不適切な処理に起因します。攻撃者は、巧妙に細工された SIP INVITE メッセージを Cisco Unity Connection サーバに送信することで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者は CuCsMgr プロセスのコア ダンプを引き起こし、結果としてサービス拒否状態になる可能性があります。この脆弱性は使用されている転送プロトコルには依存せず、UDP、TCP、または TLS の接続のいずれかを使用して不正利用される可能性があります。

この脆弱性は、Cisco Bug ID CSCul20444（ 登録ユーザ専用 ）として文書化され、CVE ID として CVE-2015-0613 が割り当てられています。

Cisco Unity Connection の SIP トランク統合における巧妙に細工された UDP INVITE メッセージによる DoS 脆弱性

Cisco Unity Connection の Connection Conversation Manager（CuCsMgr）プロセスに存在する脆弱性により、認証されていないリモートの攻撃者が CuCsMgr プロセスをコア ダンプし、再起動させる可能性があります。

この脆弱性は、巧妙に細工された SIP INVITE メッセージの不適切な処理に起因します。攻撃者は、巧妙に細工された SIP INVITE メッセージを Cisco Unity Connection サーバに送信することで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者は CuCsMgr プロセスのコア ダンプを引き起こし、結果として DoS 状態になる可能性があります。

この脆弱性は前述の脆弱性と同様ですが、SIP INVITE メッセージの異なる部分が適切に処理されません。

この脆弱性は使用されている転送プロトコルには依存せず、UDP、TCP、または TLS の接続のいずれかを使用して不正利用される可能性があります。

この脆弱性は、Cisco Bug ID CSCul26267（ 登録ユーザ専用 ）として文書化され、CVE ID として CVE-2015-0614 が割り当てられています。

注：CVE ID CVE-2015-0613 と CVE ID CVE-2015-0614 に記載されている脆弱性の相違点は、不正利用に使用される SIP INVITE メッセージのフィールドが異なることです。

Cisco Unity Connection の SIP トランク統合におけるビジー ポートによる DoS 脆弱性

Cisco Unity Connection の SIP コール処理コードに存在する脆弱性により、認証されていないリモートの攻撃者がすべての SIP 接続回線（ポート）を消費させる可能性があります。

この脆弱性は、特定の接続シナリオ下で割り当てられているリソースが解放されないことに起因します。攻撃者は、SIP セッションを異常終了させることで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者は Unity Connection のすべての使用可能な SIP ポートを使用状態とすることで、それ以上の接続ができなくなります。この脆弱性が不正利用されるとすべての SIP 回線（ポート）が使用状態となり、Cisco Unity Connection はすべてのポートがビジーであることを示す 503 エラーで応答します。この状態から回復するための唯一の方法は、Cisco Unity Connection の管理者が Conversation Manager を再起動することです。

この脆弱性は使用されている転送プロトコルには依存せず、UDP、TCP、または TLS の接続のいずれかを使用して不正利用される可能性があります。

この脆弱性は、Cisco Bug ID CSCul28089（ 登録ユーザ専用 ）として文書化され、CVE ID として CVE-2015-0615 が割り当てられています。

Cisco Unity Connection の SIP トランク統合における CuCsMg の DoS 脆弱性

Cisco Unity Connection の Connection Conversation Manager（CuCsMgr）プロセスに存在する脆弱性により、認証されていないリモートの攻撃者が CuCsMgr プロセスをコア ダンプし、再起動させる可能性があります。

この脆弱性は、不適切に終了された SIP メッセージ交換を適切に処理できないことに起因します

。攻撃者は、Cisco Unity Connection サーバへの SIP 接続を異常終了させることで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者は CuCsMgr プロセスのコア ダンプを引き起こし、結果として DoS 状態になる可能性があります。

この脆弱性を不正利用できるのは、TCP SIP 接続を使用した場合のみです。

この脆弱性は、Cisco Bug ID CSCul69819（ 登録ユーザ専用 ）として文書化され、CVE ID として CVE-2015-0616 が割り当てられています。

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。本セキュリティ 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組織の手助けとなる標準ベースの評価法です。

シスコでは、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、自身のネットワークにおける脆弱性の影響度を知ることができます。

シスコは次のリンクで CVSS に関する追加情報を提供しています。
http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

またシスコでは、各ネットワークにおける環境影響度を算出する CVSS 計算ツールを次のリンクで提供しています。
http://tools.cisco.com/security/center/cvssCalculator.x

注： このアドバイザリに記載されたすべての脆弱性は、同じ CVSS スコアを共有します。

Cisco Unity Connection SIP Trunk Integration Denial of Service Vulnerabilities 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	

影響

この脆弱性が不正利用されると、次のいずれかが発生する可能性があります。

- SIP UDP ポート 5060 が閉じ、Cisco Unity Connection の 管理者が CuCsMgr サービスを再起動する必要がある。
- Cisco Unity Connection ですべての SIP ポートがビジーとなり、Cisco Unity Connection の管理者が CuCsMgr サービスを再起動する必要がある。
- CuCsMgr のクラッシュが発生する。継続的な DoS 攻撃が発生する場合はプロセスが自動的に再起動されるものの、SIP によって Cisco Unity Connection にアクセスすることができない。

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場合は、http://www.cisco.com/go/psirt/ の Cisco Security Advisories, Responses, and Alerts アーカイブや、後続のアドバイザリを参照して、起こりうる障害を判断し、それに対応できるアップグレード 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デバイスに十分なメモリがあること、現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、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。

次の表に、このアドバイザリに記載されたすべての脆弱性への修正が含まれた最初の修正リリースを示します。

Version	First Fixed Release
8.5	8.5(1)SU7
8.6	8.6(2a)SU4
9.0	Vulnerable; Migrate to 9.1(2)SU2 or later.
9.1	9.1(2)SU2
10.0	10.0(1)SU1
10.5	Not Affected

次の表に、リリースされている最初の修正を脆弱性ごとに示します。

Version	First Fixed Release				
	CSCul28089	CSCul26267	CSCul20444	CSCuh25062	CSCul69819
8.5	8.5(1)SU7	8.5(1)SU7	8.5(1)SU7	8.5(1)SU6	8.5(1)SU7
8.6	8.6(2a)SU4	8.6(2a)SU4	8.6(2a)SU4	8.6(2a)SU4	8.6(2a)SU4
9.0	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable
9.1	9.1(2)SU2	9.1(2)SU2	9.1(2)SU2	9.1(2)SU2	9.1(2)SU2
10.0	10.0(1)SU1	10.0(1)SU1	10.0(1)SU1	Not Affected	Not Affected
10.5	Not Affected	Not Affected	Not Affected	Not Affected	Not Affected

回避策

これらの脆弱性を軽減する回避策はありません。

修正済みソフトウェアの入手

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェア 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の特有の問題をご確認ください。

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 ライセンスの条項に従うことに同意したことになります。

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.com の Software Navigator 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/cisco/software/navigator.html

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、正しい処置についてのサポートを受けてください。

回避策や修正の効果は、使用している製品、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に関するお客様の状況によって異なります。影響を受ける製品やリリースは多種多様であるため、回避策を実施する前に、対象ネットワークで適用する回避策または修正が最適であることを、お客様のサービス プロバイダーやサポート会社にご確認ください。

サービス契約をご利用でないお客様

シスコから製品を直接購入したもののシスコのサービス契約をご利用いただいていない場合、または、サードパーティ ベンダーから購入したものの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 ソフトウェアを入手してください。

- +1 800 553 2447（北米からの無料通話）
- +1 408 526 7209（北米以外からの有料通話）
- Eメール：tac@cisco.com

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの 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は TAC に無償アップグレードをリクエストしてください。

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、シスコ ワールドワイドお問い合わせ先（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 Product Security Incident Response Team（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のサービス リクエストの処理中に発見されたものです。

一部のネットワーク スキャナによって Cisco Bug ID CSCuh25062（CVE-ID-2015-0612）の不正利用が可能なことがわかっています。

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

このアドバイザリは次のリンクにある Cisco Security に掲載されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150401-cuc

また、このアドバイザリのテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで次の電子メールで配信されています。

- 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

本アドバイザリに関する今後の更新は Cisco.com に掲載されますが、メーリング リストで配信されるとは限りません。更新内容については、本アドバイザリの URL でご確認ください。

更新履歴

Revision 1.0	2015-April-01	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サポート、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の詳細については、Cisco.com の http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html を参照してください。この Web ページには、Cisco Security Advisory 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 Cisco Security Advisory は、http://www.cisco.com/go/psirt/ で確認することができます。

Cisco Security Advisories
Cisco Intrusion Prevention System Signatures
Cisco Applied Mitigation Bulletins
Cisco Security Blog
Cisco Event Response Pages
Cisco IntelliShield Alerts
Cisco Security Notices
Cisco Security Responses
Cisco Cyber Risk Reports
Cisco Security White Papers
Snort Rules