

Cisco TelePresence Video Communication Server SIP Denial of Service Vulnerability

Advisory ID: cisco-sa-20140122-vcs

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140122-vcs>

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 2014 January 22 16:00 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 TelePresence Video Communication Server (VCS) には脆弱性があり、承認されていないリモートの攻撃者が複数の重要なプロセスの障害を引き起こせる可能性があります。これにより、アクティブ コールのドロップが発生し、影響を受けたシステムがリロードされるまで、ユーザは新しいコールを確立できなくなる可能性があります。

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。これらの脆弱性に対しては回避策がありません。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-20140122-vcs>

該当製品

脆弱性が認められる製品

この脆弱性は、X8.1 よりも前の Cisco TelePresence VCS ソフトウェアが稼働している Cisco

TelePresence VCS Control、Cisco TelePresence VCS Expressway、および Cisco TelePresence VCS Starter Pack Expressway に影響します。
Cisco TelePresence VCS のハードウェアと仮想アプライアンスは両方ともこの脆弱性の影響を受けます。

脆弱性が認められない製品

この脆弱性の影響を受ける他のシスコ製品は、現在確認されていません。

詳細

Cisco TelePresence Video Communication Server は、あらゆるビデオおよびテレプレゼンス コミュニケーションをサポートすることで、ネットワーク間や組織間にわたってフェイスツーフェイスのビデオコラボレーションの利点を広げます。

Cisco TelePresence Video Communication Server (VCS) のセッション開始プロトコル (SIP) の脆弱性によって、認証されていないリモートの攻撃者が複数の重要なプロセスの失敗を引き起こせるようになり、これによってアクティブ コールが終了する可能性があります。また、影響を受けたシステムがリロードされるまで、新しいコールを確立できなくなります。

この脆弱性は、巧妙に細工されたセッション記述プロトコル (SDP) メッセージが適切に処理されないことに起因します。攻撃者は巧妙に細工された SDP メッセージを該当システムに送信することで、この脆弱性を不正利用できる可能性があります。この不正利用により攻撃者は複数の重要なプロセスの失敗を引き起こすことができ、これによって該当システムが正常に機能しなくなる可能性があります。アクティブ コールが終了するとともに、該当システムがリロードされるまで新しいコールが確立できないようになります。正常な機能を回復するにはリロードが必要です。

この脆弱性は、UDP または TCP で SDP メッセージが送信されることによってトリガーされる可能性があります。Transport Layer Security (TLS) を使用した配信も影響を受けます。UDP と TCP での配信のデフォルト ポートは UDP ポート 5060 と TCP ポート 5060 です。TLS 配信のデフォルト ポートは、TCP ポート 5061 です。

この脆弱性は、Cisco Bug ID [CSCue97632](#) ([登録ユーザ専用](#)) として文書化され、Common Vulnerability and Exposures (CVE) ID CVE-2014-0662 が割り当てられています。

脆弱性スコア詳細

シスコは本アドバイザーでの脆弱性に対し、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/>

| CSCue97632 - Cisco TelePresence Video Communication Server SDP Denial of Service Vulnerability | | | | | |
|--|-------------------|-------------------|------------------------|-------------------|---------------------|
| 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

この脆弱性の不正利用が成功すると、重要な内部プロセスがいくつか失敗し、影響を受けたシステムは正常に機能しなくなる可能性があります。その結果、アクティブ コールが終了し、該当システムがリロードされるまで新しいコールを確立できなくなります。正常な機能を回復するにはリロードが必要です。

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場合は、<http://www.cisco.com/go/psirt/> の Cisco Security Advisories, Responses, and Notices 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。

この脆弱性は、Cisco TelePresence VCS ソフトウェア X8.1 以降では解決されています。

回避策

この脆弱性を軽減する対応策はありません。

ネットワーク内のシスコ 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

ントである『Cisco Applied Intelligence』にて参照できます。

<http://tools.cisco.com/security/center/viewAMBAAlert.x?alertId=32409>

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、[Cisco.com](http://www.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。

この脆弱性はシスコ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

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

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140122-vcs>

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 E 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 | 2014-January-22 | 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、シスコのセキュリティ アドバイザリ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。