Multiple Vulnerabilities in Cisco TelePresence Video Communication Server, Cisco Expressway, and Cisco TelePresence Conductor

Advisory ID: cisco-sa-20150311-vcs

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150311-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 2015 March 11 16:00 UTC (GMT)

目次

要約

Cisco TelePresence Video Communication Server（VCS）、Cisco Expressway、および Cisco TelePresence Conductor には、次に示す脆弱性があります。

- SDP メディア記述に関連した Denial of Service の脆弱性
- 認証バイパスの脆弱性

SDP メディア記述に関連した Denial of Service の脆弱性が不正利用されると、該当システムにリロードが発生する可能性があります。
認証バイパスの脆弱性が不正利用されると、攻撃者が認証を迂回し、管理者の権限でシステムにログインできる可能性があります。

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-20150311-vcs

該当製品

脆弱性が認められる製品

これらの脆弱性は、次の製品が、該当するバージョンのソフトウェアを実行している場合に発生します。

- Cisco TelePresence VCS Control
- Cisco TelePresence VCS Expressway
- Cisco TelePresence VCS Starter Pack Expressway
- Cisco Expressway Core
- Cisco Expressway Edge
- Cisco TelePresence Conductor

Cisco TelePresence VCS、Cisco Expressway、および Cisco TelePresence Conductor のハードウェアおよび仮想アプライアンスはこれらの脆弱性の影響を受けます。

脆弱性が認められない製品

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 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 Expressway は、Cisco Unified Communications Manager、Cisco Business Edition、または Cisco Hosted Collaboration Solution（HCS）によって提供される包括的なコラボレーション サービス向けに特別に設計されています。Cisco Expressway ではファイアウォール トラバーサル技術が確立されており、従来の企業コラボレーションの境界を再定義するのに役立ちます。

Cisco TelePresence Conductor は、ミーティングにおいてすべてのユーザに対する会議リソースの割り当てを調整することによって、マルチパーティのビデオ コミュニケーションを簡素化します。

SDP メディア記述に関連した Denial of Service の脆弱性

Session Description Protocol（SDP）のパケット ハンドラ機能に脆弱性があり、認証されていないリモートの攻撃者によって該当システムにリロードが引き起こされる可能性があります。

この脆弱性は、巧妙に細工された SDP パケットの受信時に、例外が不適切に処理されることに起因します。攻撃者は、巧妙に細工された SDP パケットを該当システムへ送信することにより、この脆弱性を不正利用する可能性があります。

注：この脆弱性 は、UDP または TCP で SDP メッセージが送信される場合に発生する可能性があります。Transport Layer Security（TLS）を介して送信されるメッセージも影響を受けます。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、IPv4 および IPv6 のパケットによって引き起こされる可能性があります。

この脆弱性のうち、Cisco TelePresence VCS と Cisco Expressway に対するものは、 Cisco bug ID CSCus96593（ 登録ユーザ専用 ）として文書化され、Cisco TelePresence Conductor に対するものは、Cisco bug ID CSCun73192（ 登録ユーザ専用 ）として文書化されています。

この脆弱性には、 Common Vulnerabilities and Exposures（CVE ）ID として CVE-2015-0652 が割り当てられています。

認証バイパスの脆弱性

認証コードに脆弱性があるため、認証されていないリモートの攻撃者がシステム ログインを迂回し、システムに対する権限を取得できる可能性があります。
この脆弱性は、ログイン プロセス中に渡されるパラメータの検証が不十分であることに起因します。攻撃者は巧妙に細工したリクエスト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する可能性があります。この不正利用により、攻撃者は認証制御機能を迂回し、システムにログインできる可能性があります。この攻撃を行うには、有効なユーザ名を使用する必要があります。攻撃者は、ログイン後、そのユーザの権限を取得します。この脆弱性によって、攻撃者は該当システムへの管理アクセス権限を取得できる可能性があります。

注：この脆弱性 の不正利用が可能となるのは、HTTPS を使用し、該当システムの管理インターフェイスを宛先とした場合だけです。この脆弱性を不正利用するには、有効な TCP ハンドシェイクが必要です。また、この脆弱性は、IPv4 パケットおよび IPv6 パケットによって引き起こされる可能性があります。

この脆弱性のうち、Cisco TelePresence VCS と Cisco Expressway に対するものは、 Cisco bug ID CSCur02680（ 登録ユーザ専用 ）として文書化され、Cisco TelePresence Conductor に対するものは、 Cisco bug ID CSCur05556（登録ユーザ専用 ）として文書化されています。

この脆弱性には CVE ID として CVE-2015-0653 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

CSCus96593 and CSCun73192 - SDP Media Description Denial of Service Vulnerability 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	

CSCur02680 and CSCur05556 - Authentication Bypass Vulnerability Calculate the environmental score of					
CVSS Base Score - **10.0**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	Complete	Complete
CVSS Temporal Score - **8.3**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

SDP メディア記述に関連した Denial of Service の脆弱性が不正利用されると、該当システムにリロードが発生する可能性があります。
認証バイパスの脆弱性が不正利用されると、攻撃者が認証を迂回し、管理者の権限でシステムに

ログインできる可能性があります。

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。

Cisco TelePresence VCS、Cisco Expressway、Cisco TelePresence Conductor のソフトウェアに関する両方の脆弱性に対する最初の修正リリースを次の表に示します。Recommended Release 行には、この Security Advisory に記載されているすべての脆弱性を解決する推奨リリースに関する情報が示されています。

	Cisco TelePresence VCS and Cisco Expressway First Fixed Releases	Cisco TelePresence Conc First Fixed Releases
SDP Media Description Denial of Service Vulnerability	X8.2 and later	XC2.4 and later
Authentication Bypass Vulnerability	X7.2.4, X8.1.2, X8.2.2, X8.5 and later	X2.3.1, XC2.4.1, XC3.0 later
Recommended Release	**X8.5.1 and later**	**XC3.0.2 and later**

回避策

このアドバイザリに記載されている脆弱性に対する回避策はありません。

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/viewAMBAlert.x?alertId=37541

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、E 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。

認証バイパスの脆弱性は、Positive Technologies 社（Positive Research Center）の Andrey Medov 氏からシスコにご報告いただきました。

SDP メディア記述に関連した Denial of Service の脆弱性は、サポート ケースの解決中に発見されました。

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-20150311-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
- fulldisclosure@seclists.org

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。

今後のドキュメントや関連コンテンツの入手手順については、Security Vulnerability Policy ページの Receiving Security Vulnerability Information from Cisco を参照してください。

更新履歴

Revision 1.0	2015-March-11	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。