Cisco TelePresence Video Communication Server、Cisco Expressway、およびCisco TelePresence Conductorの複数の脆弱性

アドバイザリーID : cisco-sa-20150311-vcs
初公開日 : 2015-03-11 16:00
バージョン 1.0 : Final
CVSSスコア : 10.0
回避策 : No Workarounds available
Cisco バグ ID : CSCun73192 CSCur05556 CSCur02680 CSCus96593

CVE-2015-0653
CVE-2015-0652

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。

概要

Cisco TelePresence Video Communication Server(VCS)、Cisco Expressway、およびCisco TelePresence Conductorには、次の脆弱性が存在します。

- SDPメディア記述のDoS脆弱性
- 認証バイパスの脆弱性

SDPメディア記述のサービス拒否の脆弱性が不正利用されると、該当システムがリロードされる可能性があります。
認証バイパスの脆弱性が悪用されると、攻撃者は認証をバイパスし、管理者の権限を使用して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処するソフトウェアアップデートをリリースしています。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、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150311-vcs

該当製品

脆弱性のある製品

これらの脆弱性は、該当バージョンのソフトウェアを実行している次の製品に適用されます。

- 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のハードウェアと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。

脆弱性を含んでいないことが確認された製品

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 VCSは、Any-to-Anyの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、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ネットワークや組織に拡大します。

Cisco Expresswayは、Cisco Unified Communications Manager、Cisco Business Edition、またはCisco Hosted Collaboration Solutionを通じて提供される包括的なコラボレーションサービス専用に設計されています。確立されたファイアウォール越えテクノロジーを特徴とし、従来のエンタープライズコラボレーションの境界を再定義します。

Cisco TelePresence Conductorは、会議の各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で、マルチパーティビデオコラボレーションを簡素化します。

SDPメディア記述のDoS脆弱性

Session Description Protocol(SDP)パケットハンドラ機能の脆弱性により、認証されていないリモートの攻撃者が該当システムのリロードを引き起こす可能性があります。

この脆弱性は、巧妙に細工されたSDPパケットを受信する際の例外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SDPパケットを該当システムに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経由で送信されるSDPメッセージによって引き起こされる可能性があります。 Transport Layer Security(TLS)経由で送信されるメッセージも影響を受けます。 UDPおよびTCP展開のデフォルトポートは、UDPポート5060およびTCPポート5060です。TLS導入のデフォルトポートはTCPポート5061です。この脆弱性は、IPバージョン4(IPv4)および

IPバージョン6(IPv6)パケットによって引き起こされる可能性があります。

この脆弱性は、Cisco TelePresence VCSおよびCisco Expresswayに関するCisco Bug ID CSCus96593(登録ユーザ専用)と、Cisco TelePresence Conductorに関する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 に対してCommon Vulnerabilities and Exposures(CVE)ID CVE-2015-0652が 割り当てられています。

認証バイパスの脆弱性

認証コードの脆弱性により、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バイパスし、システムへの認証に成功す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、巧妙に細工された要求を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、攻撃者は認証制御をバイパスし、システムに正常にログインできる可能性があります。攻撃者は、有効なユーザ名を知っている必要があります。攻撃者は、ログイン後にそのユーザの権限を受け取ります。この脆弱性により、攻撃者は該当システムへの管理アクセス権を取得できる可能性があります。

注：この脆弱性の 不正利用が可能なのは、HTTPSを使用し、該当システムの管理インターフェイスを対象とする場合のみです。 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。この脆弱性は、IPv4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。

この脆弱性は 、Cisco Bug ID CSCur02680 (登録 ユーザ専用)として文書化されています Cisco TelePresence VCSおよびCisco Expresswayについては、Cisco TelePresence ConductorのCisco Bug ID CSCur05556(登録ユーザ専用)

この脆弱性にはCVE IDが割り当てられています。 CVE-2015-0653.

回避策

このアドバイザリに記載されている脆弱性を軽減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。
https://sec.cloudapps.cisco.com/security/center/viewAMBAlert.x?alertId=37541

修正済みソフトウェア

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 のシスコ セキュリティ アドバイザリ、応答、および通知のアーカイブや、後続のアドバイザリを参照して侵害の可能性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。](http://www.cisco.com/go/psirt)

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。

次の表は、Cisco TelePresence VCS、Cisco Expressway、およびCisco TelePresence Conductorソフトウェアの両方の脆弱性に対する最初の修正リリースをまとめたものです。「Recommended Release」行には、このセキュリティアドバイザリ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記載されています。

	Cisco TelePresence VCSおよびCisco Expresswayの最初の修正済みリリース	Cisco TelePresence Conductorの最初の修正済みリリース
SDPメディア記述のDoS脆弱性	X8.2以降	XC2.4以降
認証バイパスの脆弱性	X7.2.4、X8.1.2、X8.2.2、X8.5以降	X2.3.1、XC2.4.1、XC3.0以降
推奨リリース	X8.5.1以降	XC3.0.2以降

推奨事項

$propertyAndFields.get("recommendations")

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エクスプロイト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氏によってシスコに報告されました。

SDPメディア記述のDoS脆弱性は、サポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150311-vcs

改訂履歴

リビジョン 1.0	2015年3月11日	初回公開リリース

利用規約

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も示唆するものではありません。 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、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。