Cisco TelePresence Server サービス拒否の脆弱性

High

アドバイザリーID : cisco-sa-20150916-tps

初公開日 : 2015-09-16 16:00

バージョン 1.0 : Final

CVSSスコア : 7.8

回避策 : No Workarounds available

Cisco バグ ID : CSCuu28277

CVE-2015-6284

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 Server により非認証を可能にする可能性がある会議制御プロトコル API でバッファオーバーフローの脆弱性がサービス拒否（DoS）状態を引き起こすためにリモート攻撃者含まれています。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。この脆弱性を軽減する対応策は見つかりません。

このアドバイザリは、次のリンクより確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150916-tps

該当製品

脆弱性のある製品

4.1(2.33) 以下の製品で動作する前の Cisco TelePresence Server ソフトウェアのすべてのリリースはこの脆弱性から影響を受けします:

- Cisco Telepresence Server 7010
- Cisco TelePresence Server MSE 8710
- 複数政党制メディア 310 の Cisco TelePresence Server
- 複数政党制メディア 320 の Cisco TelePresence Server
- Cisco TelePresence Server on Virtual Machine

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 Server はワーカーにビジネス品質直観的なビデオ会議を提示し、Cisco Unified Communications Manager、Cisco TelePresence Management Suite（TMS）、および Cisco TelePresence Conductor によって相互運用します。

Cisco TelePresence Server により非認証を可能にする可能性がある会議制御プロトコル API でバッファオーバーフローの脆弱性が DoS 状態を引き起こすためにリモート攻撃者含まれています。

脆弱性は影響を受けたバッファにコピーされる前にユーザが指定するデータで実行された sanitization を入力すること当然の DoS 状態だけという結果に終る可能性が高いです。 攻撃者はオーバーフロー状態を誘発するように設計されている巧妙に細工された URL の提供によってこの脆弱性を不正利用する可能性があります。

この脆弱性 Cisco バグ ID CSCuu28277 （ 登録ユーザのみ ）で文書化されています、よくある脆弱性および公開（CVE） ID CVE-2015-6284 は割り当てられました。

回避策

この脆弱性を軽減する回避策がありません。

修正済みソフトウェア

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。

Cisco TelePresence Server は Cisco.com の Software Center から http://www.cisco.com/cisco/software/navigator.html **ダウンロード ホーム > 製品 > 会議ソリューション > ビデオ会議 > マルチパーティ会議 > TelePresence サーバ**の参照によってダウンロードすることができます。

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。
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。

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やその公表を確認していません。

この脆弱性は内部テストで発見されました。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150916-tps

改訂履歴

リビジョン 1.0	2015-September-16	初回公開リリース

利用規約