Cisco TelePresence Serverの巧妙に細工されたURL処理におけるDoS脆弱性

High

アドバイザリーID : cisco-sa-20160406-cts1

初公開日 : 2016-04-06 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 : CSCuv47565

CVE-2015-6313

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

ソフトウェアバージョン4.1(2.29)から4.2(4.17)を実行するCisco TelePresence Serverデバイスの脆弱性により、認証されていないリモートの攻撃者がデバイス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 URL を処理する際の HTTP 解析エンジンの障害に起因します。攻撃者は、該当デバイスに複数のURL要求を送信することで、この脆弱性を不正利用する可能性があります。クライアントからのネゴシエーションが行われないため、要求は最終的にタイムアウトします。ただし、要求が行われるたびに追加のメモリが消費され、その結果メモリが使い果たされ、デバイスがクラッシュします。成功した場合、攻撃者はすべての使用可能なメモリリソースを利用して、デバイスをリロードさせる可能性があります。

シスコはこ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。この脆弱性に対処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。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160406-cts1

該当製品

脆弱性のある製品

Cisco TelePresence Serverソフトウェアバージョン4.1(2.29) ~ 4.2(4.17)を実行している次の

Cisco TelePresence Serverデバイスには脆弱性が存在します。

- Cisco TelePresence Server 7010
- Cisco TelePresence Server Mobility Services Engine(MSE)8710
- Cisco TelePresence Server on Multiparty Media 310
- Cisco TelePresence Server on Multiparty Media 320
- Cisco TelePresence Server on Multiparty Media 820
- 仮想マシン(VM)上のCisco TelePresence Server

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。

セキュリティ侵害の痕跡

ほとんどの場合、ログファイルを使用して、デバイスが侵害されたかどうかを判断できます。攻撃者がメモリを枯渇させるためにアクセスできないURLを使用すると、次のログメッセージが表示されます。

HTTP：情報： <IP>:<Port>からの新しい着信接続"____"
HTTP：情報： "____"の新しい受信送信トンネルチャネル
HTTP：警告： <IP>:<Port>からの不完全な接続"____"の失敗

回避策

この脆弱性に対処する回避策はありません。

修正済みソフトウェア

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リリースしています。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、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ 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。

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

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 and Responses アーカイブや後続のアドバイザリを参照して、侵害を受ける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は新規リリースでも継続して適切なサポートが受けられることを確認してください。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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約を結んでいないお客様、およびサードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できないお客様は、Cisco Technical Assistance Center(TAC)に連絡してアップグレードを入手する必要があります。
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

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。

修正済みリリース

この項の該当する表に示すように、適切なリリースにアップグレードする必要があります。本アドバイザリは以下のアドバイザリを含むコレクションの一部です。これらも考慮した上、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。

- cisco-sa-20160406-cts:Cisco TelePresence Serverの巧妙に細工されたIPv6パケット処理におけるDoS脆弱性
- cisco-sa-20160406-cts1:Cisco TelePresence Serverの巧妙に細工されたURL処理におけるDoS脆弱性
- cisco-sa-20160406-cts2:Cisco TelePresence Serverにおける不正なSTUNパケット処理によるDoS脆弱性

次の表では、左の列にシスコ ソフトウェアのメジャー リリースを示します。中央の列が示すのは、本アドバイザリに記載された脆弱性によるメジャー リリースへの影響の有無、また、本脆弱性に対する修正を含む最初のマイナー リリースです。右の列は、メジャー リリースがこのコレクションのアドバイザリに記載した何らかの脆弱性に該当するかどうか、また、これらすべての脆弱性に対する修正を含む最初のリリースを示します。

Cisco TelePresence Server製品	この脆弱性に対する最初の修正リリース	この脆弱性および一連のアドバイザリ
		Cisco TelePresence Serverの巧妙に細工されたIPv6パケット
8710	4.2（4.23）	
		Cisco TelePresence Serverの巧妙に細工されたURL処理
7010/8710/310/320/VM	4.2（4.18）	
820	4.2（3.72）	

不正利用事例と公式発表

Cisco Product Security Incident Response Team (PSIRT) 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やその公表を確認していません。

出典

この脆弱性は内部テストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160406-cts1

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	-	Final	2016年4月6日

利用規約

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。