Cisco TelePresence Serverにおける巧妙に細工されたIPv6パケット処理によるDoS脆弱性

High

アドバイザリーID : cisco-sa-20160406-cts CVE-2016-1346
初公開日 : 2016-04-06 16:00
バージョン 1.0 : Final
CVSSスコア : 7.1
回避策 : Yes
Cisco バグ ID : CSCuu46673

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3.0 ~ 4.2(4.18)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でカーネルパニックを引き起こす可能性があります。

この脆弱性は、特別に巧妙に細工されたIPv6パケットストリームを適切に処理できないことに起因します。エクスプロイトに成功すると、攻撃者はカーネルパニックを引き起こし、デバイスをリブートす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。この脆弱性に対しては回避策があります。

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-cts

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3.0 ~ 4.2(4.18)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 Mobility Services Engine(MSE)8710

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。

回避策

テレビ会議にIPv6を使用しないお客様は、システムが更新されるまで、回避策としてIPv6を無効にすることができます。

次のコマンドを使用してIPv6コールを無効にできます。

Network > Network Settings > IP Configuration

ポートでIPv6を無効にします。

注：TelePresence ServerポートでIPv6を無効にできるのは、IPv4を使用してログインした場合だけです。

終了したら、Update IP Configurationをクリックします。

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ご利用いただいていない場合、また、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場合は、Cisco Technical Assistance Center(TAC)に連絡してアップグレードを入手してください。
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における巧妙に細工されたIPv6パケット処理によるDoS脆弱性
- cisco-sa-20160406-cts1:Cisco TelePresence Serverにおける巧妙に細工されたURL処理による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に記載されているすべての脆弱性に関する最初の修正済みリリース
Cisco TelePresence Serverにおける巧妙に細工されたIPv6パケット処理によるDoS脆弱性		
8710	4.2 (4.23)	4.2 (4.23)
Cisco TelePresence Serverにおける巧妙に細工されたURL処理によるDoS脆弱性		
7010/8710/310/320/VM	4.2 (4.18)	4.2 (4.23)
820	4.2 (3.72)	4.2 (3.72)
Cisco TelePresence Serverにおける不正なSTUNパケットに起因するDoS脆弱性		
7010/8710/310/320/VM	4.2 (4.18)	4.2 (4.23)

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）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-cts

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。