Multiple Vulnerabilities in Cisco TelePresence Multipoint Switch

Advisory ID: cisco-sa-20120711-ctms

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120711-ctms

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 2012 July 11 16:00 UTC (GMT)

目次

要約

Cisco TelePresence Multipoint Switch には、次の脆弱性が含まれます。

- Cisco TelePresence における不正 IP パケットに起因する DoS 脆弱性
- Cisco TelePresence における Cisco Discovery Protocol に起因するリモート実行の脆弱性

Cisco TelePresence における不正 IP パケットに起因する DoS 脆弱性の不正利用に成功した場合、認証されていないリモートの攻撃者がサービス拒否（DoS）状態を発生させ、製品が新規の接続要求に応答しなくなり、サービスまたはプロセスの停止につながる恐れがあります。

Cisco TelePresence における Cisco Discovery Protocol に起因するリモート実行の脆弱性の不正利用に成功した場合、認証されていない近接した攻撃者が特権権限を使用して任意のコードを実行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、次のリンク先で確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120711-ctms

該当製品

脆弱性が存在する製品

Cisco TelePresence Manager、Cisco TelePresence Recording Server、Cisco TelePresence Multipoint Switch、Cisco TelePresence Immersive Endpoint System は、このセキュリティ アドバイザリに記載されている脆弱性の影響を受ける可能性があります。次の表に、各脆弱性に関する具体的な情報を記載します。該当するコードに関する具体的な情報については、このセキュリティ アドバイザリの「ソフトウェア バージョンと修正」セクションを参照してください。

Cisco TelePresence における不正 IP パケットに起因する DoS 脆弱性

Product	Affected
Cisco TelePresence Manager	YES
Cisco TelePresence Recording Server	YES
Cisco TelePresence Multipoint Switch	YES
Cisco TelePresence Immersive Endpoint System	NO

Cisco TelePresence における Cisco Discovery Protocol に起因するリモート実行の脆弱性

Product	Affected
Cisco TelePresence Manager	YES
Cisco TelePresence Recording Server	YES
Cisco TelePresence Multipoint Switch	YES
Cisco TelePresence Immersive Endpoint System	YES

脆弱性が存在する製品に関する詳細情報

このセキュリティ アドバイザリでは、Cisco TelePresence Multipoint Switch に存在する脆弱性について説明します。脆弱性が存在する他の製品に対してこれらの脆弱性が与える可能性のある影響については、次の表に記載された各製品のセキュリティ アドバイザリを参照してください。

Product	Security Advisory Publication Link
Cisco TelePresence Recor	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120711-ctrs

ding Server	
Cisco TelePresence Manager	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120711-ctsman
Cisco TelePresence Immersive Endpoint System	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120711-cts

ソフトウェア バージョンを知る方法

該当するバージョンのソフトウェアが稼働している Cisco TelePresence Multipoint Switch デバイスには脆弱性が存在します。

Cisco TelePresence Multipoint Switch で稼働しているソフトウェア バージョンを確認するには、デバイスへの SSH 接続を確立し、**show version active** および **show version inactive** コマンドを実行します。次のような結果が出力されます。

```
admin: show version active
Active Master Version: 1.7.0.0-471

Active Version Installed Software Options:
No Installed Software Options Found.

admin: show version inactive
Inactive Master Version: 1.6.0.0-342

Inactive Version Installed Software Options:
No Installed Software Options Found.
```

上記の例では、デバイスにはバージョン 1.6.0 および 1.7.0 がロードされており、現在アクティブなバージョンは 1.7.0 です。デバイスは、アクティブとなっているソフトウェア バージョンに存在する脆弱性のみの影響を受けます。

脆弱性が存在しない製品

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 Multipoint Switch は、1 つのミーティングで複数のセグメントに対し、複数

ポイントの Cisco TelePresence ミーティングをサポートするよう設計されています。

このセクションでは、Cisco TelePresence Multipoint Switch に影響を与える各脆弱性に関する追加情報を提供します。

Cisco TelePresence における不正 IP パケットに起因する DoS 脆弱性

脆弱性はオペレーティング システムのネットワーク スタックに存在しており、認証されていないリモートの攻撃者はこれを不正利用してサービス拒否（DoS）状態を発生させることで、デバイスが新規の接続要求に応答しなくなり、一部のサービスおよびプロセスのクラッシュにつながる恐れがあります。この脆弱性は、不正な IP パケットの不適切な処理と、TCP 接続要求または終了が大量に送信されることに起因します。攻撃者は巧妙に細工された一連の不正な IP パケットまたは TCP セグメントを大量に送信することで、この脆弱性を悪用する可能性があります。

この脆弱性は、Cisco Bug ID CSCty11219（ 登録ユーザのみ ）、 CSCty11299（ 登録ユーザのみ ）、 CSCty11323（ 登録ユーザのみ ）、 CSCty11338（ 登録ユーザのみ ）として文書化され、Common Vulnerabilities and Exposures（CVE）ID として ID CVE-2012-3073 が割り当てられています。

Cisco TelePresence における Cisco Discovery Protocol に起因するリモート実行の脆弱性

Cisco Discovery Protocol コンポーネントの実装に存在する、リモートからのコード実行の脆弱性により、認証されていない近接した攻撃者が特権権限を使用して任意のコードを実行できる可能性があります。この脆弱性は、不正な Cisco Discovery Protocol パケットの不適切な処理によるものです。攻撃者は不正な Cisco Discovery Protocol パケットを該当するデバイスに渡すことにより、この脆弱性を悪用する可能性があります。この脆弱性の不正利用に成功した場合、攻撃者は特権権限を使用して任意のコードを実行できる可能性があります。

Cisco Discovery Protocol はデータリンク層（レイヤ 2）で動作するため、攻撃者は該当するデバイスにイーサネット フレームを直接送る方法を必要とします。これは、該当のデバイスがブリッジ型ネットワークに組み込まれている場合や、ネットワーク ハブのようなパーティション機能のないデバイスに接続されている場合に可能になります。

この脆弱性は、Cisco Bug ID CSCtz40965（ 登録ユーザのみ ）として文書化され、CVE ID として CVE-2012-2486 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。このセキュリティ 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導き出すことができます。

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、シスコは個々の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/

CSCty11219, CSCty11299, CSCty11323 and CSCty11338 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	

CSCtz40965 Calculate the environmental score of					
CVSS Base Score - **8.3**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Adjacent Network	Low	None	Complete	Complete	Complete
CVSS Temporal Score - **6.9**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

これらの脆弱性の不正利用に成功した場合、 DoS 状態が引き起こされ、製品が新規の接続要求に

応答しなくなり、サービスまたはプロセスの停止が発生したり 、あるいは特権権限で任意のコードが実行され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

このセクションでは、Cisco TelePresence Multipoint Switch に影響を与える各脆弱性について、該当するリリースおよび修正に関する詳細情報を提供します。

Cisco TelePresence における不正 IP パケットに起因する DoS 脆弱性

Version	First Fixed In
Prior to 1.6	1.8.1
1.6	1.8.1
1.7	1.8.1
1.8	1.8.1
1.9	Not Vulnerable

Cisco TelePresence における Cisco Discovery Protocol に起因するリモート実行の脆弱性

Version	First Fixed In
Prior to 1.6	1.9.0
1.6	1.9.0
1.7	1.9.0
1.8	1.9.0
1.9	Not Vulnerable

推奨リリース

次の表に、このアドバイザリで説明のあるすべての脆弱性への修正が含まれたリリースに関する情報を記載します。

Version	Recommended Release
Prior to 1.6	Upgrade to 1.9.0
1.6	Upgrade to 1.9.0
1.7	Upgrade to 1.9.0
1.8	Upgrade to 1.9.0

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、本アドバイザリ以降に公開のアドバイザリを参照して、起こりうる障害と完全なアップグレード ソリューションを判断してください。

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しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。情報が不明確な場合は、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。

回避策

これらの脆弱性を軽減する回避策はありません。

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に特有の問題に関してご確認ください。

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、適切な処置について支援を受けてください。

回避策の効果は、使用製品、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のお客様の状況に依存します。影響製品およびリリースが多種多様であるため、回避策を実際に展開する前に、対象とする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か、お客様のサービス プロバイダーやサポート会社にご相談ください。

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。

- +1 800 553 2447（北米内からのフリー ダイヤル）
- +1 408 526 7209（北米以外からの有料通話）
- 電子メール：tac@cisco.com

無償アップグレードの対象であることをご証明いただくために、製品のシリアル番号と、このア

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 を通して無償アップグレードをお求めください。

さまざまな言語向けの各地の電話番号、説明、電子メール 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を参照してください。
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

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。

これらの脆弱性は、シスコの社内テストで発見されたものです。

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。またシスコシステムズ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 Intelligence Operations ポータルに掲載されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120711-ctms

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電子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
- full-disclosure@lists.grok.org.uk

このアドバイザリに関する今後の更新があれば、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。このアドバイザリの URL で更新をご確認いただくことができます。

更新履歴

Revision 1.0	2012-July-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支援、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について詳しく知るには、Cisco.com の http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html にアクセスしてください。この Web ページには、シスコのセキュリティ アドバイザリ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。すべてのシスコ セキュリティ アドバイザリは、http://www.cisco.com/go/psirt/ で確認することができます。