Cisco TelePresence Recording Serverの複数の脆弱性

アドバイザリーID : cisco-sa-20120711-ctrs
初公開日 : 2012-07-11 16:00
最終更新日 : 2012-07-31 19:04
バージョン 1.1 : Final
CVSSスコア : 9.0
回避策 : No Workarounds available
Cisco バグ ID : CSCti21830 CSCti21851 CSCtj19086 CSCth85804 CSCtz40947 CSCty11219 CSCtz40941 CSCty11338 CSCtz40953 CSCtz40965 CSCty11323 CSCty11299 CSCtj19078 CSCtj19100

CVE-2012-2486
CVE-2012-3073
CVE-2012-3076

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 Recording Serverには次の脆弱性が含まれています。

- Cisco TelePresenceにおける不正なIPパケットに起因するDoS脆弱性
- Cisco TelePresence Webインターフェイスコマンドインジェクション
- Cisco TelePresence Cisco Discovery Protocolのリモートコード実行の脆弱性

Cisco TelePresenceの不正なIPパケットによるサービス妨害(DoS)の脆弱性 が不正利用されると、リモートの認証されていない攻撃者によってサービス妨害(DoS)状態が発生し、製品が新しい接続要求に応答できなくなり、一部のサービスやプロセスがクラッシュする可能性があります。

Cisco TelePresence Web Interfaceのコマンドインジェクションの不正利用により、認証されたリモートの攻撃者が、昇格された特権を使用して基盤となるオペレーティングシステムで任意のコマンドを実行する可能性があります。

Cisco TelePresence Cisco Discovery Protocolのリモートコード実行の脆弱性 の不正利用により、認証されていない隣接する攻撃者が昇格された特権で任意のコードを実行する可能性があります。

シスコは、コマンドおよびコード実行の脆弱性を解決するアップデート済みソフトウェアをリリースしています。 現在のところ、不正なIPパケットに関するDoS脆弱性を解決する計画はありま

せん。この製品は現在サポートされていません。

これらの脆弱性を軽減する回避策はありません。

お客様は、シスコの営業担当者に連絡して、Cisco TelePresence Recording Serverを担当する事業部門を確認する必要があります。

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-20120711-ctrs

該当製品

脆弱性のある製品

Cisco TelePresence Manager、Cisco TelePresence Recording Server、Cisco TelePresence Multipoint Switch、および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示します。

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

製品	該当
Cisco TelePresence Manager	Yes
Cisco TelePresenceレコーディングサーバ	Yes
Cisco TelePresence Multipoint Switch	Yes
Cisco TelePresenceイマーシブエンドポイントシステム	いいえ

Cisco TelePresence Webインターフェイスコマンドインジェクション

製品	該当
Cisco TelePresence Manager	いいえ
Cisco TelePresenceレコーディングサーバ	Yes
Cisco TelePresence Multipoint Switch	いい

	え
Cisco TelePresenceイマーシブエンドポイントシステム	いいえ

Cisco TelePresence Cisco Discovery Protocolのリモートコード実行の脆弱性

製品	該当
Cisco TelePresence Manager	Yes
Cisco TelePresenceレコーディングサーバ	Yes
Cisco TelePresence Multipoint Switch	Yes
Cisco TelePresenceイマーシブエンドポイントシステム	Yes

脆弱性が存在する製品の詳細情報

このセキュリティアドバイザリでは、Cisco TelePresence Recording Serverの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影響については、次の表のリンク先にある特定の製品のセキュリティアドバイザリを参照してください。

製品	セキュリティアドバイザリパブリケーショ
Cisco TelePresence Multipoint Switch	https://sec.cloudapps.cisco.com/security/center/content/CiscoSec 20120711-ctms
Cisco TelePresence Manager	https://sec.cloudapps.cisco.com/security/center/content/CiscoSec 20120711-ctsman
Cisco TelePresenceイマーシブエンドポイントシステム	https://sec.cloudapps.cisco.com/security/center/content/CiscoSec 20120711-cts

ソフトウェアバージョンの判別方法

該当するバージョンのソフトウェアを実行しているCisco TelePresence Recording Serverデバイスが影響を受けます。

Cisco TelePresence Recording Serverで実行されているソフトウェアの現在の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コマンドとshow version

inactiveコマンドを発行します。出力は次の例のようになります。

```
<#root>

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.
```

前記の例では、システムにバージョン1.6.0と1.7.0がデバイスにロードされており、バージョン1.7.0が現在アクティブです。デバイスは、アクティブなソフトウェアバージョンの脆弱性の影響のみを受けます。

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 Recording Serverは、高品質の録音機能を提供します。

このセクションでは、Cisco TelePresence Recording Server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における不正なIPパケットに起因するDoS脆弱性

オペレーティングシステムのネットワークスタックには脆弱性があり、認証されていないリモートの攻撃者がサービス妨害(DoS)状態を作成し、デバイスが新しい接続要求に応答できなくなり、一部のサービスとプロセスのクラッシュを引き起こす可能性があります。この脆弱性は、不正なIPパケットやTCP接続要求または終了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、この脆弱性を不正利用する可能性があります。

本脆弱性は、Cisco Bug ID CSCti21830(登録ユーザ専用) に文書化され、Common Vulnerabilities

and Exposures(CVE)IDとしてCVE-2012-3073が割り当てられています。

Cisco TelePresence Webインターフェイスコマンドインジェクション

管理Webインターフェイスには、認証されたリモートの攻撃者によるコマンドインジェクション攻撃を可能にする脆弱性が存在します。 攻撃者はこの問題を利用して悪意のある要求をデバイスに送信し、処理されると、攻撃者が特権権限で任意のコマンドを実行できる可能性があります。

この脆弱性は、Cisco Bug IDCSCth85804 (登録 ユーザ専用)として文書化され、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2012-3076が割り当てられています。

Cisco TelePresence Cisco Discovery Protocolのリモートコード実行の脆弱性

Cisco Discovery Protocol(CDP)コンポーネントの実装におけるリモートコード実行の脆弱性により、認証されていない隣接する攻撃者が特権権限を使用して任意のコードを実行する可能性があります。この脆弱性は、不正なCisco Discovery Protocolパケットを適切に処理できないことに起因します。 攻撃者は、不正なCisco Discovery Protocolパケットを該当デバイスに渡すことで、この脆弱性を不正利用する可能性があります。 この脆弱性の不正利用に成功すると、攻撃者は昇格された特権で任意のコードを実行する可能性があります。

Cisco Discovery Protocol(CDP)はデータリンク層（レイヤ2）で動作するため、攻撃者はイーサネットフレームを該当デバイスに直接送信する方法が必要です。このアクションは、影響を受けるシステムがブリッジ型ネットワークの一部であるか、ネットワークハブなどの非パーティションデバイスに接続されている場合に可能です。

本脆弱性は、Cisco Bug ID CSCtz40953(登録ユーザ専用) に文書化されており、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2012-2486が割り当てられています。

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

このセクションでは、影響を受けるリリースの詳細について説明します。Cisco TelePresence Recording Serverは現在開発中ではないため、これらの問題は修正されません。

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

バージョン	修復方法
1.6	修正なし

1.6	修正なし
1.7	修正なし
1.8	修正なし

Cisco TelePresence Webインターフェイスコマンドインジェクション

バージョン	修復方法
1.6	1.8.0
1.6	1.8.0
1.7	1.8.0
1.8	1.8.0

Cisco TelePresence Cisco Discovery Protocolのリモートコード実行の脆弱性

バージョン	Release
1.6	1.8.1
1.6	1.8.1
1.7	1.8.1
1.8	1.8.1

推奨リリース

次の表に、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に対する修正を含むリリースに関する情報を示します。

バージョン	Release
1.6	1.8.1 以降
1.6	1.8.1 以降
1.7	1.8.1 以降
1.8	1.8.1 以降

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)または契約し

たメンテナンスプロバイダーにお問い合わせください。

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。

これらの脆弱性は、Cisco TelePresence Recording Serverの内部セキュリティ監査中に発見されたものです。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120711-ctrs

改訂履歴

リビジョン 1.1	2012年7月 31日	誤ったハイパーリンクを修正。
リビジョン 1.0	2012年7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。