Cisco TelePresence Recording Serverの複数の脆弱性

アドバイザリーID : cisco-sa-20110223-telepresence-ctrs
初公開日 : 2011-02-23 16:00
バージョン 1.0 : Final
CVSSスコア : 10.0
回避策 : No Workarounds available
Cisco バグ ID :

CVE-2011-0391
CVE-2011-0383
CVE-2011-0384
CVE-2011-0392
CVE-2011-0382
CVE-2011-0385
CVE-2011-0386

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には複数の脆弱性が存在します。このセキュリティアドバイザリでは、次の脆弱性の概要について説明します。

- 認証されていないJavaサーブレットへのアクセス
- Common Gateway Interface(CGI)コマンドインジェクション
- 認証されていない任意のファイルのアップロード
- XML-Remote Procedure Call(RPC)の任意のファイルの上書き
- Cisco Discovery Protocolのリモートコード実行
- アドホック録音のDoS
- Java Remote Method Invocation(RMI)のサービス拒否
- 認証されていないXML-RPCインターフェイス

他のCisco TelePresenceアドバイザリでの重複する問題の特定

Java Servletへの未認証アクセスの脆弱性は、Cisco TelePresence Multipoint SwitchおよびRecording Serverに影響します。各コンポーネントに関連する不具合は、関連する各アドバイザリで説明されています。これらの不具合のCisco Bug IDは次のとおりです。

- Cisco TelePresence Multipoint Switch:CSCtf42008
- Cisco TelePresence Recording Server:CSCtf42005

Unauthenticated Arbitrary File Uploadの脆弱性は、Cisco TelePresence Multipoint SwitchおよびRecording Serverに影響します。各コンポーネントに関連する不具合は、関連する各アドバイザリで説明されています。これらの不具合のCisco Bug IDは次のとおりです。

- Cisco TelePresence Multipoint Switch:CSCth61065
- Cisco TelePresence Recording Server:CSCth85786

Cisco Discovery Protocolのリモートコード実行の脆弱性は、Cisco TelePresenceエンドポイント、Manager、Multipoint Switch、およびRecording Serverに影響します。各コンポーネントに関連する不具合は、関連する各アドバイザリで説明されています。これらの不具合のCisco Bug IDは次のとおりです。

- Cisco TelePresenceエンドポイントデバイス – CSCtd75754
- Cisco TelePresence Manager - CSCtd75761
- Cisco TelePresence Multipoint Switch:CSCtd75766
- Cisco TelePresence Recording Server:CSCtd75769

Java RMIのDoS脆弱性は、Cisco TelePresence Multipoint SwitchおよびRecording Serverに影響します。各コンポーネントに関連する不具合は、関連する各アドバイザリで説明されています。これらの不具合のCisco Bug IDは次のとおりです。

- Cisco TelePresence Multipoint Switch:CSCtg35825
- Cisco TelePresence Recording Server:CSCtg35830

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110223-telepresence-ctrs で公開されています。

該当製品

これらの脆弱性は、Cisco TelePresence Recording Serverに影響します。Cisco TelePresenceソフトウェアの1.7.1より前のすべてのリリースは、このアドバイザリに記載されている1つ以上の脆弱性の影響を受けます。

次の表に、影響を受けるソフトウェアリリースに関する情報を示します。

説明	Cisco Bug ID	影響を受けるソフトウェアリリース
認証されていないJavaサーブレットへのアクセス	0.CSCtf42005	1.6.x
CGIコマンドインジェクション	0.CSCtf97221	1.6.x
認証されていない任意のファイルのアップロード	0.CSCth85786	1.6.x
XML-RPCの任意のファイルの上書き	0.CSCti50739	1.6.x、1.7.0
Cisco Discovery Protocolのリモートコード実行	0.CSCtd75769	1.6.x
アドホック録音のDoS	0.CSCtf97205	1.6.x
Java RMIのDoS	0.CSCtg35830	1.6.x
認証されていないXML-RPCインターフェイス	0.CSCtg35833	1.6.x

脆弱性のある製品

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、SSH経由でデバイスにアクセスし、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: 1.7.0.0-151

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

admin:

show version inactive

Inactive Master Version: 1.6.2.0-237

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1.6.2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に存在する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ソリューションを使用すると、同僚、見込み客、およびパートナーと、ネットワークを介して、臨場感のある対面式のコミュニケーションおよびコラボレーションを、相手が異なる半球にいる場合でも行うことができます。

このセキュリティアドバイザリでは、Cisco TelePresence Recording Serverの複数の個別の脆弱性について説明します。これらの脆弱性は相互に関連していません。

認証されていないJavaサーブレットへのアクセス

Cisco TelePresence Recording Server内のJava Servletフレームワーク経由で配信される多数の機密Javaサーブレットにより、リモートの認証されていない攻撃者が管理ユーザに制限する必要のあるアクションを実行する可能性があります。この脆弱性を不正利用するには、攻撃者が該当デバイスのTCPポート80、TCPポート443、またはTCPポート8080に、巧妙に細工された要求を送

信する必要があります。

攻撃者がこれらの脆弱性を不正利用するには、3ウェイTCPハンドシェイクを実行し、有効なセッションを確立する必要があります。

- Cisco TelePresence Recording Server:CSCtf42005(登録ユーザ専用)にCVE IDとしてCVE-2011-0383が割り当てられています。

CGIコマンドインジェクション

Cisco TelePresence Recording ServerにはCGIコマンドインジェクションの脆弱性が存在し、認証されていないリモートの攻撃者が特権権限を使用して任意のコマンドを実行できる可能性があります。攻撃者がこの脆弱性を不正利用するには、TCPポート443経由で該当デバイスに不正な要求を送信できる必要があります。

攻撃者がこれらの脆弱性を不正利用するには、3ウェイTCPハンドシェイクを実行し、有効なセッションを確立する必要があります。

- Cisco TelePresence Recording Server:CSCtf97221(登録ユーザ専用)にCVE IDとしてCVE-2011-0382が割り当てられています。

認証されていない任意のファイルのアップロード

Cisco TelePresence Recording Serverの管理Webインターフェイスには、任意のファイルアップロードの脆弱性が存在します。認証されていないリモートの攻撃者は、巧妙に細工された要求を該当デバイスに送信することで、デバイス上の任意の場所にコンテンツを配置する可能性があります。この脆弱性を不正利用するには、攻撃者は該当デバイスのTCPポート80または443に巧妙に細工された要求を送信する必要があります。

攻撃者がこの脆弱性を不正利用するには、3ウェイTCPハンドシェイクを実行し、有効なセッションを確立する必要があります。

- Cisco TelePresence Recording Server:CSCth85786(登録ユーザ専用)にCVE IDとしてCVE-2011-0385が割り当てられています。

XML-RPCの任意のファイルの上書き

Cisco TelePresence Recording Serverデバイスには、任意のファイルを上書きする脆弱性が存在します。この脆弱性により、認証されていないリモートの攻撃者がロギングデータで任意のファイルを上書きする可能性があります。この脆弱性は、該当デバイスを完全に制御するために利用される可能性があります。この脆弱性を不正利用するには、攻撃者はTCPポート12102または12104を介して該当デバイスに不正な要求を送信する必要があります。

攻撃者がこの脆弱性を不正利用するには、3ウェイTCPハンドシェイクを実行し、有効なセッションを確立する必要があります。

- Cisco TelePresence Recording Server:CSCti50739(登録ユーザ専用)にCVE IDとしてCVE-2011-0386が割り当てられています。

Cisco Discovery Protocolのリモートコード実行

Cisco TelePresence Recording Serverデバイスには、リモートコード実行の脆弱性が存在します。この脆弱性により、認証されていない隣接する攻撃者がバッファオーバーフロー状態を引き起こす可能性があります。この脆弱性を不正利用するには、攻撃者は該当システムに悪意のあるCisco Discovery Protocolパケットを送信する必要があります。

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を持っている必要があります。これは、該当す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パーティション化されていないデバイスに接続されている場合に発生する可能性があります。

- Cisco TelePresence Recording Server:CSCtd75769(登録ユーザ専用)にCVE IDとしてCVE-2011-0379が割り当てられています。

アドホック録音のDoS

Cisco TelePresence Recording Serverデバイスには、サービス拒否の脆弱性が存在します。この脆弱性により、認証されていないリモートの攻撃者がデバイス上のすべての録音および再生スレッドを消費させる可能性があります。機能を回復するには、該当するデバイスの再起動が必要になる場合があります。攻撃者がこの脆弱性を不正利用するには、TCPポート80経由で該当デバイスに不正な要求を送信できる必要があります。

攻撃者がこの脆弱性を不正利用するには、3ウェイTCPハンドシェイクを実行し、有効なセッションを確立する必要があります。

- Cisco TelePresence Recording Server:CSCtf97205(登録ユーザ専用)にCVE IDとしてCVE-2011-0391が割り当てられています。

Java RMIのDoS

Cisco TelePresence Recording Serverデバイスには、Java ServletフレームワークのRMIインターフェイスへのアクセスを適切に制限できないサービス拒否の脆弱性が存在します。認証されていないリモートの攻撃者が、巧妙に細工された一連の要求を発行することにより、Servletホストでメモリ不足状態を引き起こす可能性があります。攻撃者がこの脆弱性を不正利用するには、TCPポート8999で該当デバイスと通信できる必要があります。

攻撃者がこの脆弱性を不正利用するには、3ウェイTCPハンドシェイクを実行し、有効なセッションを確立する必要があります。

- Cisco TelePresence Recording Server:CSCtg35830(登録ユーザ専用)にCVE IDとしてCVE-

2011-0388が割り当てられています。

認証されていないXML-RPCインターフェイス

Cisco TelePresence Recording Serverデバイス内に、認証されていないXML-RPCインターフェイスが存在する。この脆弱性により、認証されていないリモートの攻撃者が、許可されたユーザに制限する必要がある限られた数のアクションをシステムで実行できる可能性があります。攻撃者がこの脆弱性を不正利用するには、TCPポート8080で該当デバイスと通信できる必要があります。

攻撃者がこの脆弱性を不正利用するには、3ウェイTCPハンドシェイクを実行し、有効なセッションを確立する必要があります。

- Cisco TelePresence Recording Server:CSCtg35833(登録ユーザ専用)にCVE IDとしてCVE-2011-0392が割り当てられています。

回避策

特定された脆弱性に対するデバイスベースまたはシステムベースの回避策はありません。

ネットワーク内の Cisco デバイスに導入できる追加の緩和策については、このアドバイザリに関連する Cisco 適用インテリジェンス（ https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110223-telepresence ）を参照してください。

修正済みソフトウェア

アップグレードを検討する場合は、http://www.cisco.com/go/psirt と後続のアドバイザリも参照して、問題の解決状況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機器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。情報に不明な点がある場合は、Cisco Technical Assistance Center（TAC）または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

次のCisco TelePresence System Softwareの表の各行は、このアドバイザリで説明されているすべてのセキュリティの問題と、セキュリティに関連しないその他の問題を解決するための、特定の不具合、最初の修正リリース、および推奨リリースを定義しています。シスコでは、表の「推奨リリース」列のリリース、またはそれ以降のリリースにアップグレードすることを推奨します。

脆弱性	Bug ID	コンポーネント	最初の修正済	推奨リリース

			みバージョン	
認証されていないJavaサーブレットへのアクセス	0.CSCtf42005	Cisco TelePresenceレコーディングサーバ	1.6.2	1.7.1
CGIコマンドインジェクション	0.CSCtf97221	Cisco TelePresenceレコーディングサーバ	1.6.2	1.7.1
認証されていない任意のファイルのアップロード	0.CSCth85786	Cisco TelePresenceレコーディングサーバ	1.7.0	1.7.1
XML-RPCの任意のファイルの上書き	0.CSCti50739	Cisco TelePresenceレコーディングサーバ	1.7.1	1.7.1
Cisco Discovery Protocolのリモートコード実行	0.CSCtd75769	Cisco TelePresenceレコーディングサーバ	1.7.0	1.7.1

アドホック録音のDoS	0.CSCtf97205	Cisco TelePresenceレコーディングサーバ	1.7.0	1.7.1
Java RMIのDoS	0.CSCtg35830	Cisco TelePresenceレコーディングサーバ	1.7.0	1.7.1
認証されていないXML-RPCインターフェイス	0.CSCtg35833	Cisco TelePresenceレコーディングサーバ	1.7.0	1.7.1

シスコでは、Cisco TelePresenceソリューションのすべてのコンポーネントを1.7.1以降にアップグレードすることを推奨しています。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

このアドバイザリで説明されている脆弱性の公表や悪用に関する情報は Cisco PSIRT には寄せられていません。

このセキュリティアドバイザリで特定されたすべての脆弱性は、シスコ社内で発見されたものです。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110223-telepresence-ctrs

改訂履歴

リビジョン 1.0	2011年2月23日	初版リリース

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。