Cisco TelePresence Managerの複数の脆弱性

アドバイザリーID : cisco-sa-20110223-telepresence-ctsman
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-2011-0390
CVE-2011-0380
CVE-2011-0381

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 Manager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、次の脆弱性の詳細について説明します。

- Simple Object Access Protocol(SOAP)認証バイパス
- Java Remote Method Invocation(RMI)のコマンドインジェクション
- Cisco Discovery Protocolのリモートコード実行

他のCisco TelePresenceアドバイザリでの重複する問題の特定

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。不具合と各コンポーネントの関係については、関連する各アドバイザリで詳しく説明します。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

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

該当製品

これらの脆弱性は、Cisco TelePresence Managerに影響を与えます。1.7.0より前のCisco TelePresence Managerソフトウェアのリリースは、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る可能性があります。

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
SOAP認証バイパス	0.CSCtc59562	1.2.x、1.3.x、1.4.x、1.5.x、1.6.x
Java RMIコマンドインジェクション	CSCtf9085	1.2.x、1.3.x、1.4.x、1.5.x、1.6.x
Cisco Discovery Protocolのリモートコード実行	0.CSCtd75761	1.2.x、1.3.x、1.4.x、1.5.x、1.6.2

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 Managerデバイスが影響を受けます。

Cisco TelePresence Manager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 Manager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。

SOAP認証バイパス

認証バイパスの脆弱性が存在するため、リモートの認証されていない攻撃者がCisco TelePresence ManagerのSOAPインターフェイスを介して利用可能な任意の方法を呼び出す可能性があります。攻撃者は、該当するデバイスのTCPポート8080または8443で脆弱性をトリガーするように設計された不正なSOAP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 Manager:CSCtc59562(登録ユーザ専用)にCommon Vulnerabilities and Exposures(CVE)IDとしてCVE-2011-0380が割り当てられています。

Java RMIコマンドインジェクション

コマンドインジェクションの脆弱性は、Cisco TelePresence Managerで公開されるJava RMIインターフェイスに存在します。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、昇格された特権を使用してデバイスに対して多数のアクションを実行できる可能性があります。攻撃者は、該当するデバイスのTCPポート1100または32000に、巧妙に細工された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 Manager:CSCtf97085(登録ユーザ専用)にCVE IDとしてCVE-2011-0381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 Manager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。攻撃者がこの脆弱性を不正利用するには、悪意のあるCisco Discovery Protocolパケットを該当システムに送信できる必要があります。

Cisco Discovery Protocolはレイヤ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。この問題は、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 Manager:CSCtd75761(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。

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既知の回避策はありません。

ネットワーク内のシスコデバイスに適用可能な他の対応策は、このアドバイザリの付属ドキュメントである『Cisco Applied Intelligence』にて参照できます。https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110223-telepresence

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脆弱性と、セキュリティに関連しないその他の不具合を解決するための、特定の脆弱性、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お勧めします。

脆弱性	Bug ID	コンポーネント	最初の修正済みバージョン	推奨リリース
SOAP認証バイパス	0.CSCtc59562	Cisco TelePresence Manager	1.7.0	1.7.1
Java RMIコマンドインジェクション	0.CSCtf97085	Cisco TelePresence Manager	1.7.0	1.7.1
Cisco Discovery Protocolのリモートコード実行	0.CSCtd75761	Cisco TelePresence Manager	1.7.0	1.7.1

Cisco TelePresenceソリューションのすべてのコンポーネントをリリース1.7.1以降にアップグレードすることを推奨します。

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-ctsman

改訂履歴

リビジョン 1.0	2011年2月23日	初回公開リリース

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。