

Cisco TelePresence Manager の多重脆弱点

Critical	アドバイザーID : cisco-sa-20110223-telepresence-ctsman	CVE-2011-0390
	初公開日 : 2011-02-23 16:00	CVE-2011-0380
	バージョン 1.0 : Final	CVE-2011-0381
	CVSSスコア : 10.0	
	回避策 : Yes	
	Cisco バグ ID :	

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

多重脆弱点は Cisco TelePresence Manager にあります。この Security Advisory は次の脆弱性の詳細を概説します:

- シンプル オブジェクト アクセスプロトコル (石鹼) 認証 バイパス
- Java Remote Method Invocation (RMI) コマンド インジェクト
- Cisco Discovery Protocol (CDP) リモート コード 実行

他の Cisco TelePresence アドバイザリの重複した問題識別

Cisco Discovery Protocol (CDP) リモート コード 実行脆弱性は Cisco TelePresence エンドポイント、マネージャ、Multipoint Switch および Recording Server に影響を与えます。問題が各コンポーネントにどのようにについての関連しているか詳細は各々の関連するアドバイザーでカバーされます。これらの問題のための Cisco バグ ID は次の通りです:

- Cisco TelePresence エンドポイント デバイス- CSCtd75754
- Cisco TelePresence Manager - CSCtd75761
- Cisco TelePresence マルチポイント スイッチ- CSCtd75766
- Cisco TelePresence Recording Server - CSCtd75769

このアドバイザーは <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110223-telepresence-ctsman> で掲示されます。

該当製品

修正済みソフトウェア

影響を受けたソフトウェアのバージョンを実行している Cisco TelePresence Manager デバイスは影響を受けています。

Cisco TelePresence Manager で動作しているソフトウェアの最新バージョンを判別するために、デバイスへの SSH 接続を確立し、**show version アクティブ**および **show version 非アクティブ** コマンドを発行して下さい。出力は次の例に類似するはずです:

```
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.
```

前述の例では、システムにデバイスでロードされるバージョン 1.6.0 および 1.7.0 がありバージョン 1.7.0 は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 バージョンにある脆弱性からだけ影響を受けます。

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。

改訂履歴

リビジョン 1.0	2011-February-23	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、単独の転載や意識を施した場合、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。