Cisco TelePresence マルチポイント スイッチの多重 脆弱点

High

アドバイザリーID : cisco-sa-20110223-telepresence-ctms
初公開日 : 2011-02-23 16:00
最終更新日 : 2011-03-09 21:00
バージョン 1.1 : Final
CVSSスコア : 8.0
回避策 : Yes
Cisco バグ ID :

CVE-2011-0389
CVE-2011-0387
CVE-2011-0388

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 マルチポイント スイッチの内にあります。 この Security Advisory は次の脆弱性の詳細を概説します:

- Java Servlet 非認証アクセス
- 非認証任意 ファイル アップロード
- Cisco Discovery Protocol（CDP）リモート コード 実行
- Servlet 不正 な アクセス
- Java RMI Denial of Service（DoS/DDoS）
- Real-time Transport Control Protocol Denial of Service（DoS/DDoS）
- XML リモート プロシージャ コール（RPC） Denial of Service（DoS/DDoS）

他の Cisco TelePresence アドバイザリの重複した問題識別

Java Servlet 非認証アクセスの脆弱性は Cisco TelePresence マルチポイント スイッチおよび Recording Server に影響を与えます。 各コンポーネントという意味での問題は各々の関連するアドバイザリで力バーされます。 これらの問題のための Cisco バグ ID は次の通りです:

- Cisco TelePresence マルチポイント スイッチ- CSCtf42008
- Cisco TelePresence Recording Server - CSCtf42005

非認証任意 ファイル アップロード脆弱性は Cisco TelePresence マルチポイント スイッチおよび Recording Server に影響を与えます。 各コンポーネントという意味での問題は各々の関連するアドバイザリで力バーされます。 これらの問題のための Cisco バグ ID は次の通りです:

- Cisco TelePresence マルチポイント スイッチ- CSCth61065
- Cisco TelePresence Recording Server - CSCth85786

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 デバイス、マネージャ、Multipoint Switch および Recording Server に影響を与えます。 各コンポーネントという意味での問題は各々の関連するアドバイザリでカバーされます。 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

Java RMI サービス拒否の脆弱性は Cisco TelePresence マルチポイント スイッチおよび Recording Server に影響を与えます。 各コンポーネントという意味での問題は各々の関連するアドバイザリでカバーされます。 これらの問題のための Cisco バグ ID は次の通りです:

- Cisco TelePresence マルチポイント スイッチ- CSCtg35830
- Cisco TelePresence Recording Server - CSCtg35825

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110223-telepresence-ctms で掲示されます。

該当製品

修正済みソフトウェア

Cisco TelePresence マルチポイント スイッチ実行するデバイスは影響を受けたソフトウェアのバージョン影響を受けています。

Cisco TelePresence マルチポイント スイッチで動作す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: 1.6.1.0-336

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 1.6.1 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 バージョンの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

その他のCisco製品は現在これらの脆弱性から影響を受けるために知られていません

改訂履歴

リビジョン1.1	2011-March-9	CSCtj44534（CVE-2011-0390）に関する新しい情報を提供し、この問題を解決するソフトウェアに推定アベイラビリティを提供する諮問更新済。
リビジョン1.0	2011-February-23	初回公開リリース

利用規約