Cisco Unified コンタクトセンターおよび IP Contact Center JTapi Gateway サービス拒否の脆弱性

Medium	**アドバイザリーID :** Cisco-SA-20070110-CVE-2007-0198 **初公開日 :** 2007-01-10 17:06 **バージョン 1.0 :** Final **CVSSスコア :** 3.3 **回避策 :** Yes **Cisco バグ ID :**	CVE-2007-0198

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 Unified コンタクトセンターおよび Cisco IP Contact Center バージョン 5.0、6.0、7.0、および 7.1 は非認証を可能にする可能性があるサービス拒否（DoS）状態を作成するために脆弱性がリモート攻撃者含まれています。

脆弱性は予想外接続の不十分な処理が原因です。Â は JTapi Gateway サービスの再始動を引き起こす影響を受けたサーバに接続によって非認証、リモート攻撃者この脆弱性を不正利用する可能性があります。サービスが再起動に成功するまで Â は、ユーザまたは receiveÂ あらゆる新しい呼び出し開始できません。Â 既存の呼出しは影響を受けていません。

Cisco は Security Advisory のこの脆弱性を確認し、更新済ソフトウェアをリリースしました。

危険な状態のシステムは脆弱 な ソフトウェアを稼動するおよび信頼できないネットワークから接続を許可するそれらのシステムです。この脆弱性を不正利用する Â は JTapi Gateway サーバが受信するために設定された TCPポートへの攻撃者接続に成功する必要があります。Â は正確なポート番号 攻撃者に設定および未知数に依存するかもしれません。Â はまた自動化されたスキャン ツールによってネットワーク セキュリティ監査の間に脆弱性不注意に引き起こされるかもしれません。

ベンダー CVSS スコアは完全なアベイラビリティインパクトを示します; しかし Â は脆弱性から、Â JTapi Gateway だけ影響を受け、現在の呼び出しは処理され続けます。Â それはこれが部分

的なアベイラビリティインパクトだけを構成する IntelliShield チームの意見です。

不正利用の成功の結果として、攻撃者は JTapi Gateway サービスを再開できます。サービスが利用できない間、Â は、ユーザ新しい呼び出しを作成できませんが既存の呼出しはまだ標準として機能します。サービスが再起動するとき Â は、自動的におよび介入のない、ユーザ標準として新しい呼び出しを作成し続けることができます。耐久性がある努力が絶えずサービスを利用できないするかもしれない間、Â はユーザにだけ単一 攻撃一時的にサービスを否定します。冗長 な サーバが設定された場合 Â は、すべてのコール処理 機能動作し続けます。しかし Â は、攻撃者同じ影響を実現させるのに冗長 システムの同じ脆弱性を不正利用する可能性があります。

該当製品

修正済みソフトウェア

Cisco Unified 連絡先 CenterÂ および Cisco IP Contact Center バージョン 5.0、6.0、7.0、または 7.1 は脆弱です。

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

バージョン	説明	Section	ステータス	日付
1.0	初版リリース	該当なし	Final	2007-Jan-10

利用規約