

Cisco Unified Contact CenterおよびIP Contact Center JTapi Gatewayの脆弱性

severity アドバイザリーID : cisco-sa-20070110-jtapi
初公開日 : 2007-01-10 16:00
バージョン 1.1 : Final
回避策 : No Workarounds available
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

Cisco Unified Contact Center Enterprise、Cisco Unified Contact Center Hosted、Cisco IP Contact Center Enterprise、およびCisco IP Contact Center Hostedの各エディションは、JTapi Gatewayプロセスの再起動を引き起こす可能性がある脆弱性の影響を受けます。このプロセスが再起動するまで、新しい接続は処理できません。既存の接続は引き続き機能します。

Cisco Unified Contact Center ExpressおよびCisco IP Contact Center Expressは、この脆弱性の影響を受けません。

シスコでは、該当するお客様用に、この脆弱性に対応する無償ソフトウェアを提供しております。

このアドバイザリーは、

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070110-jtapi>で公開されています。

該当製品

脆弱性のある製品

Cisco Unified Contact Center Enterprise、Cisco Unified Contact Center Hosted、Cisco IP Contact Center Enterprise、およびCisco IP Contact Center Hostedエディションのすべてのバージョンが影響を受けます。

脆弱性を含んでいないことが確認された製品

- Cisco Unified Contact Center ExpressおよびCisco IP Contact Center Expressエディションは影響を受けません。
- Cisco Unified Intelligent Contact Management EnterpriseおよびHostedは影響を受けません。

この脆弱性に該当するその他の Cisco 製品は現在のところ見つかりません。

詳細

Cisco Unified Contact Center Enterprise(旧称Cisco IP Contact Center(IPCC)Enterprise)は、Cisco Unified Communicationsシステムに不可欠なコンポーネントであり、複数の通信チャネルを組み合わせ、インテリジェントなルーティングと呼処理を実現します。

Cisco Unified Contact Center Hosted(旧称Cisco IP Contact Center(IPCC)Hosted)は、カスタマーインタラクショナルネットワークへの移行を可能にするプラットフォームです。カスタマーインタラクショナルネットワークは、マルチチャネルサービスと顧客関係管理アプリケーションのスイートで構成される、分散型のIPベースのカスタマーサービスインフラストラクチャです。

脆弱性は、JTapi Gatewayプロセスの再起動を引き起こす可能性があるCisco Unified Contact Center Enterprise、Cisco Unified Contact Center Hosted、Cisco IP Contact Center Enterprise、およびCisco IP Contact Center Hostedエディションのすべてのバージョンに存在します。このプロセスの再起動には数分かかる場合があり、その間は新しいコールを処理できません。既存のコールは引き続き動作します。システムが冗長な方法で展開されている場合、冗長システムが引き継ぎ、サービスの損失を防止します。ただし、冗長システム上のJTapi Gatewayも、同じ脆弱性を不正利用して再起動できます。

この脆弱性を不正利用するには、攻撃者はJTapiサーバポートへの3ウェイTCPハンドシェイクを完了する必要があります。このポート番号は、製品の導入方法と、サーバの冗長ペアが存在するかどうかによって異なります。これは、次の場所にあるWindowsレジストリでjtapiServerPortNumber値を検索することで、Windowsレジストリで見つけることができます。

- HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\[instanceName]\PG[Number][A/B]\PG\CurrentVersion\JGWS\jgw[number]\JGWData\Config

回避策

この脆弱性に対しては回避策がありません。この脆弱性に関連する一般的な対応策は次のとおりです。Cisco Unified Contact CenterまたはCisco IP Contact Centerがデータネットワークから物理的または論理的に分離され、インターネットから分離されていることを確認します。これにより、インターネットまたは内部データネットワークから脆弱性が悪用される可能性が制限されます。

Cisco Unified Contact CenterまたはCisco IP Contact Center(IPCC)宛てのTCP/IPトラフィックが

信頼できる送信元からしか許可されないように、脆弱性のあるネットワークデバイスの前に設置されたルータ、スイッチ、およびファイアウォールにアクセスコントロールリスト(ACL)を適用します。CiscoルータにACLを適用する方法の例については、<http://www.cisco.com/warp/public/707/tacl.html>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わせください。

ソフトウェアリリース	パッチ	メンテナンス
5.0	ICM5.0(0)_SR13_ES18	Â
6.0	ICM6.0(0)_SR8_ES3 6.0(0)_SR9_ES1	6.0SR10 (2007年4月に提供開始)
7.0	ICM7.0(0)_SR4_ES43	Â
7.1	ICM7.1(3)_ES5	7.1(4) (2007年3月より利用可能)

Â

メンテナンスリリースは、<https://sec.cloudapps.cisco.com/support/downloads/go/MDFTree.x?butype=cc>からダウンロードできます。

ICM5.0(0)_SR13_ES18は、<http://www.cisco.com/cgi-bin/tablebuild.pl/d4b330d7b9c07d33f2833e1be69c6145>からダウンロードできます。

6.0.00_SR08_ES3は、<http://www.cisco.com/cgi-bin/tablebuild.pl/48b796a9ba353f2d02897ae3e6bb1140>からダウンロードできます。

6.0.00_SR09_ES1は、<http://www.cisco.com/cgi-bin/tablebuild.pl/2008d93eba6ab0cd6be05634f90962f3>からダウンロードできます。

7.0.00_SR04_ES43は、<http://www.cisco.com/cgi-bin/tablebuild.pl/47564eac9ea7b12357226a5f20bbbd66>からダウンロードできます。

7.1.03_ES5は、<http://www.cisco.com/cgi-bin/tablebuild.pl/9df0152592e9779b3f9e8701a94e4422>からダウンロードできます。

不正利用事例と公式発表

Cisco PSIRT では、本アドバイザリに記載されている脆弱性の不正利用事例やその公表は確認しておりません。

この脆弱性は、お客様からシスコに報告されたものです。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070110-jtapi>

改訂履歴

リ ビ ジ ョ ン 1.1	2007 年1月 29日	「ソフトウェアバージョンと修正」セクションで、ソフトウェアリリース6.0に関する情報を更新。
リ ビ ジ ョ ン 1.0	2007 年1月 10日	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。

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。