

# [VulnWatch] Cisco Security Advisory: Cisco Unified Contact Center and IP Contact Center JTapi Gateway Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2007-01/msg00016.html>

---

- *From:* Cisco Systems Product Security Incident Response Team <[psirt@xxxxxxxx](mailto:psirt@xxxxxxxx)>
  - *Date:* Wed, 10 Jan 2007 17:00:00 +0100
- 

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Cisco Security Advisory: Cisco Unified Contact Center and IP Contact Center JTapi Gateway Vulnerability

Advisory ID: cisco-sa-20070110-jtapi

<http://www.cisco.com/warp/public/707/cisco-sa-20070110-jtapi.shtml>

Revision 1.0

For Public Release 2007 January 10 1600 UTC (GMT)

-----

## Contents

Summary  
Affected Products  
Details  
Impact  
Software Version and Fixes  
Workarounds  
Obtaining Fixed Software  
Exploitation and Public Announcements  
Status of this Notice:FINAL  
Distribution  
Revision History  
Cisco Security Procedures

-----

## Summary

=====

Cisco Unified Contact Center Enterprise, Cisco Unified Contact Center Hosted, Cisco IP Contact Center Enterprise, and Cisco IP Contact Center Hosted editions are affected by a vulnerability that may result in the restart of JTapi Gateway process. Until this process restarts, no new connections can be processed. Existing connections will continue to work.

Cisco Unified Contact Center Express and Cisco IP Contact Center Express are not affected by this vulnerability.

Cisco has made free software available to address this vulnerability for affected customers.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070110-jtapi.shtml>.

#### Affected Products

=====

#### Vulnerable Products

+-----

All versions of Cisco Unified Contact Center Enterprise, Cisco Unified Contact Center Hosted, Cisco IP Contact Center Enterprise, and Cisco IP Contact Center Hosted editions are affected.

#### Products Confirmed Not Vulnerable

+-----

- \* Cisco Unified Contact Center Express and Cisco IP Contact Center Express editions are not affected.
- \* Cisco Unified Intelligent Contact Management Enterprise and Hosted are not affected.

No other Cisco products are known to be affected by this vulnerability.

#### Details

=====

Cisco Unified Contact Center Enterprise (formerly Cisco IP Contact Center [IPCC] Enterprise), an integral component of the Cisco Unified Communications system, provides intelligent routing and call treatment with blending of multiple communication channels.

Cisco Unified Contact Center Hosted (formerly known as Cisco IP Contact Center [IPCC] Hosted) is a platform that enables customers to move to a Customer Interaction Network. The Customer Interaction Network is a distributed, IP-based customer service infrastructure comprising a suite of multichannel services and customer relationship management applications.

A vulnerability exists in all versions of Cisco Unified Contact Center Enterprise, Cisco Unified Contact Center Hosted, Cisco IP Contact Center Enterprise, and Cisco IP Contact Center Hosted editions that may result in the restart of JTapi Gateway process. The restart of this process can take up to several minutes and during this time no new calls can be processed. Existing calls continue to work. If the system is deployed in a redundant way, the redundant system will take over preventing a loss of service. However the JTapi Gateway on the redundant system can also be restarted by exploiting the same vulnerability.

To exploit this vulnerability, an attacker will need to complete a 3-way TCP handshake to the JTapi server port. This port number can be dependent on how the product is deployed and whether there is a redundant pair of servers. It can be found in the Windows registry by looking up the jtapiServerPortNumber value in the Windows Registry, located at:

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

#### Vulnerability Scoring Details

+-----

Cisco is providing scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS). Cisco will provide a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks. Cisco PSIRT will set the bias in all cases to normal. Customers are encouraged to apply the bias parameter when determining the environmental impact of a particular vulnerability.

CVSS is a standards based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided a FAQ to answer additional questions regarding CVSS at <http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>.

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at <https://intellishield.cisco.com/security/alertmanager/cvss>.

#### Cisco Bug IDs:

CSCsh15483 (registered customers only) – Third party connects to JGW's TCP port, JGW asserts and fails over.

CVSS Base Score: 3.3

- Access Vector: Remote
- Access Complexity: Low
- Authentication: Not Required
- Confidentiality Impact: None
- Integrity Impact: None
- Availability Impact: Complete
- Impact Bias: Normal

CVSS Temporal Score: 2.7

- Exploitability: Functional
- Remediation Level: Official Fix
- Report Confidence: Confirmed

Impact

=====

Successful exploitation of the vulnerability may result in the restart of JTapi Gateway process. Restarting this process can take several minutes and during this time no new calls can be processed. Existing calls continue to work without any problems.

Software Version and Fixes

=====

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center ("TAC") or your contracted maintenance provider for assistance.

Software	Patch	Maintenance	Release
5.0	ICM5.0(0)		
		_SR13_ES18	
6.0	ICM6.0(0)	6.0SR10	
		_SR8_ES3	(Available April 2007)
7.0	ICM7.0(0)		
		_SR4_ES43	
7.1	ICM7.1(3)		
			7.1(4)

| 7.1 | \_ES5 | (Available |  
| | | March 2007) |

+-----+

Maintenance releases can be downloaded at:

<http://tools.cisco.com/support/downloads/go/MDFTree.x?butype=cc>

ICM5.0(0)\_SR13\_ES18 can be downloaded at:

<http://www.cisco.com/cgi-bin/tablebuild.pl/d4b330d7b9c07d33f2833e1be69c6145>

6.0.00\_SR08\_ES3 can be downloaded at:

<http://www.cisco.com/cgi-bin/tablebuild.pl/48b796a9ba353f2d02897ae3e6bb1140>

7.0.00\_SR04\_ES43 can be downloaded at:

<http://www.cisco.com/cgi-bin/tablebuild.pl/47564eac9ea7b12357226a5f20bbbd66>

7.1.03\_ES5 can be downloaded at:

<http://www.cisco.com/cgi-bin/tablebuild.pl/9df0152592e9779b3f9e8701a94e4422>

#### Workarounds

=====

No workarounds exist for this vulnerability. The following general mitigation actions are relevant for this vulnerability: Ensuring the Cisco Unified Contact Center or Cisco IP Contact Center is physically or logically separated from the data network and isolated from the Internet which will limit the exposure to the exploitation of the vulnerability from the Internet or internal data networks.

Apply access control lists (ACLs) on routers, switches, and firewalls installed in front of the vulnerable network device such that TCP/IP traffic destined for the Cisco Unified Contact Center or Cisco IP Contact Center is allowed only from trusted sources. Refer to <http://www.cisco.com/warp/public/707/tacl.html> for examples on how to apply ACLs on Cisco routers.

#### Obtaining Fixed Software

=====

Cisco will make free software available to address this vulnerability for affected customers. This advisory will be updated as fixed software becomes available. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at <http://www.cisco.com/public/sw-license-agreement.html>, or as otherwise

set forth at Cisco.com Downloads at  
<http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact either "psirt@xxxxxxxx" or "security-alert@xxxxxxxx" for software upgrades.

#### Customers with Service Contracts

+-----

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

#### Customers using Third Party Support Organizations

+-----

Customers whose Cisco products are provided or maintained through prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

#### Customers without Service Contracts

+-----

Customers who purchase direct from Cisco but who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as follows:

- \* +1 800 553 2447 (toll free from within North America)
- \* +1 408 526 7209 (toll call from anywhere in the world)
- \* e-mail: [tac@xxxxxxxx](mailto:tac@xxxxxxxx)

Have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized

telephone numbers and instructions and e-mail addresses for use in various languages.

Exploitation and Public Announcements

=====

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability described in this advisory.

This vulnerability was reported to Cisco by a customer.

Status of this Notice:FINAL

=====

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

Distribution

=====

This advisory is posted on Cisco's worldwide website at : <http://www.cisco.com/warp/public/707/cisco-sa-20070110-jtapi.shtml>

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- \* cust-security-announce@xxxxxxxxxx
- \* first-teams@xxxxxxxxxx
- \* bugtraq@xxxxxxxxxxxxxxxxxxxx
- \* vulnwatch@xxxxxxxxxxxxxxxx
- \* cisco@xxxxxxxxxxxxxxxxxxxx
- \* cisco-nsp@xxxxxxxxxxxxxxxxxxxx
- \* full-disclosure@xxxxxxxxxxxxxxxxxxxx
- \* comp.dcom.sys.cisco@xxxxxxxxxxxxxxxxxxxx

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

Revision History

=====

```

+-----+
| Revision | | Initial |
| 1.0 | 2007-Jan-10 | public |
| | | release |
+-----+

```

Cisco Security Procedures

=====

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html).

This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at

<http://www.cisco.com/go/psirt>.

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.6 (GNU/Linux)

```

iD8DBQFFpQoy8NUAbBmDaxQRAkL2AJ9t0g2ref0Qz0zC+41kP+4LmUHy9ACcCeGy
uCpauyAde4NmqzpRfvUesm8=
=xGr+

```

-----END PGP SIGNATURE-----