

# Cisco Security Advisory: Multiple Vulnerabilities in Cisco Unified MeetingPlace

Advisory ID: cisco-sa-20100127-mp

<http://www.cisco.com/warp/public/707/cisco-sa-20100127-mp.shtml>

## Revision 1.1

Last Updated 2010 Feb 10 1500 UTC (GMT)

For Public Release 2010 Jan 27 1600 UTC (GMT)

---

Please provide your [feedback](#) on this document.

---

## Contents

[Summary](#)  
[Affected Products](#)  
[Details](#)  
[Vulnerability Scoring Details](#)  
[Impact](#)  
[Software Versions and Fixes](#)  
[Workarounds](#)  
[Obtaining Fixed Software](#)  
[Exploitation and Public Announcements](#)  
[Status of this Notice: FINAL](#)  
[Distribution](#)  
[Revision History](#)  
[Cisco Security Procedures](#)

---

## Summary

Multiple vulnerabilities exist in Cisco Unified MeetingPlace. This security advisory outlines the details of these vulnerabilities:

- Insufficient validation of SQL commands

- Unauthorized account creation
- User and password enumeration in Cisco MeetingTime
- Privilege escalation in Cisco MeetingTime

Workarounds are not available for these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20100127-mp.shtml>.

[\[Expand all sections\]](#) [\[Collapse all sections\]](#)

## ☐ **Affected Products**

### ☐ **Vulnerable Products**

Cisco Unified MeetingPlace versions 5, 6, and 7 are each affected by at least one of the vulnerabilities described in this document.

The Cisco Unified MeetingPlace conferencing solution provides functionality that allows organizations to host integrated voice, video, and web conferencing. The solution is deployed on-network and integrated directly into an organization's private voice/data networks and enterprise applications. Cisco Unified MeetingPlace servers can be deployed so that the server is accessible from the Internet, allowing external parties to participate in meetings.

Cisco MeetingTime is a desktop application included with Cisco Unified MeetingPlace version 6.x that could be used to access and configure the Cisco Unified MeetingPlace Audio Server systems. MeetingTime classifies users as either end users, contacts, attendants, or system administrators.

The end-of-software maintenance for MeetingPlace version 5.3 occurred in April 2009. End-of-sale and end-of-life details are available at:

[http://www.cisco.com/en/US/prod/collateral/voicesw/ps6789/ps5664/ps5669/prod\\_end-of-life\\_notice0900aecd806e743c.html](http://www.cisco.com/en/US/prod/collateral/voicesw/ps6789/ps5664/ps5669/prod_end-of-life_notice0900aecd806e743c.html)

### ☐ **Products Confirmed Not Vulnerable**

No other Cisco products are currently known to be affected by these vulnerabilities.

[Top of the section](#) [Close Section](#)

## ☐ **Details**

This Security Advisory describes multiple distinct vulnerabilities in the MeetingPlace and MeetingTime products. These vulnerabilities are independent of each other.

### **Insufficient Validation of SQL Commands**

An unauthenticated user may be able to send SQL commands to manipulate the database that

MeetingPlace uses to store information about server configuration, meetings, and users. These commands could be used to create, delete, or alter any of the information contained in the Cisco Unified MeetingPlace database.

This vulnerability is documented in Cisco Bug ID [CSCtc39691](#) ([registered](#) customers only) and has been assigned CVE ID CVE-2010-0139.

## Unauthorized Account Creation

An unauthenticated user may be able to send a crafted URL to the internal interface of the Cisco Unified MeetingPlace web server to create a MeetingPlace user or administrator account.

This vulnerability is documented in Cisco Bug IDs [CSCtc59231](#) ([registered](#) customers only) and [CSCtd40661](#) ([registered](#) customers only) and has been assigned CVE ID CVE-2010-0140.

## User and Password Enumeration in Cisco MeetingTime

The MeetingTime authentication sequence consists of a series of packets that are transmitted between the client and the Cisco Meeting Place Audio Server over TCP port 5001. An attacker may be able to alter the authentication sequence to access sensitive information in the user database including usernames and passwords.

This vulnerability is documented in Cisco Bug ID [CSCsv76935](#) ([registered](#) customers only) and has been assigned CVE ID CVE-2010-0141.

## Privilege Escalation in Cisco MeetingTime

An attacker may be able to alter the packets in the MeetingTime authentication sequence to elevate the privileges of a normal user to an administrative user.

This vulnerability is documented in Cisco Bug ID [CSCsv66530](#) ([registered](#) customers only) and has been assigned CVE ID CVE-2010-0142.

[Top of the section](#)   [Close Section](#)

## ☐ Vulnerability Scoring Details

Cisco has provided scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

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

Cisco has provided a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco has provided an 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:

<http://intellishield.cisco.com/security/alertmanager/cvss>

<b>Insufficient validation of SQL commands</b>					
<b>Calculate the environmental score of <a href="#">CSCtc39691</a></b>					
CVSS Base Score - <b>9</b>					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Partial	Partial	Complete
CVSS Temporal Score - <b>7.8</b>					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

<b>Unauthorized account creation</b>					
<b>Calculate the environmental score of <a href="#">CSCtc59231/CSCtd40661</a></b>					
CVSS Base Score - <b>10</b>					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	Complete	Complete
CVSS Temporal Score - <b>8.7</b>					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

<b>User and password enumeration in Cisco MeetingTime</b>					
<b>Calculate the environmental score of <a href="#">CSCsv76935</a></b>					
CVSS Base Score - <b>6.4</b>					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Partial	Partial	None
CVSS Temporal Score - <b>5.3</b>					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

Privilege escalation in Cisco MeetingTime					
Calculate the environmental score of <a href="#">CSCsv66530</a>					
CVSS Base Score - <b>8.5</b>					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	Single	Complete	Complete	Complete
CVSS Temporal Score - <b>7.4</b>					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

[Top of the section](#)   [Close Section](#)

## Impact

Successful exploitation of these vulnerabilities may result in a variety of conditions including: information disclosure, denial of service, privilege escalation, account creation, or alteration of configuration data.

[Top of the section](#)   [Close Section](#)

## Software Versions and Fixes

The following table identifies the version of software in which each vulnerability was first fixed.

In order to obtain fixed software, administrators must install a hotfix over the latest maintenance release of MeetingPlace Web Conferencing solution.

The latest versions of Cisco MeetingPlace software can be downloaded from <http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278785523>.

Information about how to obtain the hotfixes for software versions 6.0mr5 and 7.0mr1 can be found in the release notes enclosures of one of the following bugs: [CSCtc39691](#) ( [registered](#) customers only ) , [CSCtc59231](#) ( [registered](#) customers only ) , [CSCtd40661](#) ( [registered](#) customers only ) , [CSCsv76935](#) ( [registered](#) customers only ) , or [CSCsv66530](#) ( [registered](#) customers only ) .

Vulnerability	MeetingPlace 6	MeetingPlace 7
Insufficient validation of SQL commands	6.0.639.2	7.0(2.3) hotfix 5F
Unauthorized account creation	6.0.639.3	7.0(2.3) hotfix 5F
User and password		

enumeration in Cisco MeetingTime	MR5	Not applicable
Privilege escalation in MeetingTime	MR5	Not applicable

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.

[Top of the section](#)   [Close Section](#)

## ☐ Workarounds

There are no workarounds for the vulnerabilities described in this advisory.

[Top of the section](#)   [Close Section](#)

## ☐ Obtaining Fixed Software

Cisco has released free software updates that address these vulnerabilities. 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/en/US/docs/general/warranty/English/EU1KEN\\_.html](http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html), or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact [psirt@cisco.com](mailto:psirt@cisco.com) or [security-alert@cisco.com](mailto:security-alert@cisco.com) 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 agreements 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 do not hold a Cisco service contract, and customers who purchase through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should acquire 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@cisco.com](mailto:tac@cisco.com)

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

Refer to [http://www.cisco.com/en/US/support/tsd\\_cisco\\_worldwide\\_contacts.html](http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html) for additional TAC contact information, including localized telephone numbers, and instructions and e-mail addresses for use in various languages.

[Top of the section](#)   [Close Section](#)

## ☐ Exploitation and Public Announcements

Cisco would like to thank the National Australia Bank's Security Assurance team and Credit Suisse for the discovery and reporting of these vulnerabilities.

The Cisco PSIRT is not aware of any malicious use of the vulnerabilities described in this advisory.

[Top of the section](#)   [Close Section](#)

## ☐ 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-20100127-mp.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@cisco.com](mailto:cust-security-announce@cisco.com)
- [first-bulletins@lists.first.org](mailto:first-bulletins@lists.first.org)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [full-disclosure@lists.grok.org.uk](mailto:full-disclosure@lists.grok.org.uk)
- [comp.dcom.sys.cisco@newsgate.cisco.com](mailto:comp.dcom.sys.cisco@newsgate.cisco.com)

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 1.1	2010-Feb-10	Added information on how to obtain hotfixes
Revision 1.0	2010-Jan-27	Initial 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>.

**Help us help you.**

**Please rate this document.**

- Excellent
- Good
- Average
- Fair
- Poor

**This document solved my problem.**

- Yes
- No
- Just browsing

**Suggestions for improvement:**

(256 character limit)

Send

<a href="#">Home</a>	<a href="#">How to Buy</a>	<a href="#">Login</a>	<a href="#">Profile</a>	<a href="#">Feedback</a>	<a href="#">Site Map</a>	<a href="#">Help</a>
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 - 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)