

# Cisco Security Advisory: Cisco Unified Communications Web-based Management Vulnerability

Advisory ID: cisco-sa-20071017-IPCC

<http://www.cisco.com/warp/public/707/cisco-sa-20071017-IPCC.shtml>

## Revision 1.1

Last Updated 2008 April 25 1430 UTC (GMT)

For Public Release 2007 October 17 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](#)
- [Customers with Service Contracts](#)
- [Customers using Third Party Support Organizations](#)
- [Customers without Service Contracts](#)
- [Exploitation and Public Announcements](#)
- [Status of this Notice: FINAL](#)
- [Distribution](#)
- [Revision History](#)
- [Cisco Security Procedures](#)

---

## Summary

Unified Contact Center and Intelligent Contact Management products contain a vulnerability that may result in unauthorized access to the web-based reporting and script monitoring tool (Web View) and the web-based configuration tool (Web Admin).

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20071017-IPCC.shtml>.

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

## ☐ **Affected Products**

### ☐ **Vulnerable Products**

The following products are affected by a vulnerability that may result in unauthorized access to the web-based reporting and script monitoring tool (Web View):

- Cisco Unified Intelligent Contact Management Enterprise (Unified ICME)
- Cisco Unified ICM Hosted (Unified ICMH)
- Cisco Unified Contact Center Enterprise (UCCE)
- Cisco Unified Contact Center Hosted (UCCH)
- Cisco System Unified Contact Center Enterprise (SUCCE)

The following product is affected by a vulnerability that may result in unauthorized access to the web-based configuration tool (Web Admin).

- Cisco System Unified Contact Center Enterprise (SUCCE)

To determine the version of software installed on the Administration Workstation (AW), navigate to the Add or Remove Programs window on the Windows Server. If impacted, an entry for Cisco ICM Maintenance Release ICM 7.1(5) will be observable in the list of installed applications.

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

The following products are not affected by the vulnerability described in this document:

- Cisco Unified Contact Center Express
- Cisco IP Contact Center Express

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

Only the identified products running software version ICM 7.1(5) are impacted by this vulnerability.

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

## ☐ **Details**

Cisco Unified ICME, Unified ICMH, UCCE, UCCH and SUCCE are a suite of strategic platforms

that enable customers to provide intelligent routing and call treatment with blending of multiple communication channels.

A vulnerability exists in software version 7.1(5) for Cisco Unified ICME, Unified ICMH, UCCE, UCCH and SUCCE editions that may enable any Windows Active Directory domain defined user to obtain unauthorized privilege levels. This would provide Windows Active Directory users the ability to view Web View report information for any call center instance. Cisco SUCCE is also impacted by unauthorized access to the Web Admin tool, which could result in the ability to change the application configuration, including editing application rights.

This vulnerability is documented in Cisco Bug ID: [CSCsj55686](#) ( [registered](#) customers only) .

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

## ☐ Vulnerability Scoring Details

Cisco is providing 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.

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.

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

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?target=new&version=2.0&vector=AV:N/AC:L/Au:S/C:C/I:C/A:C/E:F/RL:OF/RC:C>

<b><a href="#">CSCsj55686</a> ( <a href="#">registered</a> customers only) - AD users have privileges to log into Web View and Web Admin tools</b>					
<b>Calculate the environmental score of <a href="#">CSCsj55686</a></b>					
<b>CVSS Base Score - 9</b>					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	Single	Complete	Complete	Complete
<b>CVSS Temporal Score - 7.4</b>					
Exploitability		Remediation Level		Report Confidence	

Functional

Official-Fix

Confirmed

[Top of the section](#)

[Close Section](#)

## Impact

Successful exploitation of the vulnerability described in this document may provide any user defined in the Windows Active Directory domain with unauthorized access to view Web View information for any ICM or Contact Center instance. In addition, the vulnerability provides unauthorized access to the Web Admin tool for any user defined in the Windows Active Directory domain. It should be noted that Web Admin is only used with Cisco SUCCE. Access to Web Admin may result in the ability to change the application configuration, including editing application rights.

[Top of the section](#)

[Close Section](#)

## Software Versions 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 Release	Patch	Maintenance
7.1(5)	ICM7.1(5) _ES46	7.2(3) (Available December 2007)

Contact Center and ICM maintenance software can be downloaded from the following URL:

<http://tools.cisco.com/support/downloads/go/MDFTree.x?butype=cc> ( [registered](#) customers only)

[Top of the section](#)

[Close Section](#)

## Workarounds

Any Windows users defined in Active Directory that are not part of the ICM/IPCC Active Directory hierarchy will have full access to the Web View and Web Admin tools. There is no workaround. Users defined in the Windows Active Directory domain where the IPCC servers reside and then associated to the instance of the ICM/IPCC Active Directory hierarchy will have correct permissions. Filters such as Transit ACLs can then be used to allow access to the Administration Workstation from only the trusted hosts.

Filters that deny HTTP packets using TCP port 80 and HTTPS packets using TCP port 443 should be deployed throughout the network as part of a tACL policy for protection of traffic that enters the

network at ingress access points. This policy should be configured to protect the network device where the filter is applied and other devices behind it. Filters for HTTP packets using TCP port 80 and HTTPS packets using TCP port 443 should also be deployed in front of vulnerable network devices so that traffic is only allowed from trusted clients.

Additional information about tACLs is available in "Transit Access Control Lists: Filtering at Your Edge:

[http://www.cisco.com/en/US/tech/tk648/tk361/technologies\\_white\\_paper09186a00801afc76.shtml](http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801afc76.shtml).

Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document for this advisory:

<http://www.cisco.com/warp/public/707/cisco-amb-20071017-IPCC.shtml>.

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

## ☐ **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 "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

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

## ☐ **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>.

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

## ☐ **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.

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

## ☐ **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 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@cisco.com](mailto:tac@cisco.com)

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.

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

## ☐ **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 discovered during the resolution of customer support cases.

[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.

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

## ☐ Distribution

This advisory is posted on Cisco's worldwide website at:

<http://www.cisco.com/warp/public/707/cisco-sa-20071017-IPCC.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-teams@first.org](mailto:first-teams@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.

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

## ☐ Revision History

Revision 1.1	2008- April-25	Updated link to CVSS score for <a href="#">CSCsj55686</a> .
Revision 1.0	2007-Oct- 17	Initial Public Release

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

## ☐ 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>.

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

---

**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)

[Home](#)

[How to Buy](#)

[Login](#)

[Profile](#)

[Feedback](#)

[Site Map](#)

[Help](#)

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

© 2007 - 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)