

Cisco Security Advisory: CiscoWorks Common Services Arbitrary Code Execution Vulnerability

Advisory ID: cisco-sa-20080528-cw

<http://www.cisco.com/warp/public/707/cisco-sa-20080528-cw.shtml>

Revision 1.0

For Public Release 2008 May 28 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

CiscoWorks Common Services contains a vulnerability that could allow a remote attacker to execute arbitrary code.

Cisco has released free software updates that address this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080528-cw.shtml>.

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

☐ Affected Products

☐ Vulnerable Products

CiscoWorks Common Services versions 3.0.3, 3.0.4, 3.0.5, 3.0.6, 3.1, and 3.1.1 are vulnerable. The following Cisco products that use CiscoWorks Common Services as their base are also affected by this vulnerability.

Product	Product Version	Common Services Version
Cisco Unified Operations Manager (CUOM)	1.1	3.0.3
Cisco Unified Operations Manager (CUOM)	2.0	3.0.3
Cisco Unified Operations Manager (CUOM)	2.0.1	3.0.5
Cisco Unified Operations Manager (CUOM)	2.0.2	3.0.5

Cisco Unified Operations Manager (CUOM)	2.0.3	3.0.5
Cisco Unified Service Monitor (CUSM)	1.1	3.0.3
Cisco Unified Service Monitor (CUSM)	2.0	3.0.4
Cisco Unified Service Monitor (CUSM)	2.0.1	3.0.5
CiscoWorks QoS Policy Manager (QPM)	4.0, 4.0.1, and 4.0.2	3.0.5
CiscoWorks LAN Management Solution (LMS)	2.5, 2.5.1, 2.6	3.0.3
CiscoWorks LAN Management Solution (LMS)	2.6 Update	3.0.5
CiscoWorks LAN Management Solution (LMS)	3.0	3.1
CiscoWorks LAN Management Solution (LMS)	3.0 December 2007 Update	3.1.1
Cisco Security Manager (CSM)	3.0	3.0.3
Cisco Security Manager (CSM)	3.0.1	3.0.4
Cisco Security Manager (CSM)	3.0.2	3.0.5
Cisco Security Manager (CSM)	3.1 and 3.1.1	3.0.5

Cisco Security Manager (CSM)	3.2	3.1
Cisco TelePresence Readiness Assessment Manager (CTRAM)	1.0	3.0.5

Note: CiscoWorks Voice Manager (CVM) and Cisco Unified Intelligent Contact Management (ICM) could be vulnerable if their underlying Common Services versions were upgraded.

☐ Products Confirmed Not Vulnerable

Products that use CiscoWorks Common Services version 3.2 and later or Common Management Framework (CMF) version 2.2 are not vulnerable.

The following CiscoWorks products are also not affected by this vulnerability:

Product	Product Version	Common Services Version
CiscoWorks IP Communications Manager	1.0	3.0 SP1
CiscoWorks IP Communications Service Monitor	1.0	3.0 SP1

Note: CiscoWorks Voice Manager (CVM) and Cisco Unified Intelligent Contact Management (ICM) could be vulnerable if their underlying Common Services versions were upgraded.

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

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

☐ Details

CiscoWorks Common Services represents a common set of management services that are shared by

CiscoWorks applications. CiscoWorks is a family of products based on Internet standards for managing networks and devices. Many CiscoWorks products use and depend on Common Services.

CiscoWorks Common Services contains a vulnerability that could allow a remote attacker to execute arbitrary code. This vulnerability is documented in Cisco Bug ID [CSCsm77245](#) ([registered](#) customers only) , and has been assigned the Common Vulnerabilities and Exposures (CVE) ID CVE-2008-2054.

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

☐ Vulnerability Scoring Details

Cisco has provided scores for the vulnerability 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>.

CSCsm77245 - CiscoWorks URL Misbehavior

Calculate the environmental score of [CSCsm77245](#)

CVSS Base Score - **9.3**

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
---------------	-------------------	----------------	------------------------	------------------	---------------------

Network	Medium	None	Complete	Complete	Complete
CVSS Temporal Score - 7.7					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

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

▣ Impact

Successful exploitation of this vulnerability could allow a remote attacker to execute arbitrary code on the user client machine.

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

▣ Software Versions and Fixes

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.

This vulnerability has been corrected in CiscoWorks Common Services version 3.2 and in the following software patches:

cwcs3.x-sol-CSCsm77245-0.tar.gz - for Solaris versions

cwcs3.x-win-CSCsm77245-0.zip - for Windows versions

The CiscoWorks Common Services patches can be downloaded from:

<http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-cd-one>

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.

☐ Workarounds

Filters such as Transit ACLs (tACLs) can be used to allow access to the Administration Workstation from only trusted hosts.

Filters that deny HTTP packets using HTTPS packets using TCP port 443 and TCP port 1741 should be deployed throughout the network as part of a tACL policy to protect the network from 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 that are behind it. Filters for HTTPS packets that use TCP port 443 and TCP port 1741 should also be deployed in front of vulnerable network devices so only traffic from trusted clients is allowed.

Note: 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.

For additional information on XSS attacks and the methods used to exploit these vulnerabilities, please refer to the Cisco Applied Intelligence Response "Understanding Cross-Site Scripting (XSS) Threat Vectors", available at:

<http://www.cisco.com/warp/public/707/cisco-amb-20060922-understanding-xss.shtml>

☐ Obtaining Fixed Software

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> , 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.

☐ 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

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/warp/public/687/Directory/DirTAC.shtml> 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**

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

This vulnerability was reported to Cisco by Dave Lewis from Liquidmatrix.org

Cisco PSIRT greatly appreciates the opportunity to work with researchers on security vulnerabilities, and we welcome the opportunity to review and assist in product reports.

[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-20080528-cw.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
- first-teams@first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net

- full-disclosure@lists.grok.org.uk
- 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 1.0	2008-May-28	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. 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](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)