

Cisco Security Advisory: Multiple Vulnerabilities in Cisco Digital Media Manager

Advisory ID: cisco-sa-20100303-dmm

<http://www.cisco.com/warp/public/707/cisco-sa-20100303-dmm.shtml>

Revision 1.0

For Public Release 2010 March 03 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 the Cisco Digital Media Manager (DMM). This security advisory outlines details of the following vulnerabilities:

- Default credentials
- Privilege escalation vulnerability
- Information leakage vulnerability

These vulnerabilities are independent of each other.

There are no workarounds that can mitigate any of these vulnerabilities.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20100303-dmm.shtml>.

Note: This advisory is being released simultaneously with a vulnerability disclosure advisory that impacts the Cisco Digital Media Player. This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20100303-dmp.shtml>.

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

☐ **Affected Products**

☐ **Vulnerable Products**

The following is a list of the products affected by each vulnerability as described in detail within this advisory.

Default Credentials

Cisco DMM versions 5.0.x and 5.1.x are affected by this vulnerability. Cisco DMM versions 4.x are not vulnerable.

Privilege Escalation Vulnerability

Cisco DMM versions 5.0.x and 5.1.x are affected by this vulnerability. Cisco DMM versions 4.x are not vulnerable.

Information Leakage Vulnerability

All Cisco DMM releases earlier than 5.2 are affected by this vulnerability.

☐ **Products Confirmed Not Vulnerable**

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

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

☐ **Details**

The Cisco DMM is used to manage, schedule, and publish digital media for Cisco Digital Signs, Cisco Cast and Cisco Show and Share. This security advisory describes multiple distinct vulnerabilities in the Cisco DMM. These vulnerabilities are independent of each other.

Default Credentials

Cisco DMM versions earlier than 5.2 have default credentials that could allow an attacker full control

of the installed web applications, including settings, status, and deployment.

This vulnerability is documented in Cisco Bug ID [CSCta03378](#) ([registered customers only](#)) and has been assigned Common Vulnerabilities and Exposures (CVE) identifier CVE-2010-0570.

Privilege Escalation Vulnerability

A vulnerability exists in Cisco DMM versions 5.0.x and 5.1.x that could allow authenticated, but unauthorized users to change the configuration and obtain full access of the device.

This vulnerability is documented in Cisco Bug ID [CSCtc46008](#) ([registered customers only](#)) and has been assigned Common Vulnerabilities and Exposures (CVE) identifier CVE-2010-0571.

Information Leakage Vulnerability

The Cisco DMM can be used to manage the Cisco Digital Media Player. The Cisco Digital Media Player is an IP-based endpoint that can play high-definition live and on-demand video, motion graphics, web pages, and dynamic content on digital displays.

A vulnerability exists in all Cisco DMM versions earlier than 5.2 that could allow authenticated but unauthorized users to view Cisco Digital Media Player user credentials and LDAP credentials (if configured) in error log messages and stack traces.

This vulnerability is documented in Cisco Bug ID [CSCtc46050](#) ([registered customers only](#)) and has been assigned Common Vulnerabilities and Exposures (CVE) identifier CVE-2010-0572.

[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>.

CSCta03378 - Default password for Tomcat administration account

Calculate the environmental score of [CSCta03378](#)

CVSS Base Score - 10					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	Complete	Complete
CVSS Temporal Score - 8.7					
Exploitability		Remediation Level		Report Confidence	
High		Official-Fix		Confirmed	

CSCtc46008 - Privilege Escalation on DMM

Calculate the environmental score of [CSCtc46008](#)

CVSS Base Score - 8.5					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	Single	Complete	Complete	Complete
CVSS Temporal Score - 7					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCtc46050 - Potential Information Leakage within Stack Trace

Calculate the environmental score of [CSCtc46050](#)

CVSS Base Score - 7.1					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	High	Single	Complete	Complete	Complete
CVSS Temporal Score - 5.9					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

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

☐ Impact

Successful exploitation of the default credentials vulnerability could allow an attacker to change the settings, status, and deployment of the installed web applications.

Successful exploitation of the privilege escalation vulnerability could allow authenticated, but unauthorized users to change the configuration and obtain full access of the device.

Successful exploitation of the information leakage vulnerability could allow authenticated but unauthorized users to view Cisco Digital Media Player user credentials and LDAP credentials (if configured) in error log messages and stack traces.

[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.

All of the vulnerabilities described in this security advisory have been fixed in Cisco DMM version 5.2.

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

☐ **Workarounds**

There are no workarounds that can mitigate any of these vulnerabilities.

[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 , 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/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**

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

The privilege escalation and information leakage vulnerabilities were reported to Cisco by the National Australia Bank's Security Assurance team. Cisco PSIRT appreciates the opportunity to work with researchers on security vulnerabilities and welcomes the opportunity to review and assist in product reports.

The default credentials vulnerability was found during internal testing.

[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-20100303-dmm.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-bulletins@lists.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	2010-March-03	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](#)

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