

Cisco Security Advisory: Cisco Unified Communications Disaster Recovery Framework Command Execution Vulnerability

Advisory ID: cisco-sa-20080403-drf

<http://www.cisco.com/warp/public/707/cisco-sa-20080403-drf.shtml>

Revision 1.1

Last Updated 2008 April 25 2000 UTC (GMT)

For Public Release 2008 April 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

Several products in the Cisco Unified Communications family of products contain a command execution vulnerability in the Disaster Recovery Framework (DRF) feature. A remote, unauthenticated user could

exploit this vulnerability to execute arbitrary commands that may allow full administrative access to affected systems. There is a workaround for this vulnerability.

Cisco has released free software updates that address this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080403-drf.shtml>.

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

☐ **Affected Products**

☐ **Vulnerable Products**

The following Cisco products are known to be vulnerable:

- Cisco Unified Communications Manager (CUCM) 5.x and 6.x
- Cisco Unified Communications Manager Business Edition
- Cisco Unified Precense 1.x and 6.x
- Cisco Emergency Responder 2.x
- Cisco Mobility Manager 2.x

☐ **Products Confirmed Not Vulnerable**

Cisco Unified Communications Manager versions 3.x and 4.x are not vulnerable. No other Cisco products are currently known to be affected by these vulnerabilities.

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

☐ **Details**

The Disaster Recovery Framework (DRF) is a feature shared among several products in the Cisco Unified Communications family of products. DRF allows administrators to backup and restore a system configuration to a local tape drive or remote server.

The DRF Master server is responsible for performing backup and restoration requests. This vulnerability documents an issue where the DRF Master server does not perform authentication on requests that it receives over the network. A remote, unauthenticated user can connect to the DRF Master server and may be able to perform any DRF-related tasks. These tasks include:

- Modifying or deleting a scheduled backup
- Copying a system backup to a remote, user-specified server
- Restoring a user-specified configuration from a remote server
- Execute arbitrary operating system commands

An attacker could exploit this vulnerability to cause a denial of service condition, obtain sensitive configuration information, overwrite configuration parameters, or execute arbitrary commands with full administrative privileges.

This vulnerability is documented in [CVE-2008-1154](#) and the following Cisco Bug IDs:

- [CSCso53771](#) ([registered](#) customers only) —Cisco Unified Communications Manager 5.x and 6.x

[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>.

CSCso53771 - Unauthenticated Access to Disaster Recovery Framework (registered customers only)					
Calculate the environmental score of CSCso53771					
CVSS Base Score - 10					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	Complete	Complete
CVSS Temporal Score - 8.3					
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, unauthenticated attacker to cause a denial of service condition, obtain sensitive configuration information, overwrite configuration

parameters or execute arbitrary commands with full administrative privileges.

[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.

Fixed software is available for the following Cisco products. This advisory will be updated as additional fixes are available.

A patch has been provided that can be applied to CUCM 5.x and 6.x, CUCMBE, Cisco Unified Presence 1.x and 6.x, Cisco Emergency Responder 2.x, and Cisco Mobility Manager 2.x. The filename is *ciscocm.CSCso53771.security.patch.cop* and can be downloaded at the following link:

<http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-utilpage?psrtdcat20e2>

Please consult the COP file Readme for installation instructions.

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

☐ Workarounds

Administrators can mitigate this vulnerability by disabling the DRF Master service. However, administrators should exercise caution when disabling the DRF Master service, as system backups will not occur while the service is stopped. Administrators are encouraged to perform a complete system backup before employing this workaround and use care when making configuration changes until the DRF Master service can be safely re-enabled.

Instructions for disabling the DRF Master service on Cisco Unified Communications Manager systems are available at the following link:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/service/5_0_1/ccmsrva/sasrvact.html#wp10

The vulnerability may be mitigated by restricting access to the DRF Master service (TCP port 4040). For a Cisco Unified Communications Manager cluster, access to the port should be restricted to valid cluster nodes.

Additional mitigation techniques 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-20080403-drf.shtml>

☐ **Obtaining Fixed Software**

Cisco has released free software updates that address this vulnerability. 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/products/prod_warranties_item09186a008088e31f.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 is not aware of any malicious use of the vulnerability described in this advisory.

This vulnerability was reported to Cisco by VoIPshield Systems.

[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-20080403-drf.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 1.1	2008-april-25	Updated CVSS link for CSCso53771 .
Revision 1.0	2008-April-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)



Send

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.](#)