

# Table of Contents

<b><u>Cisco Security Advisory: CiscoWorks Application Vulnerabilities</u></b> .....	1
<u>Document ID: 44502</u> .....	1
<b><u>Revision Numeral 1.1: FINAL</u></b> .....	1
<u>Last Updated 2003 August 29 1700 (GMT)</u> .....	1
<u>For Public Release 2003 August 13 UTC 1500</u> .....	1
<u>Please provide your feedback on this document</u> .....	1
<b><u>Summary</u></b> .....	1
<b><u>Affected Products</u></b> .....	1
<b><u>Details</u></b> .....	2
<b><u>Impact</u></b> .....	2
<b><u>Software Versions and Fixes</u></b> .....	2
<b><u>Obtaining Fixed Software</u></b> .....	2
<b><u>Workarounds</u></b> .....	3
<b><u>Exploitation and Public Announcements</u></b> .....	3
<b><u>Status of This Notice: FINAL</u></b> .....	3
<b><u>Distribution</u></b> .....	3
<b><u>Revision History</u></b> .....	4
<b><u>Cisco Security Procedures</u></b> .....	4

# Cisco Security Advisory: CiscoWorks Application Vulnerabilities

Document ID: 44502

**Revision Numeral 1.1: FINAL**

**Last Updated 2003 August 29 1700 (GMT)**

**For Public Release 2003 August 13 UTC 1500**

---

**Please provide your feedback on this document.**

---

**Summary**  
**Affected Products**  
**Details**  
**Impact**  
**Software Versions and Fixes**  
**Obtaining Fixed Software**  
**Workarounds**  
**Exploitation and Public Announcements**  
**Status of This Notice: FINAL**  
**Distribution**  
**Revision History**  
**Cisco Security Procedures**

---

## Summary

CiscoWorks Common Management Foundation (CMF), also packaged as part of CiscoWorks CD One, provides an application infrastructure foundation, allowing all CiscoWorks applications to share a common model for data storage, login, user role definitions, access privileges, and security protocols, as well as for navigation and launch management.

Two vulnerabilities exist in CiscoWorks CMF versions prior to and including 2.1. The first vulnerability is a privilege escalation vulnerability where a guest user may obtain administrative privileges within the application via a specially crafted URL. The second vulnerability is an ability to run arbitrary commands on the CiscoWorks server due to an error in processing user input.

This notice will be posted at <http://www.cisco.com/warp/public/707/cisco-sa-20030813-cmf.shtml>.

Cisco is making patches available for CMF versions 2.0 and 2.1, free of charge, to correct the problem.

## Affected Products

The following products are affected:

- All versions of CiscoWorks CD One (1st through 5th editions)
- Resource Manager Essentials (RME) versions 2.0, 2.1, and 2.2

- Cisco Resource Manager (CRM) versions 1.0 and 1.1

CiscoWorks CD One is included as the base for all CiscoWorks management solutions, such as the LAN Management Solution, Routed WAN Management Solution, Small Network Management Solution, and VPN/Security Management Solution.

To determine the version of the Common Management Foundation which is installed, navigate through the menus within CiscoWorks starting with the tab on the left titled "Server Configuration" and locate the screen titled "Applications and Versions" under the folder named "About the Server". Look for the entry in the table labeled "Common Management Foundation" and the corresponding version.

## Details

The first vulnerability allows a non-privileged user of the CiscoWorks application, including the guest account if enabled, to send a specially crafted URL to the CiscoWorks server to acquire administrative privileges without authentication. Cisco Bug ID CSCdy33916 describes this vulnerability.

The second vulnerability permits an authenticated user of the CiscoWorks application to run arbitrary commands on the CiscoWorks server as "casuser", the username under which the application runs. Cisco Bug ID CSCea15281 describes this vulnerability.

## Impact

- CSCdy33916 The guest user or a normal user is capable, with a specifically crafted URL, of obtaining administrative privileges within the application allowing the user to perform tasks which it might otherwise not be allowed to do. Examples of such tasks might be approval of scheduled changes, such as software upgrades, adding and removing devices, adding, removing, and modifying accounts with the server, and viewing device configurations stored in the local archive.
- CSCea15281 A normal user is capable, with a specifically crafted URL, of running commands remotely on the CiscoWorks server to perform tasks which they may otherwise not have access to do. Examples of such tasks might be viewing device configurations stored in the local archive.

## Software Versions and Fixes

Both vulnerabilities have been resolved in CiscoWorks Common Services 2.2.

Patches for CMF versions 2.0 and 2.1 are available from the Software Center on Cisco's worldwide website.

## Obtaining Fixed Software

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Product Upgrade Tool at <http://tools.cisco.com/gct/Upgrade/jsp/index.jsp> (registered customers only).

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 assistance with the upgrade, which should be free of charge.

Customers who purchase/license the product directly from Cisco, but who 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 obtain an applicable software patch 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)

Please have your product serial number available and give the URL of this notice as evidence of your entitlement to a free patch. Free patches for non-contract customers must be requested through the TAC.

Please do not contact either "[psirt@cisco.com](mailto:psirt@cisco.com)" or "[security-alert@cisco.com](mailto:security-alert@cisco.com)" for software upgrades.

If you need assistance with the implementation of the workarounds, or have questions on the workarounds, please contact the Cisco Technical Assistance Center (TAC).

See <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.

## Workarounds

- CSCdy33916 The guest user account may be disabled, limiting the exposure to only the trusted users of the CiscoWorks server. However, a software upgrade or patch is required to completely resolve the vulnerability.
- CSCea15281 There is no workaround. A software upgrade or patch is required.

## Exploitation and Public Announcements

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

The vulnerabilities described in this advisory were both originally found by internal testing. Prior to disclosure, the bug described by CSCdy33916 was also reported by Omicron from Portcullis Computer Security Ltd. Their report can be found at <http://www.portcullis-security.com/advisory/cisco-sa-20030813.txt>

## Status of This Notice: FINAL

This is an FINAL advisory. Although Cisco cannot guarantee the accuracy of all statements in this notice, all of the facts have been checked to the best of our ability. Cisco does not anticipate issuing updated versions of this advisory unless there is some material change in the facts. Should there be a significant change in the facts, Cisco will update this advisory.

A stand-alone copy or paraphrase of the text of this security advisory 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 will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20030813-cmf.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)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [full-disclosure@lists.netsys.com](mailto:full-disclosure@lists.netsys.com)
- [first-teams@first.org](mailto:first-teams@first.org) (includes CERT/CC)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [comp.dcom.sys.cisco](mailto:comp.dcom.sys.cisco)
- Various internal Cisco mailing lists

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 1.0	<del>2003 August 13</del>	<del>Initial Public Release</del>
Revision 1.1	<del>2003 August 29</del>	Added link for patch download; changed status to FINAL.

## 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/warp/public/707/sec\\_incident\\_response.shtml](http://www.cisco.com/warp/public/707/sec_incident_response.shtml). This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

---

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

---

Updated: Sep 24, 2004

Document ID: 44502

---