

# [NEWS] CiscoWorks 2000 Privilege Escalation Vulnerabilities (CiscoWorks Application Vulnerabilities)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-08/0040.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 08/14/03

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 14 Aug 2003 12:40:00 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Get Thawte's New Step-by-Step SSL Guide for MSIS

In this guide you will find out how to test, purchase, install and use a Thawte Digital Certificate on your MSIS web server. Throughout, best practices for set-up are highlighted to help you ensure efficient ongoing management of your encryption keys and digital certificates. Get your copy of this new guide now: <http://ad.doubleclick.net/clk;5903126;8265119;j>

-----  
CiscoWorks 2000 Privilege Escalation Vulnerabilities (CiscoWorks Application Vulnerabilities)

---

## 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.

## Securiteam: [NEWS] CiscoWorks 2000 Privilege Escalation Vulnerabilities (CiscoWorks Application Vulnerabilities)

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

### DETAILS

#### 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.

## Securiteam: [NEWS] CiscoWorks 2000 Privilege Escalation Vulnerabilities (CiscoWorks Application Vulnerabilities)

Patches for CMF versions 2.0 and 2.1 should be available by the end of August 2003 (date subject to change). Should the availability date change, Cisco will update this advisory to reflect the new availability date.

### 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> (<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.

Securiteam: [NEWS] CiscoWorks 2000 Privilege Escalation Vulnerabilities (CiscoWorks Application Vulnerabilities)

\* CSCea15281 – There is no workaround. A software upgrade or patch is required.

Technical details:

Whilst requesting certain pages the raw HTTP shows a statement of who the logged on user is:

```
HTTP/1.1 200 OK
Date: Tue, 01 Jul 2003 13:01:12 GMT
Server: Apache/1.3.24 (Unix) mod_perl/1.26
Content-Length: 5
Connection: close
Content-Type: text/html
```

guest

By replacing guest with admin and using a HTTP POST request to send the information, (for the modify/delete users page) the system responds with information on all the users on the site, i.e.:

```
user1:::7 user2:::2 portcullis:portcullis@anywhere.com:::3F admin:::F
guest::admin::0
```

This allows Guest to then view information restricted to the Admin account on all users on the system.

ADDITIONAL INFORMATION

The original advisory can be downloaded from:

<http://www.portcullis-security.com/News/archives/advisory/cisco-sa-20030813.htm>  
<http://www.portcullis-security.com/News/archives/advisory/cisco-sa-20030813.htm>

The information has been provided by

<mailto:Omicron@portcullis-security.com> Omicron.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====  
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.