

# Cisco Security Advisory: CRM Temporary File Vulnerability

Document ID: 13653

Advisory ID: cisco-sa-19980813-crmtmp

<http://www.cisco.com/warp/public/707/cisco-sa-19980813-crmtmp.shtml>

## Revision 1.1

For Public Release 1998 August 13 1600 UTC (GMT)

---

Please provide your feedback on this document.

---

- Summary
- Affected Products
- 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

Versions 1.0 and 1.1 of the Cisco Resource Manager (CRM) create log files and temporary files on the management station which contain potentially sensitive information. These files are not protected using operating system mechanisms, and are therefore readable by all users of the system on which CRM is installed. The information exposed includes the usernames, passwords, and SNMP community strings used by CRM to gain access to the devices being managed.

Users who have access to the computer on which CRM is installed may gain access to information which gives them unauthorized access to the managed routers and switches. This affects both Solaris and Windows NT systems.

There are workarounds for this problem, and a patch is available for CRM 1.1. There is no patch for CRM 1.0. Other than to install the patch, the most effective solution for most installations is simply to deny untrusted users any access to the computer on which CRM is installed or to its file systems.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-19980813-crmtmp.shtml>.

# Affected Products

This section provides details on affected products.

## Vulnerable Products

All customers who run Cisco Resource Manager 1.1 or 1.0, and who allow untrusted users access to the computer on which CRM is run or to its file systems, are affected by these vulnerabilities.

## Products Confirmed Not Vulnerable

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

## Details

Several different unprotected files may contain sensitive information. Applicable Cisco bug IDs include:

- CSCdk13298
- CSCdk13579
- CSCdk14992
- CSCdk14993

These issues are described in this section.

## Remote Access Logs (CSCdk13298)

Cisco Resource Manager is capable of logging a great deal of detailed information for debugging purposes. Debugging is ordinarily under control of the administrator. However, a software error in CRM 1.0 and 1.1 causes debugging to be enabled at all times. The debugging information collected may include usernames and passwords used to log into managed devices, SNMP community strings, and enable passwords. The files containing this information are readable by any user of the computer on which CRM is run.

The log files containing the offending data are:

- /var/adm/CSCOPx/files/schedule/job-id/swim\_swd.log (Solaris) C:\Program Files\CSCOPx\files\schedule\job-id\swim\_swd.log (Windows NT).  
These files are created by software distribution jobs scheduled with "Distribute Images". Each job has its own subdirectory (designated by "job-id" above) and its own log file.
- /tmp/swim\_debug.log (Solaris) C:\Program Files\CSCOPx\temp\swim\_debug.log (Windows NT).  
This file is used for logging debugging information from Software Image Manager functions, such as "Import image from File System/Device", Job administration and History administration.

This file is used for logging debugging information from Software Image Manager functions, such as "Import image from File System/Device", Job administration and History administration.

## Database Update Logs (CSCdk13579)

The "Local/Remote Import", "Import from File", "Add Devices", and "Change Device Attributes" functions all record debugging information in files readable to any user of the computer on which CRM is run. This information may include usernames, login passwords, SNMP community strings, and/or enable passwords.

The offending information is recorded in a log file named "dbi\_debug.log", which is located in /tmp on Solaris systems and in C:\Program Files\CSCOpX\temp on Windows NT systems.

## **Import Temporary Files (CSCdk14992, CSCdk14993)**

The "Local/Remote Import" functions, which are used to load data into the CRM database from databases maintained by other network management tools, create temporary files containing usernames, login passwords, community strings, and enable passwords. The files are readable to any user of the computer on which CRM is run. The files exist only for a short time during the information gathering phase of an import operation, and are automatically deleted upon successful completion of the operation. However, should the information gathering phase of the operation fail because of some system error, the files would not be deleted.

The offending files have names beginning with "DPR\_", and are stored in "/tmp" on Solaris systems and in "C:\Program Files\CSCOpX\temp" on Windows NT systems.

## **Impact**

Users who have direct access to the machine on which CRM is installed, or who have network access to the files specified in the "Details" section of this document, may gain unauthorized access to the managed devices. The unauthorized access gained may include administrative access and the ability to modify device configurations.

## **Software Versions and Fixes**

Cisco has modified the CRM software to eliminate all of the vulnerabilities described in this notice. The first regular release containing the modifications will be CRM version 2.0, which is tentatively scheduled for release in early October, 1998. This schedule is subject to change.

Customers who do not wish to wait for CRM version 2.0 may install the CRM SWIM package version 1.1.1. The CRM SWIM package version 1.1.1 is a patched version, identical to the SWIM package in CRM version 1.1, but containing a fix for bug ID CSCdk13298, which Cisco believes to be the vulnerability most disruptive to day-to-day system operation. The other vulnerabilities listed in this notice are not addressed by the CRM SWIM package 1.1.1.

Customers with service contracts may obtain updates through their usual channels; those who are registered users of CCO (Cisco's Worldwide Web site) may download the CRM SWIM package version 1.1.1 update from CCO. Go to <http://www.cisco.com/cgi-bin/tablebuild.pl/crm-packages>. You must be a registered Cisco customer and logged into CCO to obtain this update via the web.

Customers without service contracts should contact the Cisco TAC for assistance. The CRM SWIM package 1.1.1 patch (but not the CRM 2.0 upgrade) will be made available free of charge to all CRM customers, regardless of service contract status. Please reference the URL of this notice as evidence of your entitlement to the patch.

There will be no patched version of CRM 1.0. CRM 1.0 customers are eligible for free upgrades to CRM 1.1 and the CRM SWIM package version 1.1.1. Customers who wish to continue to use CRM 1.0 are strongly encouraged to prevent all access by untrusted users to the computers on which they run CRM or to those computers' file systems.

# Workarounds

This section describes workarounds for these issues:

- CSCdk13298
- CSCdk13579
- CSCdk14992
- CSCdk14993

## Workarounds for CSCdk13298

The simplest and most effective workaround for this vulnerability is to prevent untrusted users from having access to the computer on which CRM is being run or to the file systems on which the log files are stored. The file systems in question should not be shared over a network of any kind.

If the computer on which CRM is being run must be shared, then the files in question must be protected from access by untrusted users. This may be done by issuing the following Solaris commands while running as "root" or "bin":

```
chmod 700 /var/adm/CSCOpX/files/schedule
chmod 700 /tmp/swim_debug.log
```

**Note:** *Each time your system is rebooted, you will need to change the permissions on /tmp/swim\_debug.log.*

**Note:** There is no analogous workaround for Windows NT systems.

## Workaround for CSCdk13579

The simplest and most effective workaround for this vulnerability is to prevent untrusted users from having access to the computer on which CRM is being run or to the file systems on which the log files are stored. The file systems in question should not be shared over a network of any kind.

If the computer on which CRM is run must be shared, the file "/tmp/dbi\_debug.log" or "C:\Program Files\CSCOpX\temp\dbi\_debug.log" should be deleted after any change to device attributes. Note that a window of vulnerability will exist between the time at which the database update is performed and the time at which the file is deleted. It may be desirable to deny access to untrusted users during this window, even though they may be given access to the system at other times.

## Workaround for CSCdk14992/CSCdk14993

The only effective workaround for CSCdk14992 and CSCdk14993 is to deny untrusted users access to the system on which CRM is run during any import operation. Cisco believes that such operations are sufficiently uncommon to make this a viable option.

## Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. 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/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact either "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 agreement 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 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 get their 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](mailto:tac@cisco.com)

Have your product serial number available and give the URL of this notice as evidence of your 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 special localized telephone numbers and instructions and e-mail addresses for use in various languages.

## Exploitation and Public Announcements

Cisco has had no reports of malicious exploitation of the vulnerabilities listed in this notice.

Cisco knows of no public announcements of these vulnerabilities before the date of this notice.

## 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.

## Distribution

This advisory will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-19980813-crmtmp.shtml>.

In addition to Worldwide Web posting, the initial version of this notice is being sent to the following e-mail recipients:

- [cust-security-announce@cisco.com](mailto:cust-security-announce@cisco.com)
- 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 1.1	<del>1998 August 13</del>	<del>Initial public release.</del>
--------------	---------------------------	------------------------------------

## Cisco Security Procedures

Please report security issues with Cisco products, and/or sensitive security intrusion emergencies involving Cisco products, to [security-alert@cisco.com](mailto:security-alert@cisco.com). Reports may be encrypted using PGP; public RSA and DSS keys for "security-alert@cisco.com" are on the public PGP key servers.

The alias "security-alert@cisco.com" is used only for reports incoming to Cisco. Mail sent to the list goes only to a very small group of users within Cisco. Neither outside users nor unauthorized Cisco employees may subscribe to "security-alert@cisco.com".

Please do not use "security-alert@cisco.com" for configuration questions, for security intrusions that you do not consider to be sensitive emergencies, or for general, non-security-related support requests. We do not have the capacity to handle such requests through this channel, and will refer them to the TAC, delaying response to your questions. We advise contacting the TAC directly with these requests. TAC contact information is as follows:

- Voice telephone: +1 800 553 2447 (toll-free from within North America)
- Voice telephone: +1 408 526 7209 (toll call from anywhere in the world)
- Electronic mail: [tac@cisco.com](mailto:tac@cisco.com)

All formal public security notices generated by Cisco are sent to the public mailing list "cust-security-announce@cisco.com". For information on subscribing to this mailing list, send a message containing the single line "info cust-security-announce" to "majordomo@cisco.com". An analogous list, "cust-security-discuss@cisco.com" is available for public discussion of the notices and of other Cisco security issues.

---

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

---

Updated: Aug 13, 1998

Document ID: 13653

---