

Cisco Security Advisory: LDAP Connection Leak in CTI when User Authentication Fails

Document ID: 22028

Advisory ID: cisco-sa-20020327-cm-ctifw-leak

<http://www.cisco.com/warp/public/707/cisco-sa-20020327-cm-ctifw-leak.shtml>

Revision 1.1

Last Updated 2002 March 28 1700 UTC (GMT)

For Public Release 2002 March 27 1700 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: INTERIM
- Distribution
- Revision History
- Cisco Security Procedures

Summary

The Cisco CallManager, running certain software releases, has a vulnerability wherein a memory leak in the CTI Framework authentication can cause the server to crash and result in a reload. This vulnerability can be exploited to initiate a denial of service (DoS) attack.

This vulnerability is documented as Cisco bug ID CSCdv28302. There are workarounds available to mitigate the vulnerability.

This advisory is available at
<http://www.cisco.com/warp/public/707/cisco-sa-20020327-cm-ctifw-leak.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

To determine if a product is vulnerable, review the list below. If the software versions or configuration information are provided, then only those combinations are vulnerable.

- Cisco CallManager 3.1

Products Confirmed Not Vulnerable

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

Details

A memory leak in the Cisco CallManager has been attributed to the failure of a user to properly authenticate when using Computer Telephony Integration (CTI). This behavior is most commonly seen on CallManager systems immediately following the integration with a customer directory such as Active Directory (AD) or Netscape. The most common cause in this scenario is that the WebAttendant user, CTI Framework (CTIFW), has not been configured with a valid password in the customer directory. Please note that this problem will occur even on systems that do not utilize the WebAttendant since the Telephony Call Dispatch (TCD) service is always enabled by default. The CCMAdmin->Global Directory and "Add a New User" configuration pages stop working if CTIFW user is not configured or the CTI user's password is incorrect. Various other components such as RIS Data Collector may also fail to function properly.

- **CSCdv28302**

This vulnerability is documented as Cisco Bug ID CSCdv28302.

Problem Symptoms

There are several indicators available in determining if this problem is at the root.

Tool

Message

Event Viewer

Error: kCtiProviderOpenFailure – CTI application failed to open provider CTIconnectionId: 485 Login User Id: CtiFw ReasonCode: 2362179680 IPAddress: 172.21.12.44 App ID: Cisco CTIManager Cluster ID: JMTAO-CM2-Cluster Node ID: JMTAO-CM2 CTI Application ID: Cisco Telephony Call Dispatcher Process ID: 0 Process Name: CtiHandler Provider Name: CTI Framework Explanation: Application is unable to open provider. Recommended Action: Check the reason code and correct the problem. Restart CTIManager if problem persists..

Task Manager

From the Task Manager select the **Processes** tab, click **View** and then **Select Columns...** Check **Handle Count** and click **OK**. Click on the **Handles** column to sort by handles used. You will observe that the CTIManager.exe is consuming a large number of handles (> 500).

DOS netstat

Cisco Security Advisory: LDAP Connection Leak in CTI when User Authentication Fails

Another diagnostic tool is to run "netstat -na" from a DOS command prompt on the CM server. A very large number of established connections to TCP port 389 if CallManager is integrated with AD or port 8404 when CallManager is integrated with DCD.

Impact

The vulnerabilities can be exploited to produce a Denial of Service (DoS) attack. When the vulnerabilities are exploited, they can cause an affected Cisco product to crash and reload.

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.

Version Affected	Fixed Regular Release (available now) Fix
Version 3.1	carries forward into all later versions Upgrade to 3.1(3a)

Workarounds

Configure the ctifw user by following the instructions at:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/3_0/install/ad_3011.htm#xtocid30717

Step	Action
1	Set the password for the user in the corporate directory using your standard user management tools.
2	On a Cisco CallManager server, choose Start > Run and enter command to open a command prompt. Click OK .
3	Enter the command, PasswordUtils ; for example, "passwordUtils my_passphrase"
4	The previous action generates an encrypted password. Copy the password into the Windows clipboard.
5	Choose Start > Run .
6	Enter regedit into the Open field and then click OK .
7	Browse to \\HKEY_LOCAL_MACHINE\Software\Cisco Systems, Inc.\Directory Configuration within the registry.
8	Delete the value CTIFWPW and paste the encrypted password from Step 3 into the field.
9	

	Restart the Cisco Telephony Call Dispatcher service by choosing Start > Programs > Administrative Tools > Services . Highlight the service in the list; right click on the service and then click Restart from the drop-down list.
10	Repeat Step 2 through Step 9 for each Cisco CallManager server in the cluster.

IMPORTANT: Please note that you must reboot the CM server in all cases to reset the established TCP connections and recover the lost memory.

Alternatively, if you are not using the Cisco WebAttendant and/or the Cisco Telephony Call Dispatcher Service, set it to "manual" or "disabled" from the "Services" control panel.

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

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

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

Status of This Notice: INTERIM

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. CISCO EXPECTS TO UPDATE THIS DOCUMENT AS NEW INFORMATION BECOMES AVAILABLE.

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-20020327-cm-ctifw-leak.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
- bugtraq@securityfocus.com
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- comp.dcom.sys.cisco
- firewalls@lists.gnac.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	2002–Mar–28	Corrected first fixed release
Revision 1.0	2002–Mar–27	Initial Public Release

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>.

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

Updated: Mar 28, 2002

Document ID: 22028
