Cisco Security Advisory

LDAP Connection Leak in CTI when User Authentication Fails

Severity

Advisory ID: cisco-sa-20020327-cm-ctifw-leak
Published: 2002 March 27 17:00 GMT
Version1.1: Final
Workarounds: See below

CVE-2002-0505
CWE-399

Download CVRF
Download PDF
Email

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Related Resources

IS Cisco CallManager LDAP Connection Memory Leak Vulnerability

Subscribe to Cisco Security Notifications

Subscribe

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20020327-cm-ctifw-leak .

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.

LDAP Leak Detection

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	**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.**

Workarounds

Configure the ctifw user by following the instructions at: /en/US/docs/voice_ip_comm/cucm/install/3_0/ad_3011.html#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.
	Restart the Cisco Telephony Call Dispatcher service by choosing **Start Programs Administrative Tools Services**. Highlight the

9	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.

Fixed Software

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 carries forward into all later versions**
Version 3.1	Upgrade to 3.1(3a)

Exploitation and Public Announcements

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

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20020327-cm-ctifw-leak

---

Revision History

Revision 1.1	2002-Mar-28	Corrected first fixed release
Revision 1.0	2002-Mar-27	Initial Public Release

Legal Disclaimer