

[NEWS] LDAP Connection Leak in CTI when User Authentication Fails

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-03/0118.html>

From: support@securiteam.com

Date: 03/28/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 28 Mar 2002 12:59:19 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

LDAP Connection Leak in CTI when User Authentication Fails

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.

DETAILS

Vulnerable systems:

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

No other Cisco product is known to be affected by this vulnerability.

Details:

A memory leak in the Cisco CallManager has been attributed to the failure

Securiteam: [NEWS] LDAP Connection Leak in CTI when User Authentication Fails

of a user to properly authenticate when using Call 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.

Problem Symptoms:

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

Tool: Event Viewer

Message: "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.. "

Tool: Task Manager

Message: "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)."

Tool: DOS netstat

Message: "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."

Securiteam: [NEWS] LDAP Connection Leak in CTI when User Authentication Fails

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:

Version Affected: Version 3.1

Fixed Regular Release (available now): Upgrade to 3.1(2)

Obtaining Fixed Software:

Cisco is offering free software upgrades to address this vulnerability for all affected customers. Customers may only install and expect support for the feature sets they have purchased.

Customers with service contracts should contact their regular update channels to obtain any software release containing the feature sets they have purchased. For most customers with service contracts, this means that upgrades should be obtained through the Software Center on Cisco's Worldwide Web site at <http://www.cisco.com>.

Customers whose Cisco products are provided or maintained through a 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 obtaining the free software upgrade(s).

Customers who purchased 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 fixed software by contacting the Cisco Technical Assistance Center (TAC) using the contact information listed below. In these cases, customers are entitled to obtain an upgrade to a later version of the same release or as indicated by the applicable row in the Software Versions and Fixes table (noted above).

Cisco 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

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.

Please have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade.

Please do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

Securiteam: [NEWS] LDAP Connection Leak in CTI when User Authentication Fails

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

- 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.

ADDITIONAL INFORMATION

The information has been provided by <mailto:psirt@cisco.com> Cisco Systems Product Security Incident Response Team.

=====

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

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

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

Securiteam: [NEWS] LDAP Connection Leak in CTI when User Authentication Fails

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

- **Previous message:** support@securiteam.com: "[\[UNIX\] XChat /dns Command Execution Vulnerability](#)"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)