Cisco Bash Code Injection Vulnerability Patch

Release Notes Version 1
October 2nd, 2014

Introduction:

These release notes contain important information about installation procedures for the Bash Code Injection Vulnerability Patch for Cisco Unified Communications Manager. This patch can be applied to all CUCM releases of versions 8.5(1), 8.6(2), 9.1(2), 10.0(1), and 10.5(1). For detailed information about the vulnerability itself please refer to the Release-note Enclosure of the CDETS listed below.

Note: Before you install this Patch, Cisco recommends that you review the *Important Notes* section for information about issues that may affect your system.

Updates in This Release

This patch provides a fix for CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, and CVE-2014-7169

CSCur00930 CUCM evaluation for CVE-2014-6271, 2014-7169, 2014-6277 and 2014-6278

Related Documentation:

To view documentation that supports your version of Cisco Unified Communications Manager release, go to:
http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-documentation-roadmaps-list.html

Determining the Software Versions:

Communications Manager

You can determine the Version of your Cisco Unified Communications Manager software that is running on your server by using the following command from CLI.

admin:show version active

The output of the command should be similar to the following:

admin:show version active
Active Master Version: 10.5.1.xxxxx.

Important Notes:

When upgrading to a new release of Cisco Unified Communications Manager, make sure that the updates in this release are included in the version you are upgrading to. If an ES or SU is installed after this update that does not also contain the fixes referenced in "*Updates in This Release"* then this update will need to be reapplied after the ES or SU is installed.

Installation Instructions:

As with any installation or upgrade, it is recommended that you apply this Update during off peak hours.

When applying this Update be advised that a clusterwide reboot is ***not*** required.

This update must be installed on all machines in the cluster before the cluster.

This package will install on the following System Versions:

- 8.5.1.10000-26 or any higher version starting with 8.5.1.xxxxx

- 8.6.2.10000-30 or any higher version starting with 8.6.2.xxxxx
- 9.1.2.10000-28 or any higher version starting with 9.1.2.xxxxx
- 10.0.1.10000-24 or any higher version starting with 10.0.1.xxxxx
- 10.5.1.10000-7 or any higher version starting with 10.5.1.xxxxx

You can install a patch or upgrade version from a DVD (local source) or from a computer (remote source) that the server being upgraded can access.

Note: Be sure to back up your system data before starting the software upgrade process. For more information, see the Disaster Recovery System Administration Guide

From Local Source:

Step 1: Download *ciscocm.bashupgrade.cop.sgn*

Step 2: Copy the upgrade file above to a writeable CD or DVD.

Step 3: Insert the new CD or DVD into the disc drive on the local server that is to be upgraded.

Step 4: Open Cisco Unified Communications Operating System Administration directly by entering the following URL:

http://server-name/cmplatform

where server-name is the host name or IP address of the admin server.

Step 5: Enter your OS Administrator username and password.

Step 6: Choose Software Upgrades > Install/Upgrade.

Step 7: For the software location source, choose DVD/CD.

Step 8: If you burned the patch file to a subdirectory on the CD or DVD, enter the path in the Directory field.

Step 9: To continue the upgrade process, click Next.

Step 10: Choose "*ciscocm.bashupgrade.cop.sgn*" and click Next.

Step 11: In the next window, monitor the progress of the download, which includes the filename and the number of megabytes that are getting transferred.

When the download completes, the Checksum window displays.

Step 12: Verify the checksum value:

e319f4b4f1100ad091f5116cb5f37bb3

Step 13: After determining that the checksums match, click Next to proceed with the software upgrade.

A Warning window displays the selected option.

Step 14: Click Install.

The Install Status window displays the Install log.

Step 15: When the installation completes, click Finish

Step 16: Verify the COP file version using this command from the CLI:

admin:show version active

Active Master Version: 10.5.1.xxxxx
Active Version Installed Software Options:
ciscocm.bashupgrade.cop <-- Note: Other cop files such as this may or may not already be present on your system

From Remote Source:

Step 1: Download *ciscocm.bashupgrade.cop.sgn*

Step 2: Copy the upgrade to an ftp or sftp server.

Step 3: Open Cisco Unified Communications Operating System Administration directly by entering the following URL:

http://server-name/cmplatform

where server-name is the host name or IP address of the admin server.

Step 4: Enter your OS Administrator username and password.

Step 5: Choose Software Upgrades > Install/Upgrade.

Step 6: For the software location source, choose Remote File System.

Step 7: Enter the directory name for the software upgrade, if required.

If the upgrade file is located on a Linux or Unix server, you must enter a forward slash at the beginning of the directory path. For example, if the upgrade file is in the patches directory, you must enter /patches.

If the upgrade file is located on a Windows server, check with your system administrator for the correct directory path.

Step 8: Enter the required upgrade information as described in the following table:

Remote Server: Host name or IP address of the remote server from which software will be downloaded.

Remote User: Name of a user who is configured on the remote server.

Remote Password: Password that is configured for this user on the remote server.

Download Protocol: Choose sftp or ftp.

Step 9: To continue the upgrade process, click Next.

Step 10: Choose "*ciscocm.bashupgrade.cop.sgn*" and click Next.

Step 11: In the next window, monitor the progress of the download, which includes the filename and the number of megabytes that are getting transferred.

When the download completes, the Checksum window displays.

Step 12: Verify the checksum value:

e319f4b4f1100ad091f5116cb5f37bb3

Step 13: After determining that the checksums match, click Next to proceed with the software upgrade.

A Warning window displays the selected option.

Step 14: Click Install.

The Install Status window displays and displays the install log.

Step 15: When the installation completes, click Finish

Step 16: Verify the COP file version using this command from the CLI:

admin:show version active

Active Master Version: 10.5.1.xxxxx
Active Version Installed Software Options:
ciscocm.bashupgrade.cop <-- Note: Other cop files such as this may or may not already be present on your system