Cisco Unified Communications Manager
Jan 2016 OpenSSL Update COP File

Release Notes Version 1
Mar 21, 2016

Introduction:

These release notes contain important information about the installation procedures for the OpenSSL Update COP file for Cisco Unified Communications Manager 10.5(2). This COP file, **ciscocm.ciscossl_10.5.2-v5_4_3.k3.cop.sgn**, is only designed for and has only been tested with CUCM 10.5(2).

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

Please note that the COP file name listed above is "ciscossl", not "openssl". This is because Cisco maintains a branch of OpenSSL that is known as CiscoSSL which is both FIPS Compliant and FIPS Certified. The version numbering is specific to Cisco, and is not mapped directly to specific OpenSSL versions. As CiscoSSL is OpenSSL based code, we continually integrate fixes from upstream versions of OpenSSL to ensure that the same vulnerabilities do not remain in the Cisco maintained library.

What this COP file provides:

This COP file upgrades rpms required to address the following vulnerabilities:

CVE-2016-0701, CVE-2015-3197

The CVE's listed above are already included in Engineering Specials (ES) or Service Update (SU) releases via the following Bug ID:

CSCuy07473: Evaluation of ciscocm for OpenSSL January 2016

Resolution

You must follow steps below to install the security update.

Related Documentation:

To view documentation that supports your version 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:

Cisco Unified Communications Manager

You can determine the System Version of the Cisco Unified Communications Manager software that is running on your server by accessing Cisco Unified Operating System Administration Web page.

The following information displays:

- System version: xxxxx
- VMware Installation: xxxxx

Important Notes:

The fixes provided in this COP file may not be available in older 10.5(2) ES's or SU's. If your ES or SU has a part of the fix, the cop file will take care of patching the remaining fix. If an ES or SU is installed after this update that does not

contain all of the fixes listed above, the COP file will need to be reapplied. Consult the **Known Fixed Releases:** field in the Bug Search tool to determine which ES's and SU's include these fixes.

Applying the COP multiple times will not cause any issues; if installed more than once, the installation will exit without making any changes to the system.

Installation Instructions:

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

Apply this COP to all nodes in the cluster.

Applying this update will not require a reboot.

This package will install on the following System Versions:
- 10.5.2.10000-xx -xx or any higher version starting with 10.5.2.xxxxx

***Caution*: *The updates applied with this COP cannot be uninstalled*.** 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 Remote Source:

Step 1: Download ***ciscocm.ciscossl_10.5.2-v5_4_3.k3.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.ciscossl_10.5.2-v5_4_3.k3.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:

MD5: 1f8b07ed8fc26119cc62e72dcddfdda3
SHA1: de1bef0d5a114804f259d21e4d587602b90db65f

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: 10.5.2.xxxxx-xx <-- *Note:10.5.2 is shown for example only; your version may vary*

Active Version Installed Software Options:
ciscocm.ciscossl_10.5.2-v5_4_3.k3.cop