Cisco Voice Operating System (VOS)
COP File for CSCvg22923

Release Notes Version 2
November 15, 2017

Introduction:

These release notes contain important information about the installation procedures for the COP file that addresses **CSCvg22923 - CUCM unauthorized access vulnerability** and the associated CDETS. This COP file, **ciscocm.CSCvg22923-v1.2.cop.sgn** or **ciscocm.CSCvg22923-v1.2.k3.cop.sgn** will install on:

Cisco Unified Communications Manager release (CallManager) release 8.6 or higher.
Cisco Unified Communication Manager Session Management Edition (SME) release 8.6 or higher.
Cisco Unity Connection release 8.6 or higher.
Cisco Unified Communications Manager IM and Presence Service (IM&P) release 9.0 or higher.
Cisco Emergency Responder (CER) release 8.6 or higher.
Cisco Prime License Manager (PLM) release 10.0 or higher.
Cisco Unified Presence (CUP) release 8.6

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

What this COP file provides:

This COP file makes the required changes to address the following issue:

CSCvg22923 - CUCM unauthorized access vulnerability

For detailed information about CSCvg22923 and the correlating CDETS, please see the official Cisco Security Advisory at:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-vos

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:

An administrator can use the user interface to determine which Cisco VOS-based product software release is running:

- Log in to the web-based interface
- Click the **Help** menu
- Click **About** to view the system software release

Important Notes:

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.

A server reboot is not required with this update.

Use ***ciscocm.CSCvg22923-v1.2.cop.sgn*** for any 8x or 9x systems.

Use **ciscocm.CSCvg22923-v1.2.k3.cop.sgn** for any 10x to 12.0 systems.

***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 the COP file.

Step 2: Copy the COP file 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 cop file, if required.

If the cop 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 cop file is in the patches directory, you must enter /patches.

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

Step 8: Enter the required cop file 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 cop file installation process, click Next.

Step 10: Choose **ciscocm.CSCvg22923-v1.2.cop.sgn** or **ciscocm.CSCvg22923-v1.2.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:

ciscocm.CSCvg22923-v1.2.cop.sgn

MD5 Hash Value: 615c5c80624e3b590adbb01af540f3d4
SHA1 Hash Value: 5adea08c26046214533a40027debb3eccea34472

ciscocm.CSCvg22923-v1.2.k3.cop.sgn

MD5 Hash Value: 9ff0a6da0bbc8f9a1661b65eb883d288
SHA1 Hash Value: bae780750d5ab65c74e8d60bb2006087a5300ffc

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, a server reboot or service restart is not required.

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

admin: show version active
Active Master Version: <CUCM_Version>
Active Version Installed Software Options:
ciscocm.CSCvg22923-v1.2.cop.sgn