# Cisco Unified Communications Manager
# NTP denial-of-service vulnerability security updates COP File

Release Notes Version 2
February 10, 2015

## *Introduction:*

These release notes contain important information about installation procedures for the NTP denial-of-service vulnerability security update COP file for Cisco Unified Communications Manager.

*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 addresses the Network Time Protocol (NTP) security vulnerability defined by CVE-2013-5211 where an NTP amplification attack is used to perform a Distributed Denial of Service (DDoS) that relies on the use of publically accessible NTP servers to overwhelm a victim system with UDP traffic. This update will restrict the use of NTP mode 6 and 7 control messages into CUCM.

## *Updates in This Release*

Updates are cumulative, so installing this patch will provide all of the fixes in the New Updates section plus all of the fixes in the Previous Updates section if applicable.

### *New Updates*

CSCur26956 Unable to execute commands after installation of NTP cop file

** The new version of the cop file is ***ciscocm.ntp_option-v1.11.cop.sgn***

### *Previous Updates*

CSCum76937 CUCM Distributed denial-of-service vulnerability on NTP server

## *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:*

### *Unified Communications Manager*

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

The following information displays:

- System version: xxxxx
- VMware Installation: 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. If the COP file is installed more one time, the COP file installation fails with the information that the patch is already present in the release.

## *Installation Instructions:*

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

Applying this update will require a reboot.

This package will install on the following System Versions:
- 8.5.1 or any higher version starting with 8.5.1
- 8.6.2.10000-xx or any higher version starting with 8.6.2.xxxxx
- 9.1.2.10000-xx or any higher version starting with 9.1.2.xxxxx
- 10.0.1.10000-xx or any higher version starting with 10.0.1.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.

***Caution***: 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.ntp_option-v1.11.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.ntp_option.v1.11.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:

c30aafb78f987e2822f6bd37424867a7

*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: 9.1.2.xxxxx-xx <-- *Note: 9.1.2 is shown for example only; your version may vary*

Active Version Installed Software Options:
ciscocm.ntp_option. v1.11.cop.sgn

## *Additional Instructions:*

In order to disable mode 6 and 7 type control messages, this cop file configures the "noquery" option in the /etc/ntp.conf file. That option can be removed, displayed, or set using the following commands after the COP file is installed:

- set network ntp option noquery -- configures "noquery" option in /etc/ntp.conf file
- unset network ntp option noquery -- deletes "noquery" option in /etc/ntp.conf file
- show network ntp option -- displays option configured in /etc/ntp.conf