

# Unified Communications Manager / Emergency Responder / Unity Connection / UCM IM and Presence / Prime Collaboration Deployment

## COP File for CVE-2024-6387 for version 15

Release Notes  
July 31, 2024

### *Introduction:*

This readme contains important information about the installation procedures for the COP file **ciscocm.V15\_CVE-2024-6387\_v1.1.cop.sha512** for versions 15, 15SU1 and 15ES versions below 15.0.1.12900 for Unified Communications Manager (CUCM), Emergency Responder (CER), Unity Connection (CUC), Unified Communications Manager IM and Presence (IM&P), and Prime Collaboration Deployment (PCD).

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 provides a fix to address the following issues for the 15 release:

[CSCwk62318](#) - Evaluation of Cisco Unified Communications Manager for OpenSSH regreSSHion vulnerability

[CSCwk63694](#) - Evaluation of Cisco Emergency Responder for OpenSSH regreSSHion vulnerability

[CSCwk63494](#) - Evaluation of Cisco Unity Connection for OpenSSH regreSSHion vulnerability

[CSCwk63634](#) - Evaluation of Cisco Unified Communications Manager IM&P for OpenSSH regreSSHion vulnerability

[CSCwk64755](#) - Evaluation of Cisco Prime Collaboration Deployment for OpenSSH regreSSHion vulnerability

### *Related Documentation:*

To view the support documentation for Cisco Unified Communications Manager, go to:  
<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-managercallmanager/products-documentation-roadmaps-list.html>

### *Determining the Software Versions:*

#### **Cisco Unified Communications Manager**

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

The following information displays:

- System version: xxxxx

### ***Important Notes:***

A reboot is required as part of the COP file install.

This cop should **ONLY** be Installed through CLI.

If any issues are encountered, the ciscocm.V15\_CVE-2024-6387\_v1.1\_revert.cop.sha512 (md5sum: 7f3299fd57d0ec3ca6cff1d517ddd470) file can be used to revert the changes.

### ***Installation Instructions:***

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

After applying this COP file, you are required to reboot the server. The COP file will not restart the server automatically.

This cop should **ONLY** be Installed through CLI.

#### **From Remote Source:**

Step 1: Copy the COP file to an SFTP or FTP server.

Step 2: SSH to the admin CLI of the server

Step 3: Enter your OS Administrator username and password.

Step 4: Enter “utils system upgrade initiate”

Step 5: Choose your source, whether it be a Remote Filesystem via SFTP or FTP

Step 6: 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 7: Enter the required cop file information as described in the following table:

Server:	Host name or IP address of the remote server from which software will be downloaded.
User Name:	Name of a user who is configured on the remote server.
User Password:	Password that is configured for this user on the remote server.
Transfer Protocol:	Choose SFTP or FTP.
SMTP (optional):	Hostname of SMTP server for email alerts (if desired).

Continue with upgrade after download (yes/no) [  
Switch-version server after upgrade [valid only for ISO] (yes/no)

Step 8: Choose the *ciscocm.V15\_CVE-2024-6387\_v1.1.cop.sha512* COP file and press Enter.

Step 9: Monitor the console screen as it will start the installation and output the installation log to the CLI

Step 10: To verify the checksum value search for the below line within the installation log:

```
MD5(/common/download/ciscocm.V15_CVE-2024-6387_v1.1.cop.sha512)=  
65:89:21:62:1e:09:6b:46:61:21:37:77:85:ba:2a:9e
```

Step 11: Monitor the Installation Status and when the installation completes, the output will show  
“Successfully installed ciscocm.V15\_CVE-2024-6387\_v1.1.cop.sha512”

Step 12: 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.V15_CVE-2024-6387_v1.1.cop
```

Step 13: Reboot the server by entering the command “utils system restart”