ReadMe for Cisco Unified Communications Manager Release 14SU3

First Published: 2023-05-18

Last Modified: 2023-06-27

Revision History

Date	Revision
May 18, 2023	Initial publication
June 21, 2023	Added CSCwf65881 to Open Caveats
June 27, 2023	Added CSCwf67831 to Open Caveats

Introduction

Note To view the release notes for previous versions of Cisco Unified Communications Manager, choose the Cisco Unified Communications Manager version from the following URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_release_notes_list.html

Note Please review all sections in this document pertaining to installation before you install this version. Failure to install this version as described may result in inconsistent Cisco Unified Communications Manager behavior.

This 14SU3 ReadMe file contains important information about installation procedures and resolved caveats for Cisco Unified Communications Manager release 14SU3. This version can be applied to Cisco Unified Communications Manager and Session Management Edition.

Note Before you install Cisco Unified Communications Manager, Cisco recommends that you review the Important Notes, on page 3 for information about issues that may affect your system.

System Requirements

The following sections comprise the system requirements for this release.

Server Support

In this release, you cannot install or run Cisco Unified Communications Manager on server hardware; you must run these applications on virtual machines. Please refer to the "Hardware" section of the *Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service, Release 14* for additional details:

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html

Uninterruptible Power Supply

Ensure that you connect each node to an uninterruptible power supply (UPS) to provide backup power and protect your system.

⚠️

Caution Failure to connect the Cisco Unified Communication Manager nodes to a UPS may result in damage to physical media and require a new installation of Cisco Unified CM.

Version and Description

This SU is a cumulative update that incorporates all of the fixes and changes from Cisco Unified Communications Manager 14 through 14SU2 along with additional changes that are specific to this SU.

✎

Note You can only install this SU on Cisco Unified Communications Manager Release 10.5 through 11.x, 12.0(1x), 12.5(1), 14 through 14SU2, or any 14ES from 14.0.1.11001-1 to 14.0.1.13040-2. Upgrades from any earlier supported versions require a PCD migration. If you are upgrading from a version prior to 14, ensure you have the proper licensing prior to doing the upgrade.

For a list of all supported upgrade paths and the supported upgrade method, please see the Compatibility Matrix at:

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-device-support-tables-list.html

⚠️

Caution Please note that if you install an SU it may contain fixes that are not included in the newer Unified CM releases. For example, a fix in an 12.5(1)SU, 12.5(1)SU5, may not be included in 14 because the fix was not available prior to the release of 14. In this example, an SU or ES on the 14 branch may be required to retain the same fixes.

New to this Release

For details about the features included in this release, refer to Release Notes for Cisco Unified Communications Manager and IM & Presence Service, Release 14SU3 at:

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-release-notes-list.html

In addition to the features listed in the Release Notes, the following changes were introduced in 14SU3:

- **Log4j upgrade to 2.19**

In addition to the features listed in the Release Notes, the following changes were introduced in 14SU1:

- **This release is signed with a new 2021 signing key.** See the Important Notes, on page 3 section for more details.

Important Notes

Compatibility between collaboration products is detailed at the following link. You must insure your versions are compatible before beginning your upgrade:

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/unified/communications/system/Compatibility/CSR-Compatibility-Matrix-InteractiveHTML.html

Cisco provides the following guidance to help you successfully upgrade Cisco Unified Communications Manager software:

- To minimize call-processing interruptions during the upgrade process, register all devices to servers that are running the same version of Cisco Unified Communications Manager software. Make sure that you register all devices to the backup Cisco Unified Communications Manager server or to the primary Cisco Unified Communications Manager server, but not to both the backup and primary servers.

New 2021 Signing Key

Warning

This release is signed with a new 2021 signing key. It is possible that you may need to install the ciscocm.enable-sha512sum-2021-signing-key-v1.0.cop.sgn COP file first if upgrading from CUCM versions prior to 14. See the COP file readme for specifics.

This release also removes support for the previous signing key. If you are installing phone firmware, please be sure and use the files with k4.cop.sha512 in the name, as these files are also signed with the new signing key. Installing files signed with the previous signing key will result in a "The selected file is not valid." error during install.

Warning for Upgrades from 10.5(2)

Warning

Per the Supported Upgrade and Migration Paths in the Compatibility Matrix, direct upgrades from any 10.5.2 release to any 14 release are not supported (PCD Migration or Fresh Install with Data Import are the only supported upgrade options from 10.5.2). In previous releases of 14, this upgrade path was not blocked in the code even though it is not supported. Starting with 14SU2, upgrades from release 10.5.2 are now blocked in the code so a direct upgrade attempt will now fail as an usupported upgrade.

Warning for Upgrades with FIPS Enabled

Warning
If you are upgrading with FIPS enabled and/or using PCD with FIPS enabled, see the CiscoSSL7 COP File Readme for information on the COP file ciscocm.ciscossl7_upgrade_CSCwa48315_CSCwa77974_v1.0.k4.cop. This document details the pre-requisites required for direct upgrade or direct migration to the 14SU2 or higher destination versions when FIPS is enabled.

Related Documentation

To view documentation that supports Cisco Unified CM Release 14, go to:

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-documentation-roadmaps-list.html

Before You Begin

Before upgrading, review the Upgrade and Migration Guide > Upgrade Planning for details on:

1. Supported Upgrade Paths

2. Upgrade options - There are multiple upgrade options available: Direct Upgrade, Cluster Upgrade, Fresh Install with Data Import, PCD. Detailed instructions for each may be found in the Installation Guide

3. Hardware, Software, Network, and VM requirements. Open VMWare Tools now default for new installations of version 12.5 and higher, and is recommended for upgrades from earlier versions.

4. Deprecated Phone Models

Compatibility information can be found in the Compatibility Matrix

Installation Instructions

Note
Apply this SU to all of your Cisco Unified Communications Manager servers, beginning with the publisher server and TFTP server

Refer to the *Upgrade and Migration Guide for Cisco Unified Communications Manager and IM and Presence Service, Release 14* for detailed information about doing this upgrade:

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html

Note
Because the 14.0.1.13900-155 build is a non-bootable ISO, it proves useful only for upgrades. You cannot use it for new installations. You may however install with the base version 14.0.1.10000-20 and apply 14.0.1.13900-155 as a patch during the installation.

Release 14SU3 is available in both restricted (which is the release type that has always been available from Cisco) and unrestricted versions of software to comply with import / export restrictions to various countries.

The unrestricted version is available in limited markets. Please refer to the "Export Restricted and Export Unrestricted Software" section in the **Understanding Upgrades and Migrations** chapter, of the *Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service, Release 14* referenced above, for a more detailed description.

Note Once installed, UNRST releases can never be converted or upgraded to releases which support full encryption capabilities

The file names and hash values you will use for this upgrade are:

Table 1: Restricted ISO Names and Checksum Values

ISO Name:	UCSInstall_UCOS_14.0.1.13900-155.sha512.iso
MD5:	e7f8fbc021d4311ef75d763a938f8bfa
SHA512:	07f28d0681562bccd135c52cf741b63c151ba9628b976ef1f0e722433ac6e468ff22fa231955e7c 066a7a669c85106dd23f867bd41c0948ccb7ea8bbf97765a1

Table 2: UnRestricted ISO Names and Checksum Values

ISO Name:	UCSInstall_UCOS_UNRST_14.0.1.13900-155.sha512.iso
MD5:	1aa8671dcfe2d66fbd5e6951959d88fd
SHA512:	21238d53e7451137a67104321ed9209a7770b0c40bbe16431b34a41b603a54be88010253cdb1 1890b34d4d7ff9443477b5d96667bbd174545e9544dadfc5e52b

Reverting to a Previous Version

Note Revert to the previous version on all servers in the cluster in the same order in which you performed the upgrade.

Refer to the "Switch to Previous Version" section in the **Upgrade Procedures** chapter at *Upgrade and Migration Guide for Cisco Unified Communications Manager and IM and Presence Service, Release 14* for detailed instructions on "Reverting to a Previous Version."

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/ products-installation-guides-list.html

Caveats

Caveats describe unexpected behavior on a Cisco Unified Communications server. The following sections contain lists and descriptions of resolved and open caveats in this release.

Resolved Caveats

Resolved Caveats for Cisco Unified Communications Manager Release 14SU3 describes possible unexpected behaviors in Cisco Unified Communications Manager 14 releases.

Resolved CUCM Caveats in 14SU3 (everything fixed in SU3 since SU2)
Click Here for the list

Cumulative Resolved CUCM Caveats (everything fixed in all SU's since base 14)
Click Here for the list

Open Caveats

Open Caveats for Cisco Unified Communications Manager Release 14SU3 describes a few of the possible unexpected behaviors still remaining in Cisco Unified Communications Manager Release 14SU3.

Open CUCM Caveats in 14SU3
CSCwf65881: GUI Authentication failure country specific umlaut characters after upgrading 14SU3
CSCwf67831: Online CA Credential decryption is failing when CAPF is restarted

CUCM Caveats 14 Complete List

For a complete list of caveats applicable to 14, use the following Bug Search Tool link:

https://bst.cloudapps.cisco.com/
bugsearch?pf=prdNm&sb=afr&kw=*&bt=custV&prdNam=Cisco%20Unified%20Communications%20Manager%20(CallManager)&rls=14.0(1.1

To determine the caveats that were open for a specific release, use the following steps (the screenshots below are from Excel for Mac, the Excel for Windows options are a little different but follow the same basic flow):
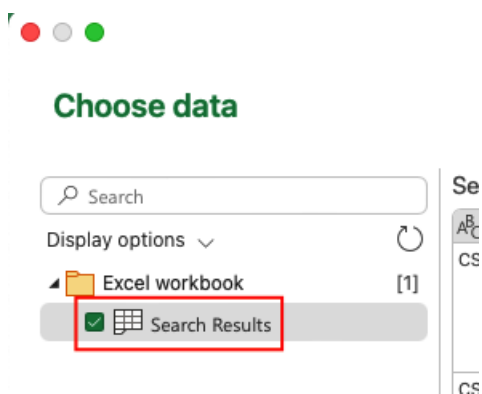
1. Click on the "Export Results to Excel" link

2. Open the downloaded file in Excel and Save As a .xlsx file

3. Open a blank Excel workbook

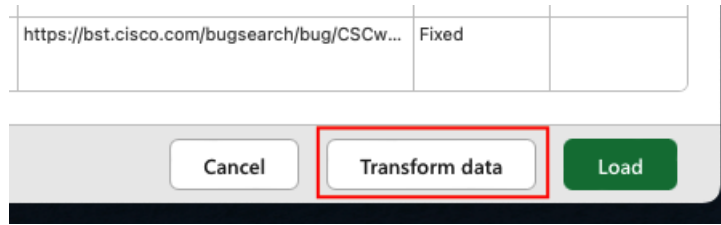4. Click on Data --> Get Data (Power Query)
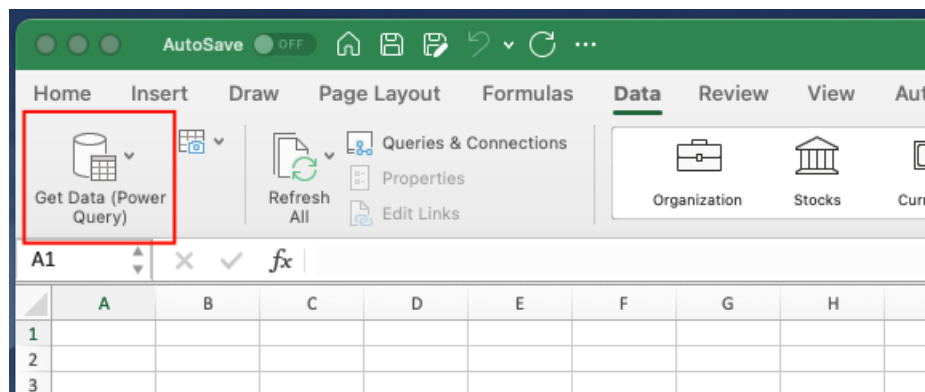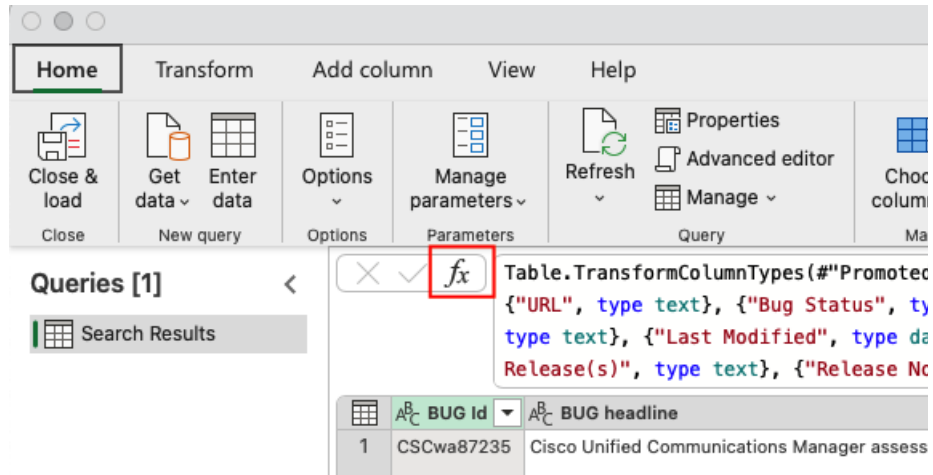

5. Choose "Excel workbook" as the source.
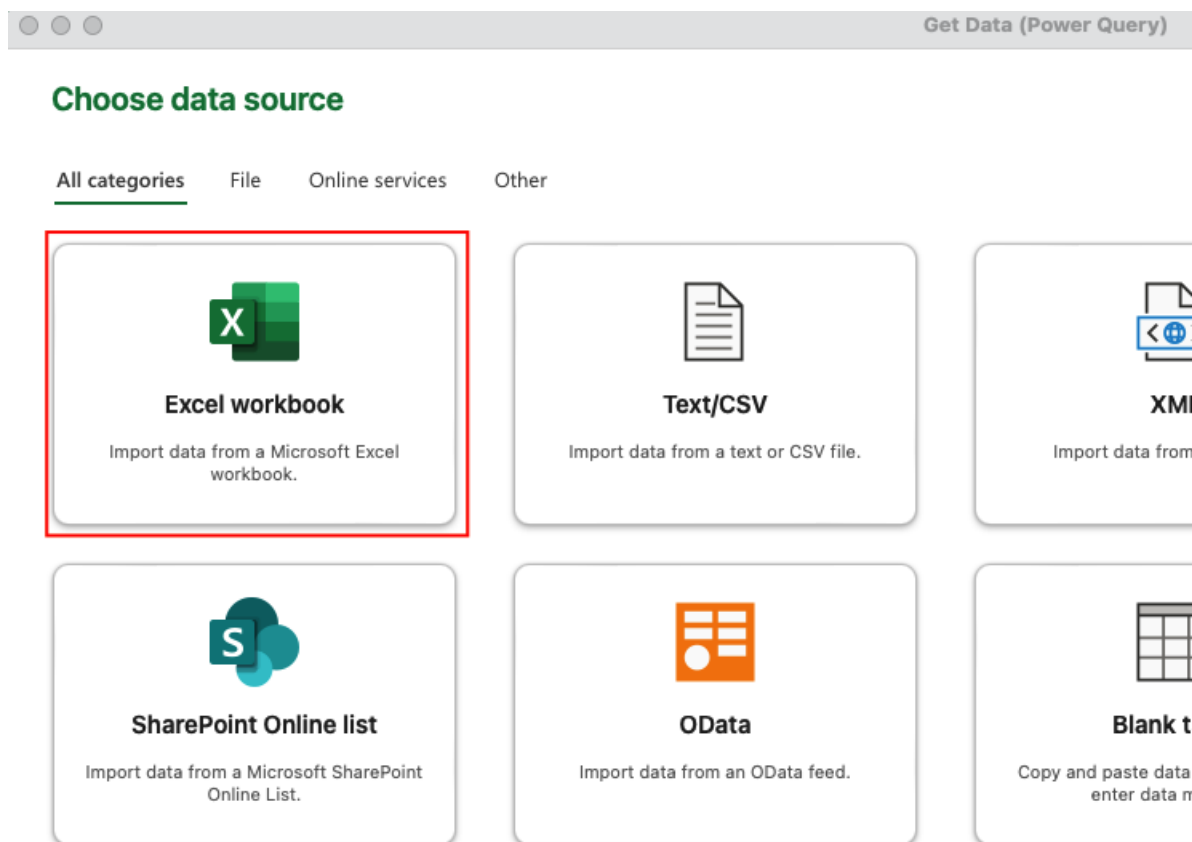
6. Click "Browse", select the .xlsx file saved previously, and click Next

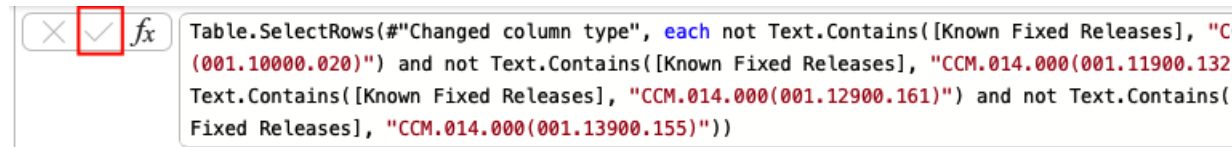7. Click the checkbox next to the Tab name (by default it will be Search Results)

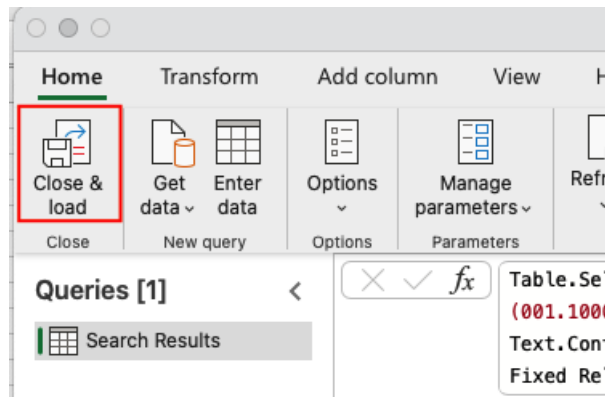8. Click on the "Transform Data" button

9. Click on the fx button to insert a new step

10. In the text box next to the fx button, paste the desired filter string (see below)

11. Click the check mark to apply the changes

12. Click the "Close and load" button

13. The results that are loaded into the Excel workbook will be all of the Open Caveats for that specific release

Filter String for 14SU3:

For Mac:
Table.SelectRows(#"Changed column type", each not Text.Contains([Known Fixed Releases], "CCM.014.000(001.10000.020)") and not Text.Contains([Known Fixed Releases], "CCM.014.000(001.11900.132)") and not Text.Contains([Known Fixed Releases], "CCM.014.000(001.12900.161)") and not Text.Contains([Known Fixed Releases], "CCM.014.000(001.13900.155)") and not Text.StartsWith([Known Fixed Releases], "UCMAP") and Text.Contains([#"Product - Series"], "CallManager"))

For Windows:
= Table.SelectRows(#"Changed Type", each not Text.Contains([Known Fixed Releases], "CCM.014.000(001.10000.020)") and not Text.Contains([Known Fixed Releases], "CCM.014.000(001.11900.132)") and not Text.Contains([Known Fixed Releases], "CCM.014.000(001.12900.161)") and not Text.Contains([Known Fixed Releases], "CCM.014.000(001.13900.155)") and not Text.StartsWith([Known Fixed Releases], "UCMAP") and Text.Contains([#"Product - Series"], "CallManager"))

Security Advisory Caveats: To get a list of caveats that are applicable to Security Advisories or other security related issues, after filtering for a specific release using the examples above, an additional filter for the keyword PSIRT can be applied to the Release Note Enclosure column.

Firmware Versions

SUs contain firmware loads, however, Cisco recommends that you always download the latest firmware load from the Software Download Center.

Phone Firmware

To download phone firmware, follow this procedure:

1. Go to https://software.cisco.com/download/home

2. Click on Browse All

3. Click on Collaboration Endpoints

4. Choose the desired Endpoint Type

5. Choose the desired Endpoint Model

Device Packages

To download phone firmware, follow this procedure:

1. Go to https://software.cisco.com/download/home

2. Click on Browse All

3. Click on Unified Communications

4. Click on Call Control

5. Click on Unified Communications Manager (CallManager)

6. Choose the desired UCM version

7. Click on the Device Packages link

Firmware Versions in this Release

```
Device type                            Load name                        Version
-------------------------------------- -------------------------------- ----------
3905                                   3905.9-4-1SR3                    9.4(1SR3.0)
3911_3951-sip                          3911_3951-sip.8-1-4a             8.1(4.0)
6608                                   6608-4.0.0.32-mgcp               4.0(0.32)
6608cfb                                6608cfb-4.0.0.03-sccp            4.0(0.3)
6608mtp                                6608mtp-4.0.0.06-sccp            4.0(0.6)
6624                                   6624-4.0.0.13-mgcp               4.0(0.13)
6901-sccp                              6901-sccp.9-3-1-SR2-2            9.3(1.0)
6901-sip                               6901-sip.9-3-1-SR2-3             9.3(1.0)
6911-sccp                              6911-sccp.9-3-1-SR2-3            9.3(1.0)
6911-sip                               6911-sip.9-3-1-SR2-4            9.3(1.0)
6945-SCCP                              6945-SCCP-9-4-1-3SR3             9.4(1.3)
6945-SIP                               6945-SIP-9-4-1-3SR3             9.4(1.3)
69xx-SCCP                              69xx-SCCP-9-4-1-3SR3            9.4(1.3)
69xx-SIP                               69xx-SIP-9-4-1-3SR3            9.4(1.3)
7832-sip.14                            7832-sip.14-2-1-0001-14.k4      14.2.1(0001.14)
78xx.14                                78xx.14-2-1-0001-14.k4          14.2.1(0001.14)
7911_7906-sccp                         7911_7906-sccp.9-4-2SR3-1       9.4(2SR3.1)
7911_7906-sip                          7911_7906-sip.9-4-2SR3-1        9.4(2SR3.1)
7914-sccp                              7914-sccp.5-0-4                 5.0(4.0)
7915                                   7915.1-0-4-2                    1.0(4.2)
7916                                   7916.1-0-4-2                    1.0(4.2)
7925-sccp                              7925-sccp.1-4-8SR1-5.k3         1.4(8SR1.5)
7926-sccp                              7926-sccp.1-4-8SR1-5.k3         1.4(8SR1.5)
7931-sccp                              7931-sccp.9-4-2SR2-2            9.4(2SR2.2)
7931-sip                               7931-sip.9-4-2SR2-2             9.4(2SR2.2)
7936-sccp                              7936-sccp.3-3-21                3.3(21.0)
7937                                   7937-1-4-5-7-SCCP               1.4(5.7)
7940-7960                              7940-7960-8.12.00-sip           8.12(00.0)
7940-7960-sccp                         7940-7960-sccp.8-1-2SR2         8.1(2SR2.0)
7941_7961-sccp                         7941_7961-sccp.9-4-2SR3-1       9.4(2SR3.1)
7941_7961-sip                          7941_7961-sip.9-4-2SR3-1        9.4(2SR3.1)
7942_7962-sccp                         7942_7962-sccp.9-4-2SR3-1       9.4(2SR3.1)
7942_7962-sip                          7942_7962-sip.9-4-2SR3-1        9.4(2SR3.1)
7945_7965-sccp                         7945_7965-sccp.9-4-2SR3-1       9.4(2SR3.1)
7945_7965-sccp                         7945_7965-sccp.9-4-2SR4         9.4(2SR4.0)
7945_7965-sip                          7945_7965-sip.9-4-2SR4-3        9.4(2SR4.3)
7975-sccp                              7975-sccp.9-4-2SR3-1            9.4(2SR3.1)
7975-sccp                              7975-sccp.9-4-2SR4             9.4(2SR4.0)
7975-sip                               7975-sip.9-4-2SR4              9.4(2SR4.0)
7985                                   7985-4-1-7-0-sccp               4.1(7.0)
8821-sip                               8821-sip.11-0-6SR4-3.k4         11.0(6SR4.3)
8831-sip                               8831-sip.10-3-1SR7-2            10.3(1SR7.2)
8832-sip.14                            8832-sip.14-2-1-0001-14.k4      14.2.1(0001.14)
8845_65-sip.14                         8845_65-sip.14-2-1-0001-14.k4   14.2.1(0001.14)
88xx-sip.14                            88xx-sip.14-2-1-0001-14.k4      14.2.1(0001.14)
894x-sccp                              894x-sccp.9-4-2SR3-1            9.4(2SR3.1)
894x-sip                               894x-sip.9-4-2SR3-1            9.4(2SR3.1)
8961                                   8961.9-4-2SR4-1.k3             9.4(2SR4.1)
9951                                   9951.9-4-2SR4-1.k3             9.4(2SR4.1)
9971                                   9971.9-4-2SR4-1.k3             9.4(2SR4.1)
ata                                    ata-3.2.4-sccp                 3.2(4.0)
ata187                                 ata187.9-2-3-1                 9.2(3.1)
ata190                                 ata190.1-2-2-003_SR2-1         1.2(2.3)
ATA191.12                              ATA191.12-0-1-0506-010         12.0.1(0506.10)
headset-builtin                        headset-builtin.3-1-0001-1.k4  3.1(0001.1)
PHONEOS-8875.2                         PHONEOS-8875.2-0-1-0001-16     2.0.1(0001.16)
```

```
Plug-in Report
----------------------------------------
cm-rtmt-client-plugin-14.0.0.0-0.i386.rpm
cm-ctlc-plugin-6.0.0.1-1.i386.rpm
cm-taps-plugin-7.0.2.0-1.i386.rpm
cm-tsp-plugin-14.0.1.0-0.i386.rpm
cm-axlsqltoolkit-plugin-1.1.0.0-1.i386.rpm
cm-jtapi-plugin-14.0.1.13900-3.i386.rpm

TZDATA file                             Version
-------------------------------------  ----------
platform-tzdata-2022g-1.el7_9.noarch.rpm  2022-g
```