Release Notes for the Ultra Cloud Core Subscriber Management Infrastructure Version 2023.04.1.12

First Published: 2023-10-17

Ultra Cloud Core Subscriber Management Infrastructure

Introduction

This Release Notes identifies changes and issues related to this software release.

Release Lifecycle Milestones

Release Lifecycle Milestone	Milestone	Date
First Customer Ship	FCS	31-Oct-2023
End of Life	EoL	31-Oct-2023
End of Software Maintenance	EoSM	30-Apr-2025
End of Vulnerability and Security Support	EoVSS	30-Apr-2025
Last Date of Support	LDoS	30-Apr-2026

These milestones and the intervals between them are defined in the Cisco Ultra Cloud Core (UCC) Software Release Lifecycle Product Bulletin available on cisco.com.

Release Package Version Information

Software Packages	Version
smi-install-disk.20.04.0-20231009.iso.SPA.tgz	20.04.0-20231009
cee.2023.04.1.12.SPA.tgz	2023.04.1.12
cluster-deployer-2023.04.1.12.SPA.tgz	2023.04.1.12

Descriptions for the various packages provided with this release are provided in the Release Package Descriptions, on page 5 section.

Verified Compatibility

UCS Server	CIMC Firmware Version
Cisco UCS C220 M6	4.2(2a) or later
Cisco UCS C220 M5	4.1(3f) or later

What's New in this Release

New in Documentation

This version of Release Notes includes a new section titled **What's New in this Release** comprising all new features, enhancements, and behavior changes applicable for the release.

This section will be available in all the 5G release notes and will supersede content in the Release Change Reference (RCR) document. Effective release 2024.01, the RCR document will be deprecated.

Features and Enhancements

This section covers a brief description of the features and enhancements introduced in this release. It also includes links to detailed documentation, where available.

Feature	Description
Configurable XFS File System	SMI supports a new XFS file system to install the */data* partition using Mongo DB for new deployments. This file system can be configured using the **smi-data fs-type xfs** command. **Default Setting**: Disabled – Configuration required to enable
CPU Isolation	SMI provides a higher level of CPU isolation for VPP workers to support cnUPF. Using the host profile, SMI defines isolcpu to isolate CPUs from the kernel scheduler. **Default Setting**: Disabled – Configuration required to enable
Kubernetes Version Upgrade	With this release, the Kubernetes version is upgraded from 1.25 to 1.26. **Default Setting**: Enabled – Always On
UCS M7 Server Support	SMI Bare Metal supports the UCS C220 M7 server with a single socket for Private 5G deployments in this release. The Cisco UCS C220 M7 Rack Server is a high-density, 1RU, general-purpose infrastructure and application server that provides industry-leading performance and efficiency. **Note** The UCS M7 server is not supported for on-prem deployments.

Related Documentation

For a complete list of documentation available for this release, go to: https://www.cisco.com/c/en/us/support/wireless/ultra-cloud-core-subscriber-microservices-infrastructure/tsd-products-support-series-home.html

Installation and Upgrade Notes

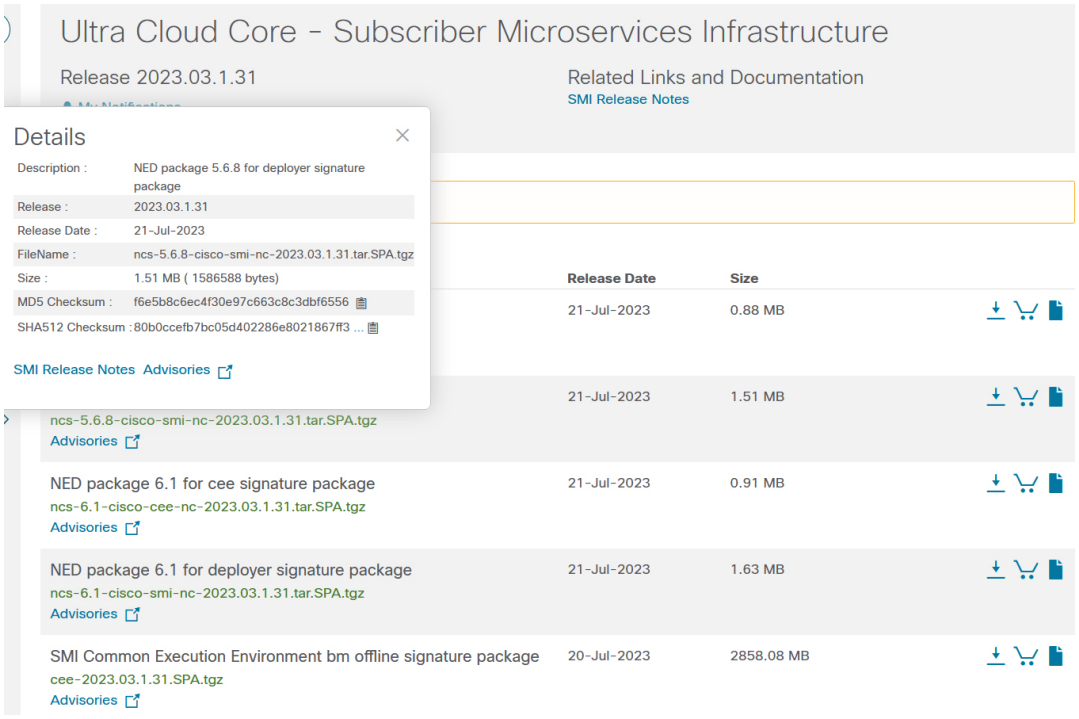
This Release Note does not contain general installation and upgrade instructions. Refer to the existing installation documentation for specific installation and upgrade considerations.

Note In this release, you must install a patch to use all the functionalities in SMI. For more information, contact your Cisco Account representative.

Software Integrity Verification

To verify the integrity of the software image you have from Cisco, you can validate the SHA512 checksum information against the checksum identified by Cisco for the software.

Image checksum information is available through **Cisco.com Software Download Details.** To find the checksum, hover the mouse pointer over the software image you have downloaded.



At the bottom you find the SHA512 checksum, if you do not see the whole checksum you can expand it by pressing the "..." at the end.

To validate the information, calculate a SHA512 checksum using the information in the following table and verify that it matches with the one provided on the software download page.

To calculate a SHA512 checksum on your local desktop, refer to the following table please.

Table 1: Checksum Calculations per Operating System

Operating System	SHA512 Checksum Calculation Command Examples
Microsoft Windows	Open a command line window and type the following command: **> certutil.exe -hashfile <filename>.<extension> SHA512**
Apple MAC	Open a terminal window and type the following command: **$ shasum -a 512 <filename>.<extension>**
Linux	Open a terminal window and type the following command: **$ sha512sum <filename>.<extension>** Or **$ shasum -a 512 <filename>.<extension>**
NOTES: <*filename*> is the name of the file. <*extension*> is the file extension (e.g. .zip or .tgz).	

If the SHA512 checksum matches, you can be sure that no one has tampered with the software image, or the image has not been corrupted during download.

If the SHA512 checksum does not match, we advise you to not attempt upgrading any systems with the corrupted software image. Download the software again and verify the SHA512 checksum again. If there is a constant mismatch, please open a case with the Cisco Technical Assistance Center.

Certificate Validation

SMI software images are signed via x509 certificates. Please view the .README file packaged with the software for information and instructions on how to validate the certificates.

Open Bugs for This Release

The following table lists the open bugs in this specific software release.

Note This software release may contain open bugs first identified in other releases. Additional information for all open bugs for this release are available in the Cisco Bug Search Tool.

Bug ID	Headline
CSCwh85836	Only 16 VPP threads being used on M6 UPF instead of 24

Resolved Bugs for This Release

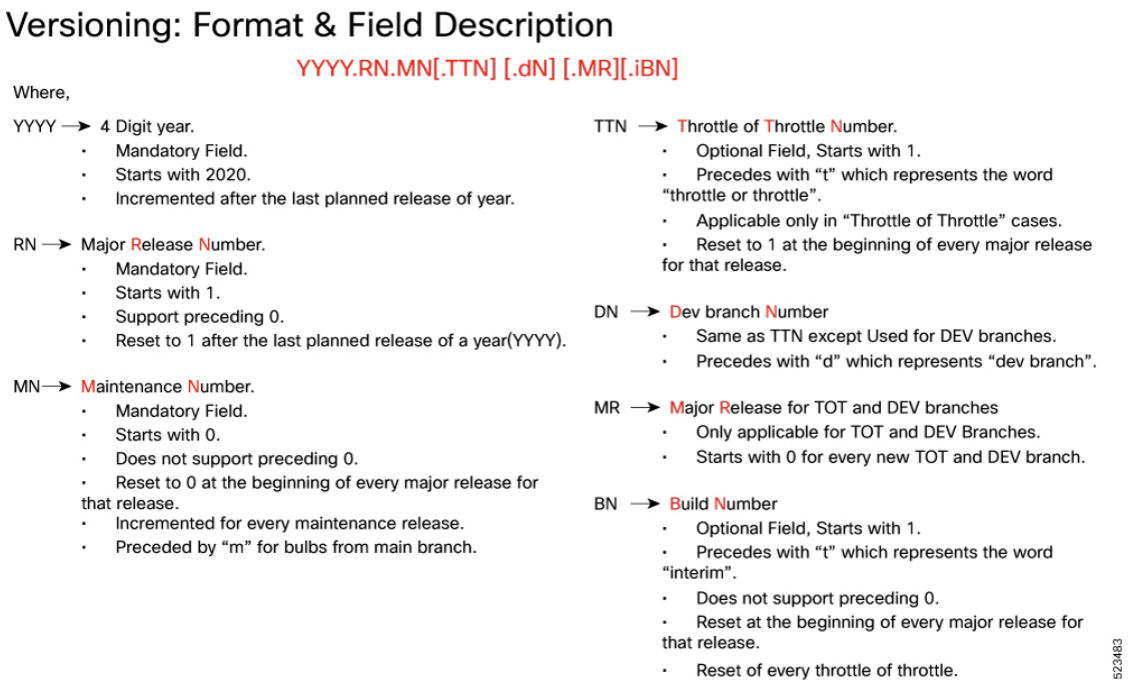
The following table lists the resolved bugs in this specific software release.

Bug ID	Headline	Behavior Change
CSCwh50257	Cluster sync failed during SMF upgrade to ccg.2023.03.m0.d8.0.i30	No

Operator Notes

Cloud Native Product Version Numbering System

The **show helm list** command displays detailed information about the version of the cloud native product currently deployed.



The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research software releases.

Release Package Descriptions

The following table lists the descriptions for packages that are available with this release.

Table 2: Release Package Information

Software Packages	Description
base.<version>.iso.SPA.tgz	The application-level POD ISO image signature package for use with bare metal deployments. This package contains the base ISO image as well as the release signature, certificate, and verification information.
cee.<version>SPA.tgz	The SMI Common Execution Environment (CEE) offline release signature package. This package contains the CEE deployment package as well as the release signature, certificate, and verification information.
cluster-deployer-<version>.SPA.tgz	The SMI Deployer image signature package for use with bare metal deployments. This package contains the Deployer v image as well as the release signature, certificate, and verification information.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, refer to https://www.cisco.com/c/en/us/support/index.html.

© 2023 Cisco Systems, Inc. All rights reserved.