



UCC 5G UPF Release Notes, Release 2024.03.1

First Published: 2024-09-05

Ultra Cloud Core User Plane Function

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-Jul-2024
End of Life	EoL	31-Jul-2024
End of Software Maintenance	EoSM	29-Jan-2026
End of Vulnerability and Security Support	EoVSS	29-Jan-2026
Last Date of Support	LDoS	31-Jan-2027

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
companion-vpc-2024.03.1.zip.SPA.tar.gz	2024.03.1
qvpc-si-2024.03.1.bin.SPA.tar.gz	2024.03.1
qvpc-si-2024.03.1.qcow2.zip.SPA.tar.gz	2024.03.1
NED package	ncs-6.1.11-cisco-staros-5.53
NSO	6.1.11

Use this [link](#) to download the NED package associated with the software.

Descriptions for the various packages provided with this release are available in the [Release Package Descriptions, on page 7](#) section.

Verified Compatibility

Products	Version
ADC Plugin	2.74.2.2209
RCM	2024.03.0
Ultra Cloud Core SMI	2024.03.1.12
Ultra Cloud Core SMF	2024.03.0

What's New in this Release

Features and Enhancements

There are no features or enhancements in this release.

Behavior Changes

This section covers a brief description of behavior changes introduced in this release.

Behavior Change	Description
Increased BGP Monitoring Capacity in RCM	<p>This release supports the following enhancements for BGP monitoring in RCM:</p> <ul style="list-style-type: none"> Configurable number of BGP monitors is increased from 16 to 26 Configurable number of BGP monitor groups is increased from 10 to 13 <p>Previous Behavior: You were allowed to configure a maximum number of 16 BGP monitors and 10 BGP monitor groups in RCM.</p> <p>New Behavior: You can now configure up to 26 BGP monitors and 13 BGP monitor groups in RCM. Use the monitor bgp context context_name peer-ip [group group_number] CLI command in RCM Config mode to enable the configuration.</p>
Reject Update FAR with Cause IE	<p>Previous Behavior: The session manager on UPF used to crash when SMF sends Update FAR for any FAR without an associated PDR.</p> <p>New Behavior: When SMF sends Update FAR for an unassociated FAR, UPF will now reject it with the MANDATORY_IE_INCORRECT (69) PFCP cause.</p> <p>Customer Impact: UPF will handle Update FAR gracefully and reject Sx Modify Request, while SMF is expected to tear down the session.</p>

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.

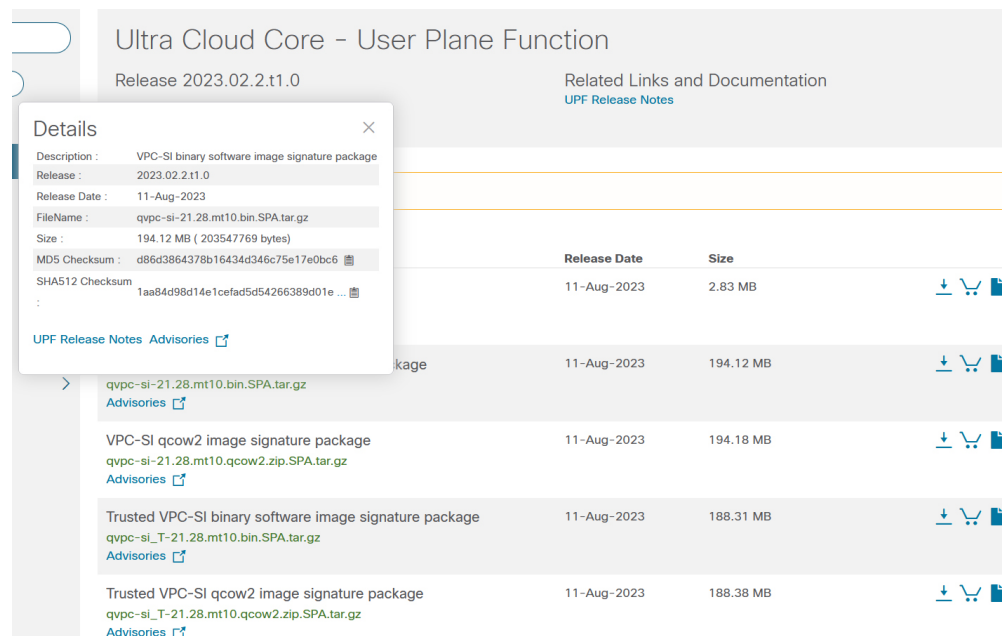
Software Integrity Verification

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.

The following screenshot is an example of a UPF release posted in the Software Download page.

Figure 1:



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 Table 1 and verify that it matches either the one provided on the software download page.

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

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

Operating System	SHA512 checksum calculation command examples
Apple MAC	Open a terminal window and type the following command: \$ shasum -a 512 <i>filename.extension</i>
Linux	Open a terminal window and type the following command: \$ sha512sum <i>filename.extension</i> OR \$ shasum -a 512 <i>filename.extension</i>
NOTES: <i>filename</i> is the name of the file. <i>extension</i> is the file extension (for example, .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

UPF 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	Product
CSCwk66799	UPF performance improvement for DATA call model	UPF
CSCwk74741	vpp throws error at non-existent physical address	UPF
CSCwk84615	vpnmgr resiliency event takes around 9-10 min to program the vrf	UPF
CSCwm38238	VRCC feature not having support in smart license	UPF
CSCwm39952	NSO takes additional cli "group" for deleting BGP monitors	NSO
CSCwm40737	sessmgr gives error at sessmgr_uplane_cleanup_clp_data()	UPF

Resolved Bugs for this Release

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



Note This software release may contain resolved bugs first identified in other releases. Additional information for all resolved bugs for this release are available in the [Cisco Bug Search Tool](#).

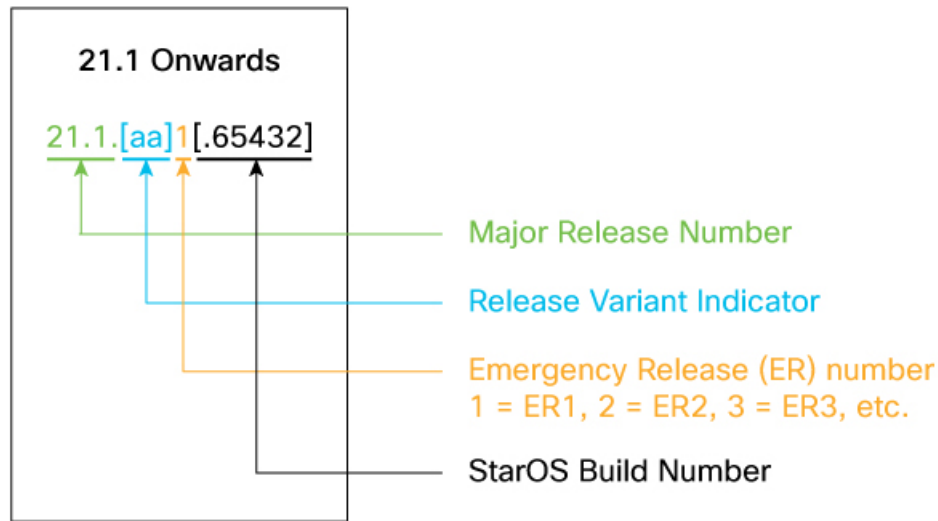
Bug ID	Headline	Behavior Change
CSCwj98482	IP chunks not cleared post association release when sxdemux/sessmgr recovery is there.	No
CSCwk83598	hat system crash leads to change in boot config the new-standby	No
CSCwk83702	Continuous sessmgr restart with function sessmgr_uplane_send_sx_sess_report_req()	No
CSCwk84612	Increase the max configurable BGP Monitors limit	Yes
CSCwk91422	21.28.m16 UPF EDR charging volume bytes seem to be limited to 2GB	No
CSCwm08155	Seeing issue with burtsy traffice limiting the okala speed test throughput	No
CSCwm14072	bulkstat cli getting stuck with performance driven schema	No
CSCwm14726	sessmgr restart @ sessmgr_uplane_process_sx_update_far	Yes
CSCwm33315	Increase RCM BGP Monitor Group limit to 13 to support 26 BGP Monitors	Yes

Operator Notes

StarOS Version Numbering System

The output of the **show version** command displays detailed information about the version of StarOS currently running on the ASR 5x00 or Cisco Virtualized Packet Core platform.

The Version Build Number for releases 21.1 and later include a major and emergency release number, for example, "21.1.1".



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.



Note The 5G UPF software is based on StarOS and implements the version numbering system described in this section. However, as a 5G network function (NF), it is posted to Cisco.com under the Cloud Native Product Numbering System as described in [Cloud Native Product Version Numbering System, on page 6](#).

Cloud Native Product Version Numbering System

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

Versioning: Format & Field Description

YYYY.RN.MN[.TTN] [.dN] [.MR][.iBN]

Where,

YYYY → 4 Digit year.

- Mandatory Field.
- Starts with 2020.
- Incremented after the last planned release of year.

RN → Major Release Number.

- Mandatory Field.
- Starts with 1.
- Support preceding 0.
- Reset to 1 after the last planned release of a year(YYYY).

MN → Maintenance Number.

- Mandatory Field.
- Starts with 0.
- Does not support preceding 0.
- Reset to 0 at the beginning of every major release for that release.
- Incremented for every maintenance release.
- Preceded by "m" for bulbs from main branch.

TTN → Throttle of Throttle Number.

- Optional Field, Starts with 1.
- Precedes with "t" which represents the word "throttle or throttle".
- Applicable only in "Throttle of Throttle" cases.
- Reset to 1 at the beginning of every major release for that release.

DN → Dev branch Number

- Same as TTN except Used for DEV branches.
- Precedes with "d" which represents "dev branch".

MR → Major Release for TOT and DEV branches

- Only applicable for TOT and DEV Branches.
- Starts with 0 for every new TOT and DEV branch.

BN → Build Number

- Optional Field, Starts with 1.
- Precedes with "t" which represents the word "interim".
- Does not support preceding 0.
- Reset at the beginning of every major release for that release.
- Reset of every throttle of throttle.

523483

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 provides descriptions for the packages that are available with this release.

Software Packages	Description
companion-vpc-<staros_version>.zip.SPA.tar.gz	Contains files pertaining to VPC, including SNMP MIBs, RADIUS dictionaries, ORBEM clients, etc. These files pertain to both trusted and non-trusted build variants. The VPC companion package also includes the release signature file, a verification script, the x.509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-<staros_version>.bin.SPA.tar.gz	The UPF release signature package. This package contains the VPC-SI deployment software for the UPF as well as the release signature, certificate, and verification information. Files within this package are nested under a top-level folder pertaining to the corresponding StarOS build.

Software Packages	Description
qyipc-si-<staros_version>.qcow2.zip.SPA.tar.gz	<p>The UPF release signature package. This package contains the VPC-SI deployment software for the UPF as well as the release signature, certificate, and verification information.</p> <p>Files within this package are nested under a top-level folder pertaining to the corresponding StarOS build.</p>
ncs-<nso_version>-cisco-staros-<version>.signed.bin	<p>The NETCONF NED package. This package includes all the files that are used for NF configuration.</p> <p>Note that NSO is used for NED file creation.</p>

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>.

