Release Notes for the Ultra Cloud Core User Plane Function Version 2023.03.0

First Published: July 28, 2023

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-2023
End of Life	EoL	31-Jul-2023
End of Software Maintenance	EoSM	28-Jan-2025
End of Vulnerability and Security Support	EoVSS	28-Jan-2025
Last Date of Support	LDoS	31-Jan-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
companion-vpc-21.28.m11.tgz.SPA.tar.gz	21.28.m11
qvpc-si-21.28.m11.bin.SPA.tar.gz	21.28.m11
qvpc-si-21.28.m11.qcow2.tgz.SPA.tar.gz	21.28.m11
qvpc-si_T-21.28.m11.bin.SPA.tar.gz	21.28.m11
qvpc-si_T-21.28.m11.qcow2.tgz.SPA.tar.gz	21.28.m11
NED package	ncs-6.1.2-cisco-staros-5.50.2
NSO	6.1.2

Descriptions for the various packages provided with this release are available in the Release Package Descriptions section.

Verified Compatibility

Products	Version
ADC Plugin	2.73.2.1718
RCM	2023.03.0
Ultra Cloud Core SMI	2023.03.1
Ultra Cloud Core SMF	2023.03.0

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-user-plane-function/series.html

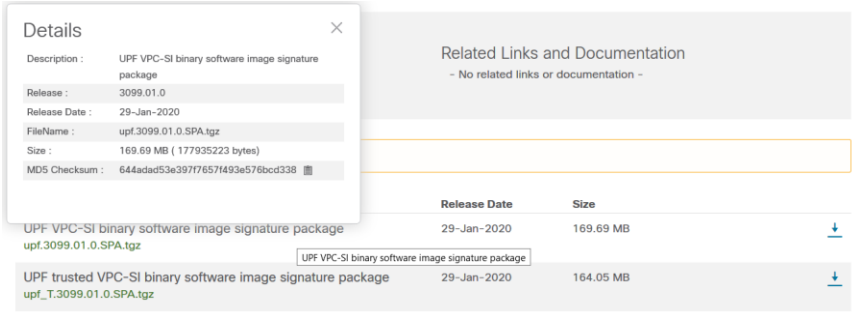
Installation and Upgrade Notes

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

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 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 please see the table below.

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

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
CSCwf11828	Error logs Invalid FAR with id 5 received in PDU. IMSI: 311480071230621 Interface: N4
CSCwf40504	After planned switchover seen session disconnect with reason graceful-cleanup-on-audit-fail
CSCwf77945	The CPU 1/0 is running low on memory. (0M free)
CSCwf84872	Seen Error logs with sessmgr task kill

Bug ID	Headline
CSCwf85212	Max 2-pcaps are generating instead of 4 in UPF for slowpath
CSCwf93466	vpp error at hatsystem_process_card_fail_msg()
CSCwf96687	sm restart observed on stdby HUPF at sessmgr_recover_uplane_pdr_info() post SWO
CSCwh02919	4g converged and non converged calls getting drop with echo req/res on MPLS over N9
CSCwh04079	MPLS routing not working between HUPF and VUPF on hermes branch
CSCwh04938	sessmgr restart observed at sn_slist_remove_by_key()

Resolved Bugs for this Release

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

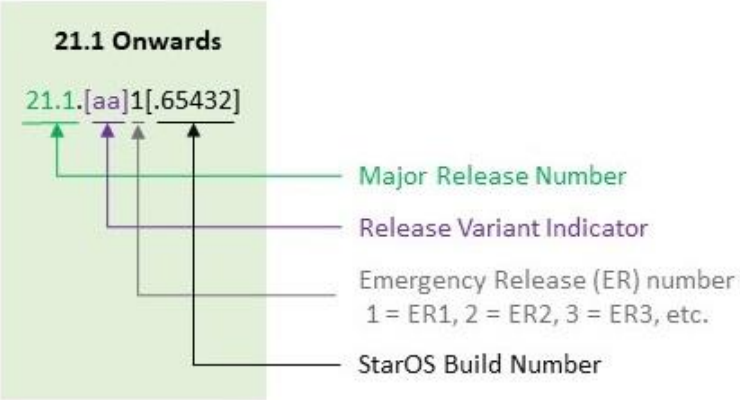
Bug ID	Headline	Behavior Change
CSCwd60981	UPF does not initiate Sx_Session_Report_Req after receiving GTP_ERROR_IND_MSG	No
CSCwe33291	Continuous error logs on standby UPF "SMGR ID mismatch during recovery"	No
CSCwe74774	Sx status report is not sent for 4G/Wifi calls	No
CSCwe88330	Continuous error logs on vpnmgr - RTNETLINK socket recv buffer under on hermes	No
CSCwe96265	Exit code in case of converged 4G calls is not correct, monsub enabled using console/smf	No
CSCwf45714	4G Homer Echo Request Tx stats not getting updated	No
CSCwf84260	bgp stuck after doing port shut/no shut	No

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”.

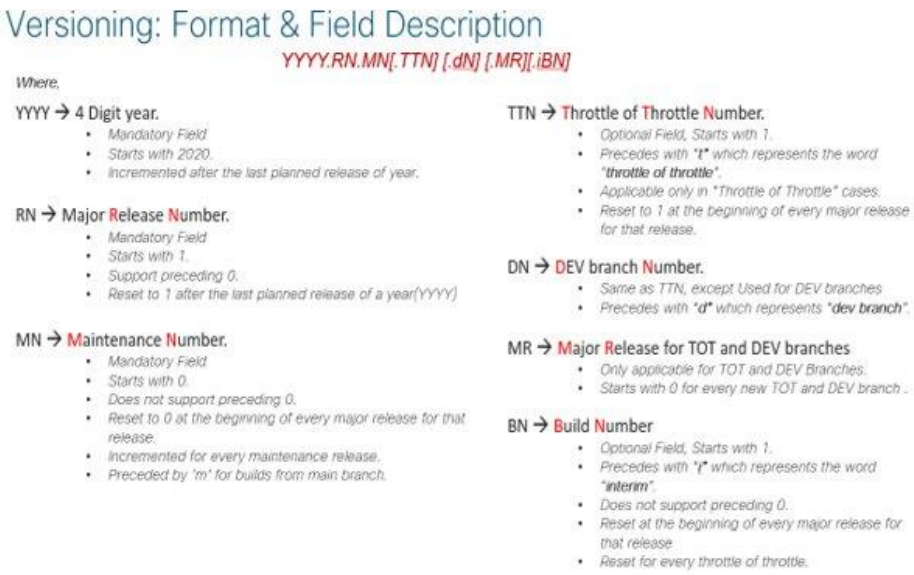


The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research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

Cloud Native Product Version Numbering System



Release Package Descriptions

Table 2 provides descriptions for the packages that are available with this release.

Table 2 - Release Package Information

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.
qvpc-si-<staros_version>.qcow2.zip.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.
qvpc-si_T-<staros_version>.bin.SPA.tar.gz	The trusted 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.
qvpc-si_T-<staros_version>.qcow2.zip.SPA.tar.gz	The trusted 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.
ncs-<nso_version>-cisco-staros-<version>.signed.bin	The NETCONF NED package. This package includes all the files that are used for NF configuration. Note that NSO is used for NED file creation.

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.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANYKIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITHTHE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSEOR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright ©1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.