Release Notes for the Ultra Cloud Core User Plane Function Version 2023.04.0

First Published: 2023-10-30

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-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
companion-vpc-21.28.m16.tgz.SPA.tar.gz	21.28.m16
qvpc-si-21.28.m16.bin.SPA.tar.gz	21.28.m16
qvpc-si-21.28.m16.qcow2.tgz.SPA.tar.gz	21.28.m16
NED package	ncs-6.1.3-cisco-staros-5.50.8
NSO	6.1.3

Descriptions for the various packages provided with this release are available in the Release Package Descriptions, on page 11 section.

Verified Compatibility

Products	Version
ADC Plugin	2.73.4.1828
RCM	2023.04.0
Ultra Cloud Core SMI	2023.04.1
Ultra Cloud Core SMF	2023.04.0

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
Binding Multiple GTPU IP Addresses	UPF allows binding of multiple GTPU IP addresses to provide high uplink throughput in Private 5G deployments. UPF creates unique GTPU 3-tuple hash entries to ensure uniform distribution of ingress traffic on all VPP worker threads. **Default Setting**: Enabled – Always-on
EDR Last Uplink and Downlink Packet Time Attributes	The EDR configuration supports two new attributes **sn-last-uplink-pkt-time** and **sn-last-downlink-pkt-time** to identify the data stall issue. **Default Setting**: Disabled – Configuration required to enable
NAT Support on the N4 Interface	The Network Address Translation (NAT) feature translates non-routable private IP addresses to routable public IP addresses from a pool of public IP addresses. UPF supports NAT on the N4 interface to configure network addresses and send NAT binding records to N4. The NAT policy and IP pool for NAT public IP addresses are configured on UPF for N4. **Default Setting**: Disabled – Configuration required to enable

Feature	Description
Recalculate Measurement IE on the N4 Interface	UPF supports the Recalculate Measurement custom IE as received over the N4 interface. This IE is added to the Update-URR process (URR-ID: Gz-Bearer) to support the PGW-CDR generation due to the max_LOSDV change condition.
Support for Multiple N4/Sx Interfaces	A single UPF can establish multiple N4 or Sx interfaces with any number of control plane network functions such as SMF, cnSGWc, SAEGW-C, PGW-C, and SGW-C. The maximum number of supported N4/Sx peer nodes has been increased from 16 nodes to 18 nodes in this release. **Default Setting**: Disabled – Configuration required to enable
TCP Idle Timeout Action	The Firewall feature inspects subscriber traffic performing IP session-based access control to protect subscribers from security attacks. UPF supports the TCP Idle Timeout action to drop the subscriber flow or send reset on TCP timeout expiry. **Default Setting**: Disabled – Configuration required to enable
WPS Prioritization on UPF	The Wireless Priority Services (WPS) feature provides finer control for priority handling over multiple interfaces. UPF supports WPS services based on the message priority indicated by SMF. The configured priority value set on SMF will be sent to UPF over N4 as part of the PFCP header. **Default Setting**: Disabled – Configuration required to enable

Behavior Changes

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

Behavior Change	Description
Discard Reason Statistics	**Previous Behavior**: In the **show sx-service statistics all** CLI command, some discard reason statistics were listed under "Session Management Messages:". **New Behavior**: All discard reason statistics will now be listed under "Session Rejection Stats:" in the output of the **show sx-service statistics all** CLI command.

Behavior Change	Description

Returning Correct PFCP Cause Code	UP sends the PFCP error cause code PFCP_CAUSE_NO_RESOURCE_AVAILABLE in the following failure scenarios during:
	• Sx Establishment Request and Sx Modification request message processing
	  • Bearer stream creation failure for Sxa
	  • TEP row add failure for Sxa
	  • Local GTPU endpoint address mismatch or unavailability
	  • Above failure scenarios for N4 visited call
	• PFCP_IE_QGR_INFO IE processing memory failures
	• NAT rulebase change or policy change cases and failure due to
	  • FW-and-NAT policy initilization failure during call setup or rulebase change
	  • Invalid CLP destination context
	  • Memory allocation failure
	• Sx Establishment or Sx Modification message processing – local GTPU TEID allocation failure
	Previous Behavior: UP sent the error cause PFCP_CAUSE_REQUEST_REJECTED for the above failure scenarios.
	New Behavior: UP sends the error cause PFCP_CAUSE_NO_RESOURCE_AVAILABLE instead of PFCP_CAUSE_REQUEST_REJECTED for the above failure scenarios.

Roaming Status during Inter-PLMN Handover	**Previous Behavior**: The Old Roaming Status field in the output of the **show subscribers user-plane-only full all** command was defined for both intra-PLMN and inter-PLMN handover. **New Behavior**: The Old Roaming Status field in the output of the **show subscribers user-plane-only full all** command is applicable for inter-PLMN handover only. This field will not be defined for intra-PLMN HO.

Behavior Change	Description
Sending Offending IE during UPF Handover Failure	**Previous Behavior**: During an error scenario where incorrect IMSI is used due to wrong TEID for the same UPF combo call, handover used to pass. **New Behavior**: If IMSI mismatches during the same UPF combo call handover, then Handover Modify Request fails with offending IE Outer Header Creation (OHC). **Customer Impact**: The customer will observe handover failure in the error scenario.
Session Manager ID Check in TEID	The behavior of UPF has changed in the following scenarios for a converged core call when: • N4 and SxA are on the same UPF • S-GW relocation is triggered where target SGW-u is same as that of source SGW-u • SMF initiates N4 Modification to update downlink FAR with new TEID and IP • UPF uses the TEID and finds the target Sxa session **Previous Behavior**: If the Sxa session was not found, then UPF updated FAR and retained the N4 call as combo only. **New Behavior**: UPF inspects SMGR-ID in TEID: • If SMGR-ID in TEID does not match, then UPF marks the N4 call as non-combo and updates FAR. • If SMGR-ID matches and the corresponding Sxa session is not present, then UPF rejects N4 Modification with cause *Mandatory IE Incorrect* and faulty IE *Outer Header Creation*.

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

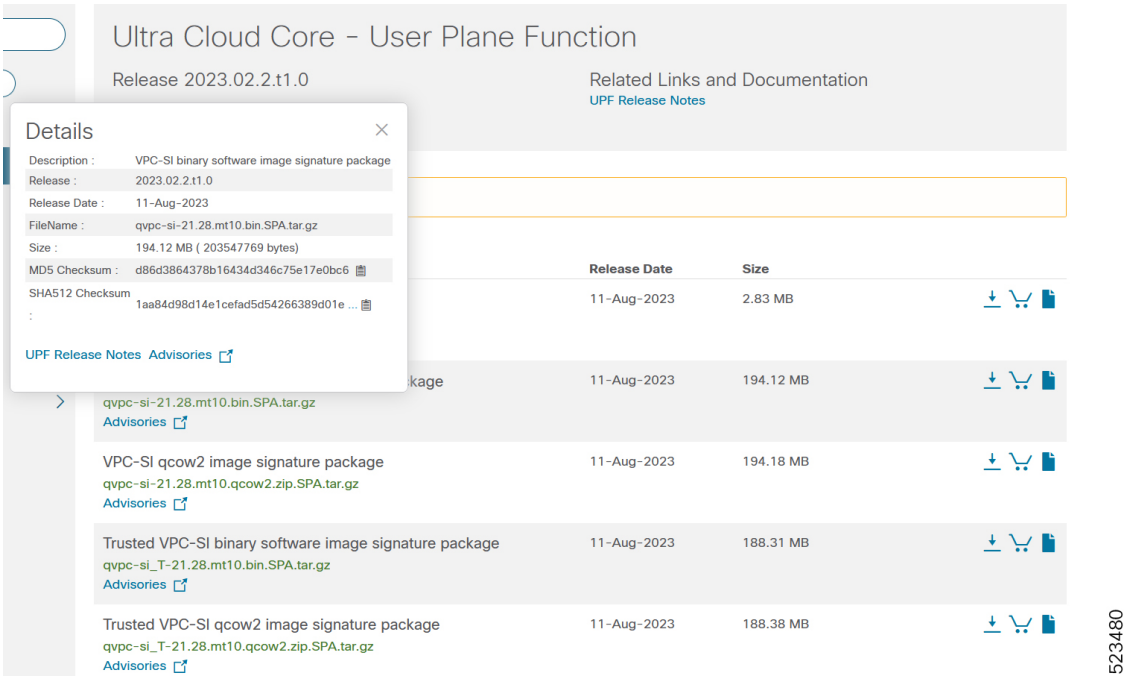
Installation and Upgrade Notes

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, 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**
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*

Operating System	SHA512 checksum calculation command examples
NOTES: *filename* is the name of the file. *extension* 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 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
CSCwf08057	Observed Update FAR not found with FAR ID
CSCwf92160	sessmgr vs vpp state is incorrect on non syn flow during pdn update.
CSCwh02919	4g converged and non converged calls getting drop with echo req/res on MPLS over N9
CSCwh25088	VUPF doesn't update proper counts in show user-plane-service statistics for RA packet
CSCwh51860	Sx peers are in associated state when configured CPGROUP is not associated with user-plane-ser
CSCwh55448	restart seen for the func /pC :libc.so.6/__strlen_sse2_bsf
CSCwh62914	UPF show gtpu statistics peer-address should display bytes and pks for gtpu peer (umbrella Stats)
CSCwh82744	SFW stats incorrectly getting reconciled from VPP to sessmgr
CSCwh83130	Observing unknown disconnect reason when QGR is enabled

Bug ID	Headline
CSCwh84396	Discrepancies in stat counters and disconnect reasons during gtpu path failure
CSCwh93681	Sessmgr restart at function sessmgr_uplane_process_sx_sess_modify_request()
CSCwh94672	Sessmgr crashed with function ld-linux.so.2/_dl_sysinfo_int80()

Resolved Bugs for this Release

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

Bug ID	Headline	Behavior Change
CSCwd08526	sessmgr restarts at sessmgr_uplane_cleanup_clp_data()	Yes
CSCwf12887	Fatal Signal 11: smgr_uplane_rule_compare_icmp_type()	No
CSCwf96687	sm restart observed on stdby HUPF at sessmgr_recover_uplane_pdr_info() post sessmr recovery	Yes
CSCwf99389	Interface type mismatch stat should be under sx service statistics for n4 modify.	Yes
CSCwf99733	TCP Reset packet sent twice on winnuke attack flow terminate as well as idle timeout expiry	No
CSCwh00402	Incorrect error cause when 4g combo call is tried with no sgw service	Yes
CSCwh03798	Sessmgr dropping ICMP fragmented pkts when Firewall is enabled	No
CSCwh09791	"VPP Crash, Segmentation fault after 6 Hours call-Run on Multiple User-Planes"	No
CSCwh12530	Incorrect firewall flooding attack detected	No
CSCwh14297	UPF to have option to ignore OHR IE in Update-Core-PDR in sx-mod-req	No
CSCwh17462	Roaming calls disconnected(V-UPF) due to sx-mand-ie-incorrect	No
CSCwh17947	Seen sessmgr restart at sn_memblock_memcache_alloc()	No
CSCwh22453	sessmgr restart at sessmgr_uplane_process_sx_update_far_update_tep_teid_n4()	Yes
CSCwh27513	RTP Packet drops seen with NAT64 ALG RTSP enabled	No
CSCwh32137	Outer header removal type[1] does not match the configure gtpu endpoint for PDR ID	No

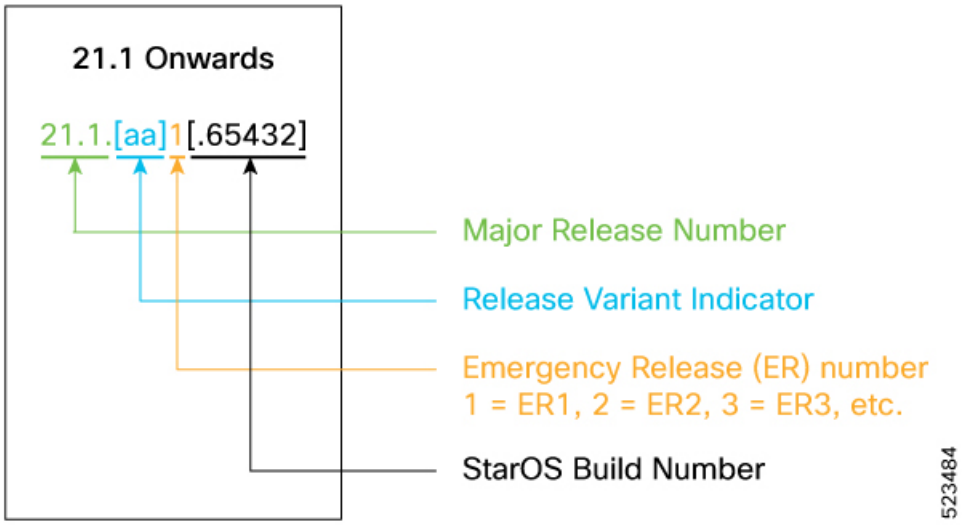
Bug ID	Headline	Behavior Change
CSCwh36214	Rule match stats not updated correctly when Firewall enabled on call and P2P configured	No
CSCwh37366	Flow gets cleared on hitting max port chunk for icmpv6	No
CSCwh38784	Dos Attack stat is not incremented when Firewall attack is been detected at VPP	No
CSCwh62790	Packet with Invalid IP Options length getting detected as Source Router Attack in SFW VPP	No
CSCwh64600	UPF sessmgr recovery calls dropped with reason=sessmgr_audit_do_failure_handling Failed	No
CSCwh66078	show user-plane-service gtpu local-addresses CLI not working after ICSR on newActive	No
CSCwh71108	"UPF PDR allowed non existent loopback ip address for gtpu local-adress, "	No
CSCwh72304	GTPU Echo generated from incorrect address for 5g to 4g homer HO with n3 n9 separation	No
CSCwh72339	sessmgr restart at egtpu_process_update_req_evt() with inter/intra plmn HO calls	No
CSCwh77256	EDR timestamp are not proper for attribute sn-last-downlink-pkt-time & sn-last-uplink-pkt-time	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".

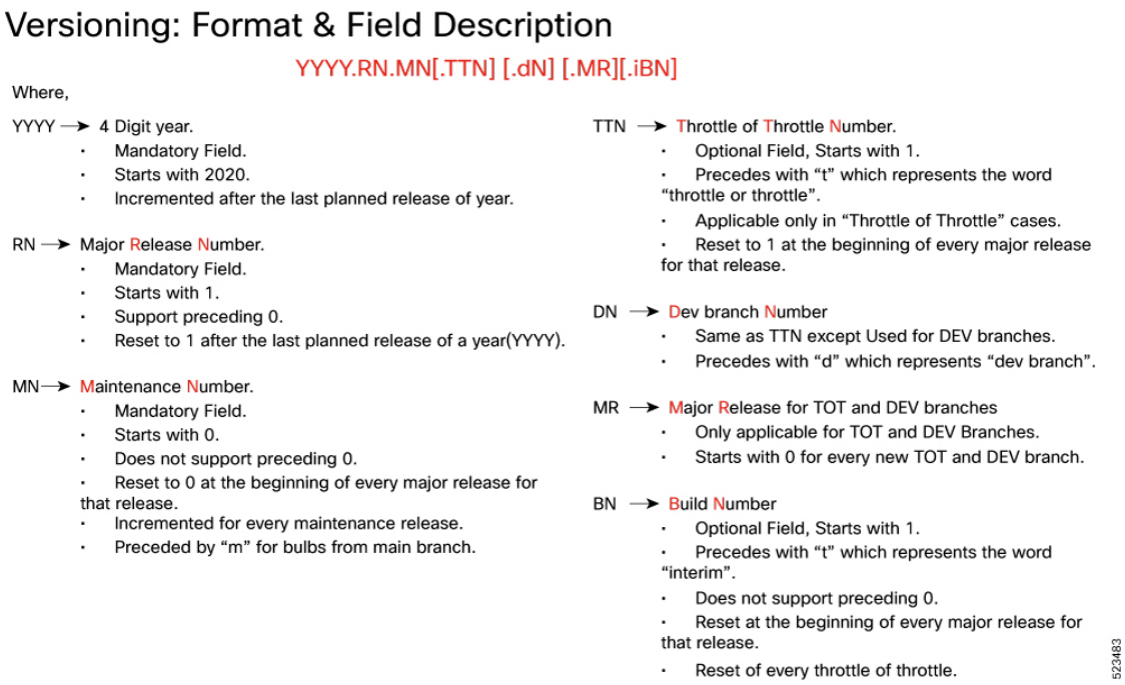


The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research 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 10.

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 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
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.
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.