Release Notes for StarOS™ Software Version 21.14.0 and Ultra Service Platform Version N6.8.0

First Published: June 27, 2019
Last Updated: June 27, 2019

Introduction

This Release Note identifies changes and issues related to this software release. This release is the next major feature release since 21.13.0 and N6.7.0.

Release Package Version Information

Table 1 - Release Package Version Information

Software Packages	Version
StarOS packages	21.14.0 build 72257
Ultra Service Platform ISO	6_8_0-9247
usp-em-bundle*	6.7.0, Epoch 7128
usp-ugp-bundle*	21.14.0, build 72257, Epoch 7102
usp-yang-bundle	1.0.0, Epoch 7093
usp-uas-bundle	6.8.0, Epoch 7162
usp-auto-it-bundle	5.8.0, Epoch 7305
usp-vnfm-bundle	4.5.0.112, Epoch 7094
USP RPM Verification Utilities	6.8.0
* These bundles are also distributed separately from the ISO.	

Descriptions for the various packages provided with this release are located in Table 3.

Feature and Behavior Changes

Refer to the *Release Change Reference* for a complete list of feature and behavior changes associated with this software release.

Related Documentation

For a complete list of documentation available for this release, go to:

- StarOS: https://www.cisco.com/c/en/us/support/wireless/asr-5000-series/products-installation-and-configuration-guides-list.html
- Ultra Gateway Platform (including the UltraM Solution): https://www.cisco.com/c/en/us/support/wireless/ultra-gateway-platform/products-installation-and-configuration-guides-list.html
- Ultra Automation Services: https://www.cisco.com/c/en/us/support/wireless/ultra-automation-services/products-installation-and-configuration-guides-list.html
- Virtual Packet Core (including VPC-SI and VPC-DI): https://www.cisco.com/c/en/us/support/wireless/virtual-packet-core/products-installation-and-configuration-guides-list.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.

Ultra M Hyper-Converged Model Component Version Information

Table 2 - Ultra M Hyper-Converged Model Component Version Information

HW	SW	6.2	6.3	6.4	6.5	6.6	6.7	6.8
	StarOS	69296	69977	70597	70741	71244	71540	72257
	ESC	4.0.0.104	4.2.0.74	4.3.0.121	4.3.0.121	4.4.0.88	4.4.0.88	4.5.0.112
	RH Kernel	7.4	7.5	7.5	7.5	7.5	7.5	7.5
	OSP	10	10	10	10 or 13 **NOTE**: OpenStack Platform 13 with RHEL 7.5 is validated only for standalone AutoVNF-based deployments of the UGP VNF.	10 or 13 **NOTE**: OpenStack Platform 13 with RHEL 7.5 is validated only for standalone AutoVNF-based deployments of the UGP VNF.	10 or 13 **NOTE**: OpenStack Platform 13 with RHEL 7.5 is validated only for standalone AutoVNF-based deployments of the UGP VNF.	10 or 13 **NOTE**: OpenStack Platform 13 with RHEL 7.5 is validated only for standalone AutoVNF-based deployments of the UGP VNF.
UCS C240 M4S	BIOS	3.0(4a)	3.0(4a)	3.0(4a)	3.0(4a)	3.0(4a)	3.0(4a)	3.0(4a)
	CIMC (BMC)	3.0(4a)	3.0(4d)	3.0(4d)	3.0(4d)	3.0(4d)	3.0(4d)	3.0(4d)

HW	SW	6.2	6.3	6.4	6.5	6.6	6.7	6.8
SFF (NFVI)	MLOM	4.1 (3a)	4.1 (3f)	4.1 (3f)	4.1 (3f)	4.1 (3f)	4.1 (3f)	4.1 (3f)
C2960 XR-48TD-I (Management)	Boot Loader	15.2(3r)E1	15.2(3r)E1	15.2(3r)E1	15.2(3r)E1	15.2(3r)E1	15.2(3r)E1	15.2(3r)E1
	IOS	15.2.(2) E5	15.2.(2) E5	15.2.(2) E5	15.2.(2) E5	15.2.(2) E5	15.2.(2) E5	15.2.(2) E5
C3850-48T-S (Management)	Boot Loader	3.58	3.58	3.58	3.58	3.58	3.58	3.58
	IOS	03.06.06E	03.06.06E	03.06.06E	03.06.06E	03.06.06E	03.06.06E	03.06.06E
Nexus 93180-YC-EX (Leafs)	BIOS	7.59	7.59	7.59	7.59	7.59	7.59	7.59
	NX-OS	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)
Nexus 9236C (Spines)	BIOS	7.59	7.59	7.59	7.59	7.59	7.59	7.59
	NX-OS	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)

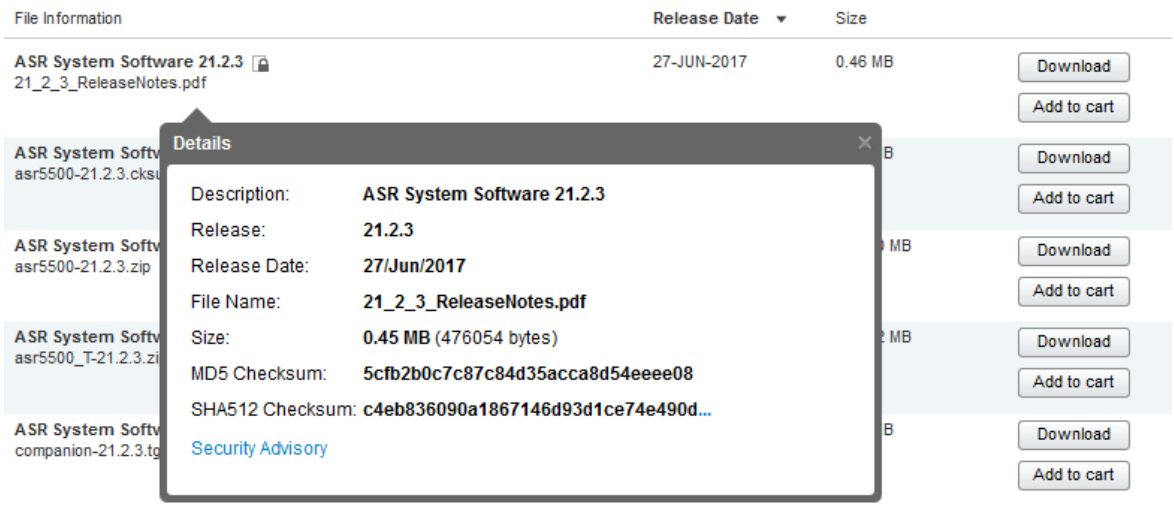
Firmware Updates

There are no firmware upgrades required for this release.

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

To calculate a SHA512 checksum on your local desktop see Table 3.

Table 3 - 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

In 21.12.0 and later releases, software images for StarOS, VPC-DI, and VPC-SI, and the companion software packages for StarOS and VPC are signed via x509 certificates. In pre-21.12.0 releases, image signing is not supported for VPC-DI and VPC-SI images, and for StarOS and VPC companion software packages.

USP ISO images are signed with a GPG key.

For more information and instructions on how to validate the certificates, refer to the README file available with the respective software packages.

Open Bugs in this Release

The following table lists the known bugs that were found in, and remain open in this 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.

Table 4 - Open Bugs in this Release

Bug ID	Headline	Product Found*
CSCvo32007	[PLT-CUPS] CUPS continuous SESSMGR Restarts observed on CP when bringing up static calls	cups-cp
CSCvp13568	sessmgr restart at saegwdrv_ue_fsm_st_active_evt_snx_line_close	cups-cp
CSCvq31677	[BP-CUPS]-SGW CP sends extra SxMODRes every usage Report for time-volume interval	cups-cp
CSCvp36411	[CUPS] sessmgr error log fastpath_row_read()returned error 0x80002001flow action is discard/normal	cups-up
CSCvq06447	[CUPS] VPP Coredumps are not available at the configured coredump file location	cups-up
CSCvp38248	[PLT-CUPS] : issue seen in vpp with signature vpp(sn_assert_signal_handler()	cups-up
CSCvp97678	[BP-CUPS] IPv6 address is getting changed after Sesion recovery / switchover in UP	cups-up
CSCvp43335	"KT EPC: MME, double counting statistics of decor rerouted attach accept"	mme
CSCvp47084	Issue when LTE to WIFI HO take place and CB and UB Response are pending	pdn-gw
CSCvg05683	sessmgr restart - with the function trace of get_rtmp_hdr_len()	pdn-gw
CSCvp06042	[BP-ICUPS] : Sessmgr restarts observed after 8hrs of callmodel @PC: acs_http_pkt_inspection()	pdn-gw
CSCvq25025	[PLT-ICUPS-VPP]: [sessmgr 11956 error] [acsmgr 91432 error] Policer Row add Failed	pdn-gw
CSCvn75072	[BP:ICUPS]:Sessmgr restart@fapi_tp_process_incoming_local_row_req on DPC2 card reboot.	pdn-gw
CSCvq24280	Buffered PCRF messages are not processed when UBResp is received (pending buffer size was 2)	pdn-gw

Bug ID	Headline	Product Found*
CSCvq31798	TODR's not generated for data-record only config with the latest CUTO library integration	pdn-gw
CSCvq31832	IPv6 PMTU discovery does not work and MSS 9040 is chosen by BGP	staros
* Information in the “Product Found” column identifies the product in which the bug was initially identified.		

Resolved Bugs in this Release

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

NOTE: This software release may contain bug fixes first introduced in other releases. Additional information for all resolved bugs for this release are available in the Cisco Bug Search Tool.

Table 5 - Resolved Bugs in this Release

Bug ID	Headline	Product Found*
CSCvm83524	[BP-CUPS] Assert failure at egtpc_handle_user_sap_event()	cups-cp
CSCvo32007	[PLT-CUPS] CUPS continuous SESSMGR Restarts observed on CP when bringing up static calls	cups-cp
CSCvp02150	[BP-CUPS] Disconnect reason with “Unknown”	cups-cp
CSCvp13568	sessmgr restart at saegwdrv_ue_fsm_st_active_evt_snx_line_close	cups-cp
CSCvp77946	[BP-CUPS] Single call getting dropped after recovery in Pure-p	cups-cp
CSCvk17716	[BP-CUPS] On UBRes failure for Dynamic rule modification URRs getting removed for default Bearer	cups-cp
CSCvo22255	[BP-CUPS] Assert failure at sessmgr_pgw_send_delete_bearer_to_driver()	cups-cp
CSCvo25753	sm restart observed in UP with make break calls in the background	cups-cp
CSCvo48919	"[BP-CUPS]: CREATE FAR not sent, when rule installed in 2nd SX_MODIFY, after 1st SX_MODIFY failure"	cups-cp
CSCvo75761	[CUPS] sessmgr crash PC: [05d3fd87/X] sgwdrv_handle_dsr_sx_term_rsp()	cups-cp
CSCvo75771	[CUPS] Sessmgr crash Assertion failure at sess/egtp/egtpc/egtpc_interface.c:256	cups-cp
CSCvo80112	[PLT-CUPS]New chunk allocation to UPs not happening after pool context vpnmgr recovery	cups-cp
CSCvq01585	volte audio was dropped after ICSR due to CP is responding no content found in Sx_session_update	cups-cp
CSCvq06898	"[BP-CUPS]- multiPDN IDFT, extra SXModReq for PDN which is not requested for IDFT"	cups-cp
CSCvm59761	[PLT-CUPS-VPP]IPv6 fragmentation issue	cups-up

Bug ID	Headline	Product Found*
CSCvp36411	[CUPS] sessmgr error log fastpath_row_read()returned error 0x80002001flow action is discard/normal	cups-up
CSCvp78287	[PLT-CUPS-VPP]: Some particular SSL based sites and APP not working with specific handset	cups-up
CSCvq06447	[CUPS] VPP Coredumps are not available at the configured coredump file location	cups-up
CSCvq06683	[KT-CUPS] User Plane Inactivity Report received before the timer expiry	cups-up
CSCvq14110	[BP-CUPS]: Fullcores are not getting generated on UP with redundancy enabled.	cups-up
CSCvn14097	[BP-CUPS] Access Type of Pure-S call is displayed as 'Unknown'	cups-up
CSCvo48870	[PLT-CUPS]Calls are not coming up after adding new UP when new UP doesn't get any chunks	cups-up
CSCvp97678	[BP-CUPS] IPv6 address is getting changed after Sesion recovery / switchover in UP	cups-up
CSCvp98220	UL pkts coming up even if stream is in active state due to TEID-mismatch after session recovery	cups-up
CSCvq07042	[CUPS] Reclassification for rule matching isn't happening after TEID change	cups-up
CSCvj58241	MME does not respond to PLR if IMSI is unknown (no mapping information found)	mme
CSCvk58720	Handover rejected (S10 HO) - After congestion is cleared	mme
CSCvo88008	"MME, Collision Case - E-RAB Mod for NR addition & CBReq for VoLTE termination call attempt"	mme
CSCvp22149	"KT EPC: MME, Inter-TAU or S1 HO - EGTP_CAUSE_MANDATORY_IE_INCORRECT from new MME"	mme
CSCvp43902	KT-EPC MME; GBR bearer preservation by Inter-RAT redirection cause in UE context release	mme
CSCvp49268	KT-EPC MME; S1 H/O MME status transfer apply specific IE Criticality	mme
CSCvm97400	Assert at mme_app_fill_s1_bearer_values	mme
CSCvn79786	MME sessmgr restart egtpc_handle_ps_to_cs_cancel_notf_evt	mme
CSCvo13661	cc overwrite apn remap is case sensitive	mme
CSCvo22843	Paging edrx h-sfn should be a 10 bits counter	mme
CSCvo33689	inter-rat-nnsf mme-codes parameter missing after reload	mme
CSCvo57948	Very inbalanced sessmgr distribution after enabling “sgsn-mme subscriber-data-optimization”	mme
CSCvp76784	"MME does not take into account NOTE 5 of 3GPP 24.008, Table 10.5.5.32 Extended DRX parameters"	mme

Bug ID	Headline	Product Found*
CSCvp91571	show hss-peer-service statistics all CLI gives unexpected value for R request/R Answer counters	mme
CSCvp98353	"KT EPC: CLI, “ddn-delay” is not applied after staros rebooting"	mme
CSCvn09785	sessmgr restart after modify ECS configuration	pdn-gw
CSCvo85261	[BP-ICUPS]:sessmgr restart observed at acsmgr_fp_handle_stream_state_change()	pdn-gw
CSCvp15648	[BP-ICUPS] Fatal Signal 11: SF PC: [f6540a68/X] <unknown>()	pdn-gw
CSCvp31063	Modify bearer request getting rejected due to IMEI check while using IMS APN	pdn-gw
CSCvp35767	SRP connection fluctuations and continuous restart of Orbs task	pdn-gw
CSCvp47084	Issue when LTE to WIFI HO take place and CB and UB Response are pending	pdn-gw
CSCvp80850	sessmgr restart at tftcpsendpacket()	pdn-gw
CSCvq00562	[VPC-DI] Demux IPv6 TCP large packet handling broken.	pdn-gw
CSCvn27653	IP source violation should support L2TP allocated IP + Framed route combinations	pdn-gw
CSCvn33912	PGW sends Update Bearer Request with unknown filters in TFT	pdn-gw
CSCvn97839	Threshold process goes into warn state because of memory	pdn-gw
CSCvo20908	[PLT-ICUPS-VPP]:VPP Main in memory over state	pdn-gw
CSCvo22218	[BP:ICUPS]:VPP restart at vnet_per_buffer_interface_output_avx2() on call model run	pdn-gw
CSCvo25833	SM fail due to Segmentation fault on snx_pgw_driver_recreate_pdn	pdn-gw
CSCvo33361	"[BP-ICUPS] For IPv4v6 dual PDP call, dual VRF context support needs to be added."	pdn-gw
CSCvo93783	[BP-ICUPS]: bunch of fastpath_stream_add and fastpath_stream_modify error	pdn-gw
CSCvo93796	[PLT-ICUPS]: multiple error logs for ROW_MODIFY failed	pdn-gw
CSCvo93860	BP-ICUPS: ipsecmgr in warn state for HS LI with ipsec	pdn-gw
CSCvp01726	[PLT-ICUPS] Fragmented downlink packets not intercepted properly	pdn-gw
CSCvp05331	[BP-ICUPS] PGWCDR is not generated with dynamic DDL config	pdn-gw
CSCvp08341	[BP-ICUPS]:Sessmgr restart at PC: [0996e027/X] acsmgr_fp_populate_chrg_buckets()	pdn-gw
CSCvp08691	[BP-ICUPS]:Sessmgr restarted at PC: [09ac3773/X] acsmgr_match_rule_after_cf()	pdn-gw
CSCvp08733	[BP-ICUPS] sessmgr 12332 error Bearer Id 255 is not Valid	pdn-gw
CSCvp11723	BP-ICUPS: All crypto maps lost post demux card migration	pdn-gw

Bug ID	Headline	Product Found*
CSCvp31540	[BP-ICUPS]: sessmgr assert on 21.13.1 FCS smgr_fp_handle_bearer_stream_external_event()	pdn-gw
CSCvp32975	PCC provisioned dynamic rule not enforced when FAPA/TRM activated	pdn-gw
CSCvp40883	[BP-ICUPS]: Session manager reload is observed for multi-PDN call	pdn-gw
CSCvp50493	Memory leak in CLI show active-charging credit-control statistics	pdn-gw
CSCvp55575	GTPU end marker packet forwarded on fast path leads to buffer corruption and KPI drop	pdn-gw
CSCvp75218	"[PLT-ICUPS]: HSLI issue: Li Server sent FIN,ACKs sent to the PGW but the connection never goes down"	pdn-gw
CSCvp83881	PGW CDR is missing byte count in uplink direction during big file transfer due to low Gy quotas	pdn-gw
CSCvp86524	[PLT-ICUPS]: HSLI: TCP LI connection never goes down (no UDP LI) debug instrumentation only	pdn-gw
CSCvp88862	[PLT-ICUPS]: HSLI issue: connection never goes down when UDP and TCP LI runs on same demux cpu	pdn-gw
CSCvq05427	High Speed LI support on ASR5500: TCP RST debug instrumentation + TCP timeout	pdn-gw
CSCvm71645	Task restart while processing the ipsec packet	pdn-gw
CSCvo09517	VPP related logs appear during DPC migration even if VPP function is disabled.	pdn-gw
CSCvo17281	aaamgr memory leak due to checkpointing	pdn-gw
CSCvo66133	Sessmgr restart in Mon-key installation path	pdn-gw
CSCvo66706	[PLT-ICUPS]vpp restart for pcap generation with panopticon in vec_resize_allocate_memory for ASR5500	pdn-gw
CSCvo99003	[ICUPS] High CPU observed with mon sub is enabled for a subscriber.	pdn-gw
CSCvp13958	"[BP-ICUPS] : sessmgr 0 error Timeout Processing: Time out, MSG ID:83773,wheel Slot Id:2951,cmd: 15"	pdn-gw
CSCvp61256	CCR-U with Requested-Service-Unit sent by PGW to OCS for blacklisted MSCC on traffic match	pdn-gw
CSCvo10110	Additional debug info required in syslog when CCR update not sent during handover	pdn-gw
CSCvp03633	'Accounting-Request' counter is not getting pegged if response from RADIUS server is missing	pdn-gw
CSCvo36105	[BP-ICUPS]: acsmgr 91369 error Error: Client-Server API: Add conneciton request to Dhost failed	sae-gw
CSCvo45264	[BP-ICUPS]: Data is not proper for 5G UE of ipv6 pdntype	sae-gw
CSCvo64893	[saegw-gn] LI interception of calltype saegw does not intercept 2G/3G calls	sae-gw

Bug ID	Headline	Product Found*
CSCvo82068	[BP-ICUPS]: 4G sub with NAT44 fragmented traffic NOT getting charged to Dynamic rule	sae-gw
CSCvo89516	[BP-ICUPS] CDR is not correct for uplink packets when 3 pipelined get requests are there.	sae-gw
CSCvo98432	[PLT-ICUPS-VPP]: VPP Logs - Continously seen - vm_alloc_shm_rw / vpp_vec_alloc_shm	sae-gw
CSCvo98718	[ICUPS]'Unknown' session disc-reasons incremented after DSReq received instead of MBreq in multipdn	sae-gw
CSCvp00476	[BP-ICUPS]:sessmgr restart acs_http_update_accel_hss() / acs_http_update_inline_fp_accel_info_pkt()	sae-gw
CSCvp09529	Cisco SGW restart observed in case of HLCOM related IEs in DDN ack from MME	sae-gw
CSCvp10742	[BP-ICUPS] ITC uplink traffic is not getting throttled	sae-gw
CSCvp11137	[BP-ICUPS] smp-fp-brr-stream-oper-failure and smp-fp-strm-chrg-oper-failure pegging in 21.13.1	sae-gw
CSCvp22175	[BP-ICUPS] HS-LI-UDP:Call type need to be PGW for SAE-GW service-type in LI header	sae-gw
CSCvp25635	[BP-ICUPS] smp-fp-strm-chrg-oper-failure pegging in 21.13.1.71625 session disconnect-reasons	sae-gw
CSCvp25641	[BP-ICUPS] smp-fp-tep-oper-failure pegging in 21.13.1.71625 session disconnect-reasons	sae-gw
CSCvp32124	[BP-ICUPS] Seg. faults at acs_process_transactn() after 24hrs of call model run.	sae-gw
CSCvp54598	[BP-ICUPS]: Config does not survive chassis reload Enable HS CALEA FOA for 5G NR	sae-gw
CSCvo47301	[BP-ICUPS]Quota_Exhaust not triggered for pipelined request packet	sae-gw
CSCvo85755	[PLT-ICUPS] HS-LI-UDP: Uplink packets are not getting intercepted	sae-gw
CSCvo95499	[BP-ICUPS] 21.13.M0 starent.my returns a compilation error for severity2 `starTrapGroup'	sae-gw
CSCvp28704	[BP-ICUPS] Unable to decode most PGWCDRs on 21.13.x with WLAN due to incorrect tag[253] generated	sae-gw
CSCvp49907	[ICUPS]Fatal Signal 11: Segmentation fault acs_http_update_accel_info_pkt	sae-gw
CSCvp61777	Sessmgr restart in DCCA path for buffered packet processing	sae-gw
CSCvp71773	Cisco SGW restart observed when Delete Session Req received during IDFT for collapsed call	sae-gw
CSCvk43515	Assertion failure at sm_rab_mgmt	sgsn

Bug ID	Headline	Product Found*
CSCvk45571	sessmgr restart function: sessmgr_gprs_process_sub_session_idle()	sgsn
CSCvj51716	Task restart on modify bearer request	sgsn
CSCvj89699	sessmgr Assertion failure in pmm_ms_fsm_invalid_event_handler	sgsn
CSCvk05536	SM fail due to Assertion failure on egtpc_handle_update_bearer_rsp_evt	sgsn
CSCvm93457	Assertion failure in Function: egtpc_handle_create_sess_rsp_msg	sgsn
CSCvn77932	SGSN EDR header does not have EOL character	sgsn
CSCvn78512	Session manager restarted Fatal Signal 6: Aborted	sgsn
CSCvo04661	sessmgr restart- Assertion failure	sgsn
CSCvo55588	Session Manager assert during S4 SRNS	sgsn
CSCvo58153	SM fail due to Assertion failure at sessmgr_gprs_process_del_sub_session	sgsn
CSCvo60264	sessmgr: DATACORRUPTION-AVERTED: Attempt to strncat 3 bytes limited to 10 bytes	sgsn
CSCvo64397	Invalid Event NTWK-MODIFY-REQUEST from SM-APP in NTWK-REMOTE-HANDOFF-IN-PROGRESS-IN-INACTIVE state	sgsn
CSCvo65976	Rcvd Invalid Event NTWK-INTRA-SGSN-HANDOFF-REQUEST from SM-APP in NTWK-INTER-SGSN-RAU-BEGIN state	sgsn
CSCvo94363	Headers needs to be updated for the new fields added as part of EDR Enhancement	sgsn
CSCvp09454	session manager restart due to RABassign request	sgsn
CSCvo83261	sessmgr assertion: Rcvd Invalid Event NTWK-HANDOFF-CANCEL from SM-APP in NTWK-SUSPENDED state	sgsn
CSCvp31789	sessmgr restarted related to GnGp (GGSN 2 PGW) HO	sgw
CSCvo00288	Cisco SGW Restart observed on Standby ICSR chassis	sgw
CSCvp10744	[BP-ICUPS] SGW CDR shows double value in dataVolumeGPRSDownlink for buffered data after Re-establish	sgw
CSCvm93753	MIB Syntax Errors in 21.8.1 (69429) and 21.9.1 (70183)	staros
CSCvo35624	new unexpected diamproxy instance spawned	staros
CSCvo70530	SAEGW-VPC-DI- Sw Version 21.12.0 - MTU higher than Default value not working correctly	staros
CSCvp06026	VPC-DI NAT keepalive packets should be dropped.	staros
CSCvp14022	[PLT-CUPS-ICUPS-VPP] OsShellAccessed SNMP traps coming from SDR collection	staros
CSCvm96218	"ASR5K device sends wrong objects for the traps with ifIndex 1343, 1344, 1345, 1346."	staros

Bug ID	Headline	Product Found*
CSCvn82817	[VPP] Automatic recovery of failed card/VM after VPP core complete	staros
CSCvo29918	Wrong echo-max-retransmissions value when not explicitly configured	staros
CSCvp47435	ipv4 reassembly timeout - vpp restart	staros
CSCvp82910	cli that shows local origin state id on the node	staros
CSCvo84219	multi-vnfd generation fails when using different pools of same net	usp-uas
CSCvo95462	Same virtual_router_id for all UEM deployments	usp-uas
* Information in the "Product Found" column identifies the product in which the bug was initially identified.		

Operator Notes

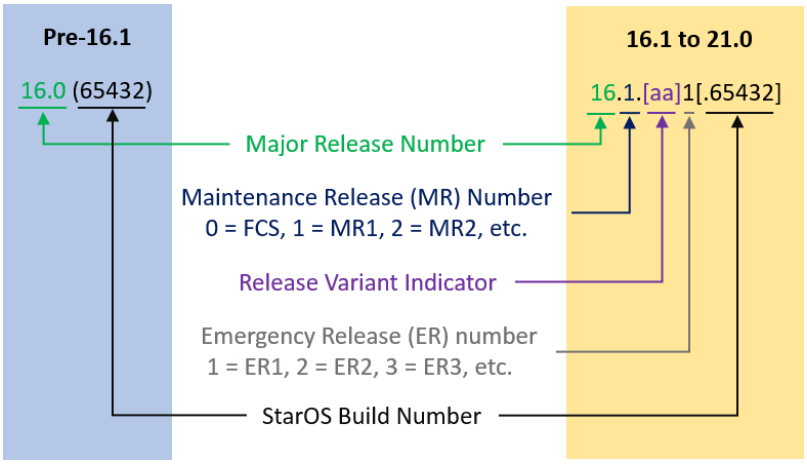
StarOS Version Numbering System

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.

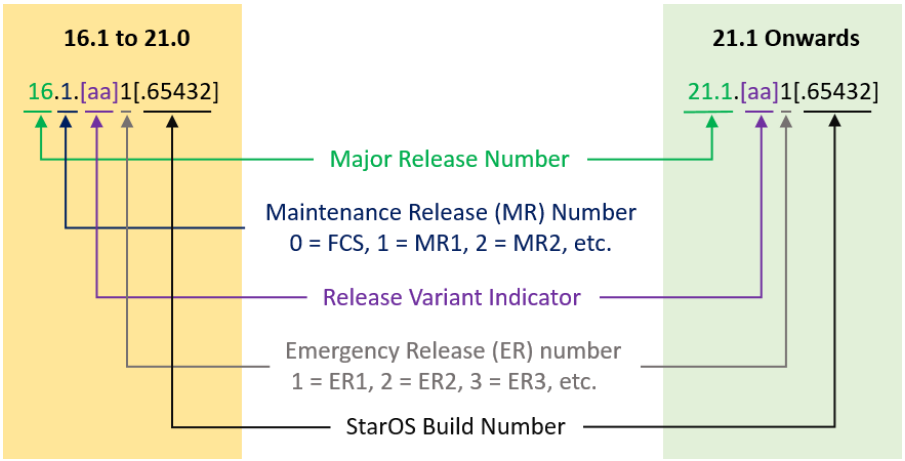
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build number.

From release 16.1 onwards, the output of the **show version** command, as well as the terminology used to describe the Build Version Number fields, has changed. Additionally, **show version** will display slightly different information depending on whether or not a build is suitable for deployment.

The Version Build Number for releases between 16.1 and 21.0 include a major, maintenance, and emergency release number, for example "16.1.2".



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



In either scenario, 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 will facilitate identifying the changes between releases when using Bug Search Tool to research software releases.

Release Package Descriptions

Table 6 provides descriptions for the packages that are available with this release.

Table 6 - Release Package Information

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
ASR 5500		
asr5500-<release>.zip	asr5500-<release>.bin	Contains the signed ASR 5500 software image, the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
asr5500_T-<release>.zip	asr5500_T-<release>.bin	Contains the signed, trusted ASR 5500 software image, the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
StarOS Companion Package		
companion-<release>.zip	companion-<release>.tgz	Contains numerous files pertaining to this version of the StarOS including SNMP MIBs, RADIUS dictionaries, ORBEM clients. These files pertain to both trusted and non-trusted build variants. In 21.12.0 and later releases, the StarOS companion package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
VPC-DI		

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qvpc-di-<release>.bin.zip	qvpc-di-<release>.bin	Contains the VPC-DI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di_T-<release>.bin.zip	qvpc-di_T-<release>.bin	Contains the trusted VPC-DI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di-<release>.iso.zip	qvpc-di-<release>.iso	Contains the VPC-DI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di_T-<release>.iso.zip	qvpc-di_T-<release>.iso	Contains the trusted VPC-DI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di-template-vmware-<release>.zip	qvpc-di-template-vmware-<release>.tgz	Contains the VPC-DI binary software image that is used to on-board the software directly into VMware. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di-template-vmware_T-<release>.zip	qvpc-di-template-vmware_T-<release>.tgz	Contains the trusted VPC-DI binary software image that is used to on-board the software directly into VMware. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qvpc-di-template-libvirt-kvm-<release>.zip	qvpc-di-template-libvirt-kvm-<release>.tgz	Contains the same VPC-DI ISO identified above and additional installation files for using it on KVM. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di-template-libvirt-kvm_T-<release>.zip	qvpc-di-template-libvirt-kvm_T-<release>.tgz	Contains the same trusted VPC-DI ISO identified above and additional installation files for using it on KVM. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di-<release>.qcow2.zip	qvpc-di-<release>.qcow2.tgz	Contains the VPC-DI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di_T-<release>.qcow2.zip	qvpc-di_T-<release>.qcow2.tgz	Contains the trusted VPC-DI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
VPC-SI		
qvpc-si-<release>.bin.zip	qvpc-si-<release>.bin	Contains the VPC-SI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si_T-<release>.bin.zip	qvpc-si_T-<release>.bin	Contains the trusted VPC-SI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qvpc-si-<release>.iso.zip	qvpc-si-<release>.iso	Contains the VPC-SI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si_T-<release>.iso.zip	qvpc-si_T-<release>.iso	Contains the trusted VPC-SI ISO used for new deployments a new virtual machine is manually created and configured to boot from a CD image. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-template-vmware-<release>.zip	qvpc-si-template-vmware-<release>.ova	Contains the VPC-SI binary software image that is used to on-board the software directly into VMware. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-template-vmware_T-<release>.zip	qvpc-si-template-vmware_T-<release>.ova	Contains the trusted VPC-SI binary software image that is used to on-board the software directly into VMware. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-template-libvirt-kvm-<release>.zip	qvpc-si-template-libvirt-kvm-<release>.tgz	Contains the same VPC-SI ISO identified above and additional installation files for using it on KVM. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-template-libvirt-kvm_T-<release>.zip	qvpc-si-template-libvirt-kvm_T-<release>.tgz	Contains the same trusted VPC-SI ISO identified above and additional installation files for using it on KVM. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qvpc-si-<release>.qcow2.zip	qvpc-si-<release>.qcow2.gz	Contains the VPC-SI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si_T-<release>.qcow2.zip	qvpc-si_T-<release>.qcow2.gz	Contains the trusted VPC-SI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
VPC Companion Package		
companion-vpc-<release>.zip	companion-vpc-<release>.tgz	Contains numerous files pertaining to this version of the VPC including SNMP MIBs, RADIUS dictionaries, ORBEM clients. These files pertain to both VPC-DI and VPC-SI, and for trusted and non-trusted build variants. In 21.12.0 and later releases, the VPC companion package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
Ultra Service Platform		
usp-<version>.iso		The USP software package containing component RPMs (bundles). Refer to Table 7 for descriptions of the specific bundles.
usp_T-<version>.iso		The USP software package containing component RPMs (bundles). This bundle contains trusted images. Refer to Table 7 for descriptions of the specific bundles.
usp_rpm_verify_utils-<version>.tar		Contains information and utilities for verifying USP RPM integrity.

Table 7 - USP ISO Bundles

USP Bundle Name	Description
usp-em-bundle-<version>-1.x86_64.rpm*	The Element Manager (EM) Bundle RPM containing images and metadata for the Ultra Element Manager (UEM) module.
usp-ugp-bundle-<version>-1.x86_64.rpm*	The Ultra Gateway Platform (UGP) Bundle RPM containing images for Ultra Packet core (VPC-DI). There are trusted and non-trusted image variants of this bundle.

usp-yang-bundle-<version>-1.x86_64.rpm	The Yang Bundle RPM containing YANG data models including the VNFD and VNFR.
usp-uas-bundle-<version>-1.x86_64.rpm	The Ultra Automation Services Bundle RPM containing AutoVNF, Ultra Web Services (UWS), and other automation packages.
usp-auto-it-bundle-<version>-1.x86_64.rpm	The bundle containing the AutoIT packages required to deploy the UAS.
usp-vnfm-bundle-<version>-1.x86_64.rpm	The VNFM Bundle RPM containing an image and a boot-up script for ESC (Elastic Service Controller).
ultram-manager-<version>-1.x86_64.rpm*	This package contains the script and relevant files needed to deploy the Ultra M Manager Service.
* These bundles are also distributed separately from the ISO.	

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, see *What's New in Cisco Product Documentation*, at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

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 ANY KIND, 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 WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR 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: 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)

© 2019 Cisco Systems, Inc. All rights reserved.