Release Notes for StarOS™ Software Version 21.28.h1

First Published: May 11, 2023
Last Updated: May 11, 2023

Introduction

This Release Note identifies changes and issues related to this software release. This release is the next major feature release since 21.28.h0. This release note is specific to CUPS User Plane only.

Release Package Version Information

Table 1 - Release Package Version Information

Software Packages	Version
StarOS packages	21.28.h1, build 89884

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 http://www.cisco.com/c/en/us/support/wireless/asr-5000-series/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.

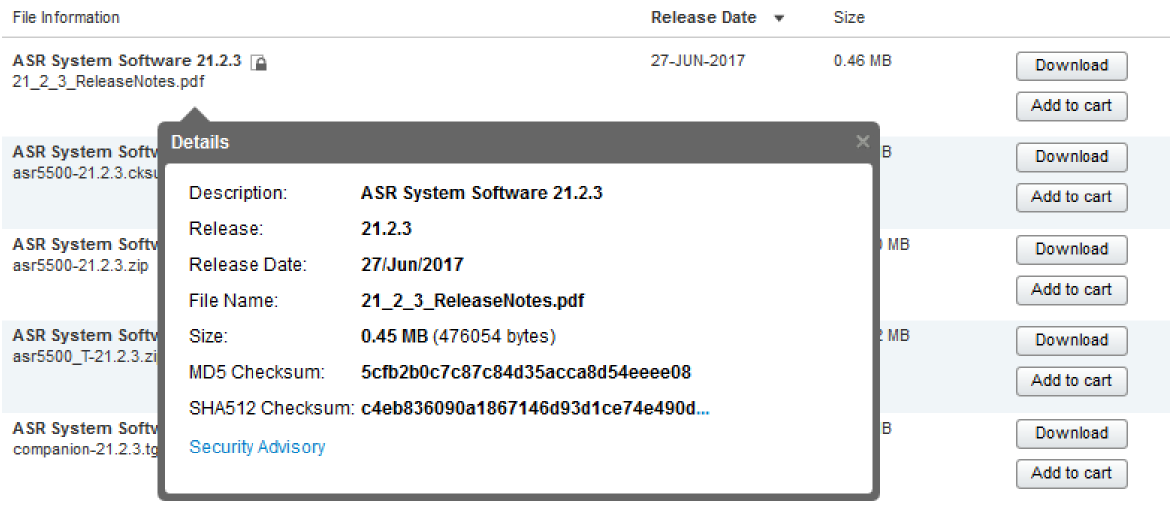
Firmware Updates

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.



File Information | Release Date | Size

ASR System Software 21.2.3
21_2_3_ReleaseNotes.pdf | 27-JUN-2017 | 0.46 MB

ASR System Softw
asr5500-21.2.3.cksu

ASR System Softw
asr5500-21.2.3.zip

ASR System Softw
asr5500_T-21.2.3.zi

ASR System Softw
companion-21.2.3.tg

Details

Description: ASR System Software 21.2.3
Release: 21.2.3
Release Date: 27/Jun/2017
File Name: 21_2_3_ReleaseNotes.pdf
Size: 0.45 MB (476054 bytes)
MD5 Checksum: 5cfb2b0c7c87c84d35acca8d54eeee08
SHA512 Checksum: c4eb836090a1867146d93d1ce74e490d...
Security Advisory

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 2 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 2.

Table 2 - 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 3 - Open Bugs in this Release

Bug ID	Headline	Product Found*
CSCwc34754	Active call got disconnected during handoff from 4G to wifi on ICSR setup with Gx-Alias enabled.	cups-cp
CSCwe39584	Discrepancy in hermes behaviour during QoS update of 3G call	cups-cp
CSCwe91396	Duplicate TEP removal by CP.	cups-cp
CSCwf25021	sessmgr crash at acsmgr_activate_predef_rule_or_group()	cups-cp
CSCwe94671	[CUPS-CP]CP not sending Used-Service-Unit in CCRT-GY message after clearing call	cups-cp
CSCwd99519	[UPF-ST] Error logs seen on UPF PDR not found with PDR ID 0x149 and Remove PDR PDR with ID 0x2ce	cups-cp
CSCwf26675	[BP-CUPS] Abnormal Release record closure for 3g call with custom38 disctionary	cups-cp
CSCwd19379	[BP-CUPS] call drops on sessmgr task kill - recover_sgx_from_crr failed	cups-cp
CSCwe08636	[BP-CUPS] Dynamic rule is not getting installed with no policy-control update-default-bearer	cups-cp
CSCwf01589	[CUPS-UP]UP send SX_mod_resp with PFCP_CAUSE_MANDATORY_IE_INCORRECT while doing handover	cups-cp
CSCwf14306	"F138422: Show Subscribers cli with UUT, CC and UPG values displays no subs in multi-pdn pure-s call"	cups-cp
CSCwf24872	"[BP-CUPS]After sxdemux card migration,fresh ip pool chunks not pushed & existing pools got depleted"	cups-cp
CSCwf26822	push config-to-up all takes longer than 5mins to finish	cups-cp
CSCwe86265	Behavior of command documentation in CUPS-CP User Guide	cups-cp
CSCwe97010	[CUPS-CP] mismateched in show ip pool summary stats	cups-cp
CSCwd27672	[BP-CUPS]:Assertion failure at Function: sn_memblock_memcache_alloc()	cups-cp
CSCwf15212	[BP-CUPS] egtp echo request not making it out of the CP	cups-cp

Bug ID	Headline	Product Found*
CSCwc29508	[BP-CUPS][sessmgr 12341 error][essmgr_uplane.c:36574][SXAB] UE IP Address is different in Traffic	cups-up
CSCvu76574	[BP-CUPS] recovery-invalid-crr-clp-uplane-gtpu-session checkpoint error	cups-up
CSCwf09429	VPP NSH Fastpath Tables Not Initialized	cups-up
CSCwe97231	[CUPS-UP]: Field missing in cli "show subscribers user-plane-only callid <;call-id> flows full"	cups-up
CSCwf20606	[cups-up][21.28.m7.89804] Assertion failure at sess/smgr/sessmgr_audit_utils.c:15456	cups-up
CSCwc73243	[BP-CUPS] Assertion failure at sess/sctrl/sessctrl_uplane_cfg_sync.c:23721	cups-up
CSCwf03289	[CUPS-UP]UP not sending correct Uplink Volume in SX_SESSION_REPORT_REQUEST	cups-up
CSCwf01800	[CUPS-UP]Stats mismatch rulebase change during HO with only predef rule	cups-up
CSCwb83398	[BP-CUPS] Lots of error logs GTPU Recover Session Failed for GTP-u Peer on standby UP	cups-up
CSCwd72712	[CUPS UP] gtpumgr shows memory warn in standby UP	cups-up
CSCwe73462	[BP-CUPS][sessmgr 10396 error]smgr_recovery.c:13989]Sessmgr-10Recover call from CRR failed post SR	cups-up
CSCwe51492	Sessmgr crash with function :: uplane_create_app_data_flow on Data UPs	cups-up
CSCwf13605	ipsecdemux crash on asr5500 during crypto call model longevity	epdg
CSCwf18184	Multiple Ipsecmgr's are in warn state in 21.28.m3 build	epdg
CSCwf13612	asr500: ipsecdemux crash ipsecdemux_deallocate_session_entry() during chip hang longevity	epdg
CSCwc65963	sessmgr restart is seen when configuring and unconfiguring Lawful intercept CLIs multiple times	mme
CSCwd29108	[NSO-MOB-FP] error with nfv-vim package with NSO 5.7.6.2 or 5.8.4 or 5.6.8 and MFP 3.4	nso-mob-fp
CSCwe45652	PGW is not triggering UBR after RAR from PCRF for IP Filter Replace	pdn-gw
CSCwc53741	Checkpointed information lost after checkpointmgr pod restart	rcm
CSCwe62325	Ubuntu 16.04 ESM/18.04LTS/20.04LTS/22.04LTS/22.10 : systemd vulnerability seen in RCM VM Nessus Scan	rcm
CSCwd91543	IKE notify packets are not responded after pod reload	rcm
CSCwf04371	sessmgr restart at acsmgr_clp_send_checkpoint_dcca	sae-gw
CSCwf15441	egtpegmgr restart seen on SPGW after recent SW upgrade.	sae-gw
CSCwc67766	[UPF_SVI] N4 Session Report request is getting assigned wrong peer IP addr ::ffff:192.10.25.23	smf
CSCwf12837	[UPF-ST]: 5g-wlan HO failing due to remove pdr	smf
CSCwf01246	[UPF-ST] : Sessmgr error logs "[N4] UE IP Address is different in PDR with PDR ID "	smf

Bug ID	Headline	Product Found*
CSCwf13514	[UPF-ST] SessoinModReq failure with FAR already present with FAR ID " Mandatory IE incorrect"	smf
CSCwd51484	Apache Tomcat 9.0.0-M1 Req Smuggling and Azul Zulu java (2022-10-18) Mulitple Vulnerabilities	smi
CSCwe79529	opscenter 2 container are crashing (confd & confd-notifications)	smi
CSCwd81548	[5GaaS] Edge proxy NFs rely on NF restarts to apply config changes	smi
CSCwe51959	v21.28.mx as the upstream branch :: RHEL-8 Build Issues fix in downstream Dev Branch v21.28.ZVx	staros
CSCwe88330	[UPF-SVI] Continuous error logs on vpnmgr - RTNETLINK socket recv buffer under on hermes	upf
CSCwf00180	[UPF-SVI] : Seen Error logs "[CDR 1966 - URR ID -2147435417]" with ICSR SW	upf
CSCwf15247	[ST-UPF] hold queue cli getting configured but not persistent on UPF	upf
CSCwf20862	[UPF-ST] p2p plugin not loaded correctly after upf reload	upf
CSCwd35335	SFR: UPF not able to send trafic on E810 100Gbps links	upf
CSCwf21120	[UPF-ST] gtpumgr going to warn/over state with high memory usage	upf
CSCwd60981	[UPF] UPF does not initiate Sx_Session_Report_Req after receiving GTP_ERROR_IND_MSG	upf
CSCwf08057	[UPF-SVI] : Seen Update FAR not found with FAR ID 0x11e with RCM planned/Unplanned SW	upf
CSCwe33291	[UPF-SVI]: Continuous error logs on standby UPF "SMGR ID mismatch during recovery"	upf
CSCwe92004	No user-plane traffic after 4G (eNB in IPv4) to 5G (gNB in IPv6) mobility in idle mode	upf
CSCwf20631	[UPF-ST]: LI intercept for combo/Pure S call is not maintained post ICSR/N:M RCM SWO	upf
CSCwe74774	[UPF-MONSUB]Sx status report is not sent for 4G/Wifi calls.	upf
CSCwf14455	[UPF-ST] : sessmgr restarted at smgr_is_proto_enabled_for_callid_cups()	upf
***** 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 were found in, and remain open in this 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 4 - Open Bugs in this Release

Bug ID	Headline	Product Found*
CSCwc84548	[CUPS-CP] [ICSR] SRP Standby CP sending Sx Session Delete Request which is not expected	cups-cp
CSCwc88588	"CUPS-CP - After quota holding timer expiry, CP doesn't invoke Gy"	cups-cp
CSCwd14939	[CUPS-CP] Incorrect duration for time limit triggered CDRs after configuration change	cups-cp

Bug ID	Headline	Product Found*
CSCwd44023	SGW incorrectly handling collision between MBR & CBR during N26 handover	cups-cp
CSCwe48599	Sessmgr assertion failure in egtpc_handle_csfb_suspend_notf_evt function.	cups-cp
CSCwe54888	CDR with data volume greater than configured threshold volume	cups-cp
CSCwd29916	IP Pool-ID changes after reload - causing call recovery failures in CP ICSR setup	cups-cp
CSCwd66766	cli display shows contradictory information for UP-Group name and UP-NODE-ID	cups-cp
CSCwe37928	Observing sessmgr crash::sn_aaa_session_get_user_data	cups-cp
CSCwd39954	[CUPS-CP] Delay seen when CP handles 32 Sx associated UPs	cups-cp
CSCwd40067	4G QOS sent on UP after CCA-U while UE still in 3G	cups-cp
CSCwe42876	aaamgr in warn state for CP	cups-cp
CSCwd40162	[BP-CUPS] sesmgr crash: Assertion failure at sess/smgr/sessmgr_fsm_func.c:10998	cups-cp
CSCwe01868	SX collision in Delete IDFT and logs Misc Error3: Internal Failure : SX_MODIFY_REQ failed for Trans	cups-cp
CSCwe32996	[BP-CUPS]: sessmgr crashes at Function: acsmgr_deactivate_predef_rules()	cups-cp
CSCwe44005	[BP-CUPS]21.28.3.88871:sessmgr crash has been seen after stopping the call model	cups-cp
CSCwe80883	Incorrect Max Sessions under UP reselection situation	cups-cp
CSCwc19599	Gy credit control failure handling not working when Gy link is down between CP and OCS	cups-cp
CSCwc94195	CUPS: PGW CDR containing wrong (future) timestamp in “record opening time”	cups-cp
CSCwd65151	[CUPS CP] sessmgr restart seen in function sessmgr_saegw_send_sx_modify_req_li()	cups-cp
CSCwc59454	slow response for new calls to existing apn / ip pool at “push config” and “update ip-pool”	cups-cp
CSCwd19554	[BP-CUPS] memory bloating at acsmgr_cups_allocate_charging_snapshot	cups-cp
CSCwd19632	Assertion failure at sessmgr_app_svr_event_control_dispatch	cups-cp
CSCwd60353	CUPS - SAEGW - 21.25.10 - acsmgr_process_qgr_and_create_pdr_far	cups-cp
CSCwd96839	CP triggers CCRU with RESOURCE_ALLOCATION_FAILURE performing 4gto3g Qos Change	cups-cp
CSCwc53115	Fatal Signal 11 in sessmgr_send_modify_rsp_towards_saegw_sgw_drv 21.23.24 of CUPS CP	cups-cp
CSCwd08502	[CUPS CP] MBR reduced to 1Kbps during 4G to 3G handoff if 4G AMBR is 4294968	cups-cp
CSCwd37844	[BP-CUPS]Multiple occurrence sessmgr_nlp_gtpu_sess_abort_hndler()sessmgr_nlp_mqueue_timer_handler	cups-cp
CSCwd76879	Sessmgr process restarted at function sessmgr_compress_call_info()	cups-cp
CSCwe46117	[CUPS-CP] Error SX_MODIFY_REQ failed for Trans: Proc Type: SMGR_GGSN_MODIFY_REQ_QUERY_VOG	cups-cp
CSCwe64039	"[BP-CUPS]After sx-demux recovery,fresh ip-pool chunks not pushed to UP's,existing pools depleted"	cups-cp

Bug ID	Headline	Product Found*
CSCwe79487	sessmgr restart at sessmgr_saegw_handle_cleanup_smgr_data	cups-cp
CSCwd19115	[BP-CUPS]:Assertion failure at ipms/ipms_api.c:1239 Function: ipms_event()	cups-cp
CSCwe93220	Modification required in syslog error on CUPS CP	cups-cp
CSCwd20301	[BP-CUPS] SessMgr restart due to corruption when processing secondary RAT records	cups-cp
CSCwd28140	QER update for AMBR not received by UP from CP	cups-cp
CSCwe17344	[BP-CUPS] Fatal Signal 11: 11 PC: [0a2e24dc/X] check_n_update_gx_rules()	cups-cp
CSCwe70452	[CUPS-CP] SessMgr restart while handling response for deletion	cups-cp
CSCwd39782	[BP-CUPS] root-dir line in the local context sshd configuration is missing after reboot of StarOS	cups-cp
CSCwd71878	[BP-CUPS] Sessionnot terminated after Gy Bypass time exhaustion (SU_URR time quota)	cups-cp
CSCwd87905	[BP-CUPS] Observed sessmgr restart “free_acct()” during sessmgr kill in longevity setup.	cups-cp
CSCwe24070	[BP-CUPS]: sessmgr crash at Function: acsmgr_collect_usage_for_all_monitoring_keys()	cups-cp
CSCwe74646	sessmgr restart on CUPS CP at function acsmgr_create_nsh_info	cups-cp
CSCwe75230	CP Tries Updating PDR ID 0x0000 - resulting in Reject and VoLTE Call Drop	cups-cp
CSCwd39033	Multiple Sessmgr Crash with function:ipms_flush_hidx	cups-cp
CSCwd40148	[CUPS-CP] SessMgr restarts on Sec rat trigger hitting threshold with 2 def bearers for pure-S calls	cups-cp
CSCwd51827	CUPS CP sessmgr crash in sessmgr_app_svr_event_control_dispatch - 21.23.26	cups-cp
CSCwe50682	MCPTT flow not working after CUPS Upgrade to 21.28.m0	cups-cp
CSCwd40057	"After all sessmgr restart, sx-peer-node info is lost on standby chassis"	cups-up
CSCwe53212	MLX5 Core Driver - missing local and vnfmeth interfaces	cups-up
CSCwd09429	[CUPS] Active ftp is failing - SYN-ACK dropped due to “Invalid TCP pre-connection Request”	cups-up
CSCwd32296	UP credit-control group config after SO (diameter ignore-service-id option) is not proper	cups-up
CSCwd96944	Sessmgr instance restarted at function sessmgr_populate_pdr_in_teid_list()	cups-up
CSCwe32987	[BP_CUPS] NSH Traffic steering is broken on hermes - 21.26.hx	cups-up
CSCwc18750	ARP Request have wrong Sender IP set to network address instead of interface address	cups-up
CSCwd38945	[BP-CUPS] Cfgmgr - Unable to browse traffic even with quota available	cups-up
CSCwe62837	difference between CUPS and ASR5500 in case of redirected flow getting reclassified	cups-up
CSCwd10956	[BP-CUPS]: Sessmgr crash at uplane_populate_nbr_field_edr_charging_id() after task kill	cups-up
CSCwc97902	[BP-CUPS] V6 peers not coming up due to cause PFCP_CAUSE_REQUEST_REJECTED	cups-up
CSCwd95901	"CUPS UP - After sessmgr crash, sessmgr is not showing p2p as loaded in 'show module'"	cups-up
CSCwe40695	CUPS UP - ruledefs associated with host-pool are not working after UP Switchover	cups-up

Bug ID	Headline	Product Found*
CSCwc55681	CUPS CP Usage Report Failure. Received URR : 0x80000xxx not requested	cups-up
CSCwc63061	sessmgr restart during egtp signalling procedure	cups-up
CSCwc81666	[CUPS RCM] RCM trying to create the server list before the UP instance created	cups-up
CSCwd46457	SSD collection may cause BFD timeout with 16 vpp workers due to show memory main-heap	cups-up
CSCwc44036	EDR printing wrong end time	cups-up
CSCwd16366	LI IPSec tunnel flaps intermittently due to SA Collision	epdg
CSCwd10414	OFR Requirement to enable DH Group 5 in 21.27	epdg
CSCwd52626	Assert at egtpc_resume_suspended_proc()	mme
CSCwe81395	MME is sending wrong Macro eNodeB ID under “GLOBAL ENB-ID” IE in PWS Restart and Failure Indication	mme
CSCwc99355	Target MME sending Source SGW IPv6 address in Handover Request	mme
CSCwd10265	[5GaaS] MME sending wrong destination realm resulting in 3002 from DRA	mme
CSCwe42649	MME using IPv6 address wrongly during TAU triggered inter-SGW change.	mme
CSCwc93870	DCNR Devices and Attached DCNR calls shows different values	mme
CSCwd71339	Increase in DUCON_NSA errors / path switch failures	mme
CSCwe56368	Sessmgr restart due to assertion failure in sn_gt_handle_mm_req_failure function.	mme
CSCwd68562	ASR5500 - MME- 21.25.4 (83215) - MMES1PathFail increase	mme
CSCwb59168	Encoding error @Stop-Warning-Indication message for multiple eNB-ID in “Broadcast-Empty-Area-List”	mme
CSCwc95123	[MME] Mmemgr restart are seen during regression carried on VPC-DI with PWS messages	mme
CSCwe30923	Observing sessmgr crash with function :: egtpc_resume_suspended_proc()	mme
CSCwc95044	MME continues to use blockedlisted SGW	mme
CSCwe82813	Incorrect Cell-ID value observed in PWS Restart Indication message in mon pro	mme
CSCwd08401	MME requirement in the 3GPP Specifications with respect to EPS to 5GS Mobility registration	mme
CSCwd97399	Observing mmemgr crash:: cmPAsnDecChExt	mme
CSCwc80299	"CBC , MME send Write Replace Warning Indication before Write Replace Warning Response"	mme
CSCwe54365	MME sets incorrect NRI container in ULR to VLR when receiving NRI container in attach-req	mme
CSCwe74210	SBcAP encoding error when S1AP PWS Restart Indication does not contain optional IE EmergencyAreaID	mme

Bug ID	Headline	Product Found*
CSCwc88038	MSCC AVP missing in retried Gy CCR-I message	pdn-gw
CSCwe95764	PGW-MPN: Session Manager restart happen during host-pool change	pdn-gw
CSCwe15218	Diamproxy Restart After FQDN Configuration on Gy Endpoint	pdn-gw
CSCwe21674	Authentication Failing during UDP Socket Creation when using IP VRF Forwarding	pdn-gw
CSCwd43478	PGW rejecting create_Session_Req even if SGW is sending a Conditional/Optional IE	pdn-gw
CSCwe23018	CLI corruption in the output after running “update active-charging override-control rulebase-config	pdn-gw
CSCwd46286	"Gy Server returns RC 5030 causing Assume Positive to kick in, CCR-T will contain USU with all zero"	pdn-gw
CSCwd55724	Duplicate Precedence assignment by PGW in TFT packet Filters	pdn-gw
CSCwd40511	sessmgr restart on acsmgr_process_tcp_packet	pdn-gw
CSCwd67200	Incomplete MSISDN in servedMSISDN CDR field	pdn-gw
CSCwd80515	PGW not binding Gx Dynamic rule for dedicated bearer in WiFi to LTE handoff scenario	pdn-gw
CSCwa49391	[BP-CUPS] Traffic Optimization UP stats not getting incremented/decremented properly	pdn-gw
CSCwc09456	Sessmgr instance restart due to assertion failure at acs/acsmgr/acsmgr	pdn-gw
CSCwc97269	APN configuration getting removed	pdn-gw
CSCwd12198	[ICUPS-Smoke2] Assertion Failure @ acsmgr_config_acs_rule_options	pdn-gw
CSCwd26943	AA Request sent by PGW with MCC 314 has the User-Name AVP MNC transposed to 024 in the Realm	pdn-gw
CSCwd44164	sessmgr task unexpected restarted occurred on PGW acs_http_accel_check	pdn-gw
CSCwf01825	One way traffic reported after UE goes into assume positive state when CCR-U triggered by VT	pdn-gw
CSCwd32146	?Update Bearer Request? is send PGW->SGW without EPS Bearer QoS, which is not aligned with 3GPP	pdn-gw
CSCwd39197	E911 calls fail with GTPv2 Cause Code 73 - No Resources Available after PGW fails to send DNS Query	pdn-gw
CSCwe21138	BP-ICUPS: sessmgr restart : sfw_nat_allocate_port_chunk_from_recovery_list()	pdn-gw
CSCwc83287	[Smoke2-ICUPS] Undefined_Function_PC and hatsystem_process_card_fail_msg crash seen in regression	pdn-gw
CSCwc88534	Diagnostic code for unexpected dra peer switch	pdn-gw
CSCwd02729	Continuous EGTPCPathFailClear traps after receiving echo requests during no session	pdn-gw
CSCwd65441	E911 calls fail with GTPv2 Cause Code 73 - No Resources Available after PGW fails to send DNS Query	pdn-gw
CSCwc53423	Sessmgr task restart on sess/egtp/egtpc/egtpc_evt_handler_func	pdn-gw

Bug ID	Headline	Product Found*
CSCwe24837	New sessions accepted while APN set with newcall policy reject	sae-gw
CSCwd18840	Missing framed route after ICSR switchover	sae-gw
CSCwd64943	[SAEGW] - ASR5500- - 21.23. 12 ICSR Standby sessmgr in Memory over state	sae-gw
CSCwd99902	Assertion Failures triggered during ADMF provisioning/auditing LI configuration	sae-gw
CSCwe04086	Sessmgr Restart at sess/sgsn/stackmgr/sn_gprs_gtp.c	sgsn
CSCwc69565	[S8HR] show lawful-intercept s8hr statistics all display the wrong ebi value	sgw
CSCwd41016	No session deletion after S5 path failure followed by bearer resource command	sgw
CSCwd41111	[S8HR] SGW increments “Apn Lookup Failed” wrongly for packets sent over non-s8hr bearers	sgw
CSCwd07968	aaamgr going to warn/over state again and again	staros
CSCwd65439	Password change option for user in warning period before expiration.	staros
CSCwe36928	[ares] AFIO - by default disable fabric device register dump collection when DCH FIFOs overflow	staros
CSCwd89468	Cisco StarOS Software Key-based SSH Authentication Privilege Escalation Vulnerability	staros
CSCwe74149	SRIOV MAC Reset during unbind for Trusted VF	staros
CSCwd12668	DL packets held within UPF after stream offload/onload	upf
CSCwe10556	[UPF] Flow Idle timing out even thought traffic is seen on fastpath	upf
CSCwd05061	EDNS readdress is not working	upf
***** Information in the “Product Found” column identifies the product in which the bug was initially identified.		

Operator Notes

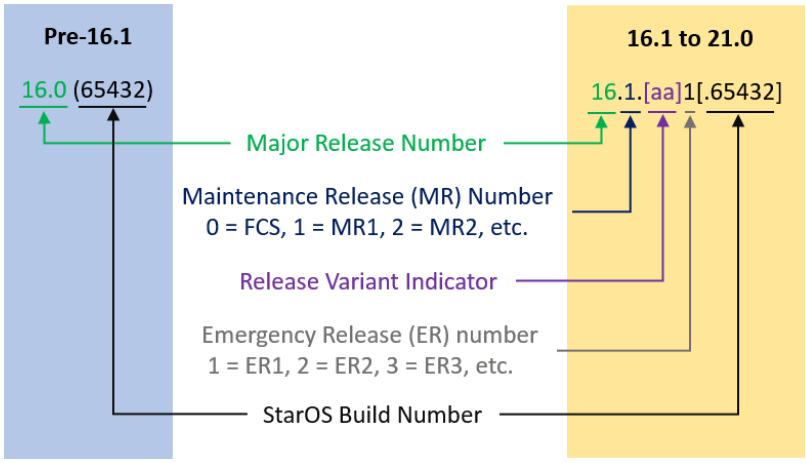
StarOS Version Numbering System

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.

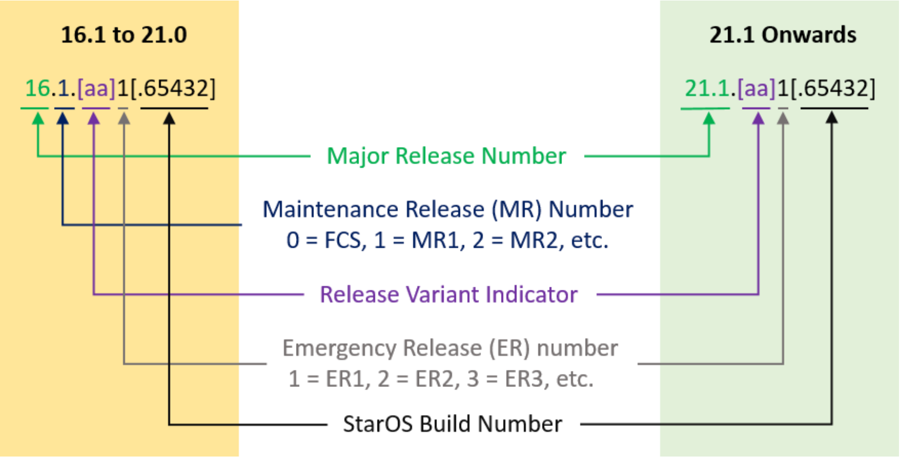
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example “16.0 (55435)”. Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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


Pre-16.1
16.0 (65432)
16.1 to 21.0
16.1.[aa]1[.65432]
Major Release Number
Maintenance Release (MR) Number
0 = FCS, 1 = MR1, 2 = MR2, etc.
Release Variant Indicator
Emergency Release (ER) number
1 = ER1, 2 = ER2, 3 = ER3, etc.
StarOS Build Number

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


16.1 to 21.0
16.1.[aa]1[.65432]
21.1 Onwards
21.1.[aa]1[.65432]
Major Release Number
Maintenance Release (MR) Number
0 = FCS, 1 = MR1, 2 = MR2, etc.
Release Variant Indicator
Emergency Release (ER) number
1 = ER1, 2 = ER2, 3 = ER3, etc.
StarOS Build Number

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

Table 5 - 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		
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.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
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.
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.
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.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
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 6 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 6 for descriptions of the specific bundles.
usp_rpm_verify_utils-<version>.tar		Contains information and utilities for verifying USP RPM integrity.

Table 6 - 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.