Release Notes for StarOS™ Software Version 21.27.m1

First Published: May 16, 2023
Last Updated: May 16, 2023

Introduction

This Release Note identifies changes and issues related to this software release. This major release is based on release 21.27.m0. These release notes are applicable to StarOS LegGW & ICUPS products.

Release Package Version Information

Table 1 - Release Package Version Information

Software Packages	Version
StarOS packages	21.27.m1, build 89722

Feature and Behavior Changes

For information on feature and behavior changes associated with this release, refer to the *CUPS Release Change Reference*, and the corresponding *StarOS Release Change Reference*.

Related Documentation

For the complete list of CUPS documentation available for this release, go to https://www.cisco.com/c/en/us/support/wireless/virtual-packet-core/products-installation-and-configuration-guides-list.html.

For the complete list of the corresponding StarOS documentation, go to https://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.

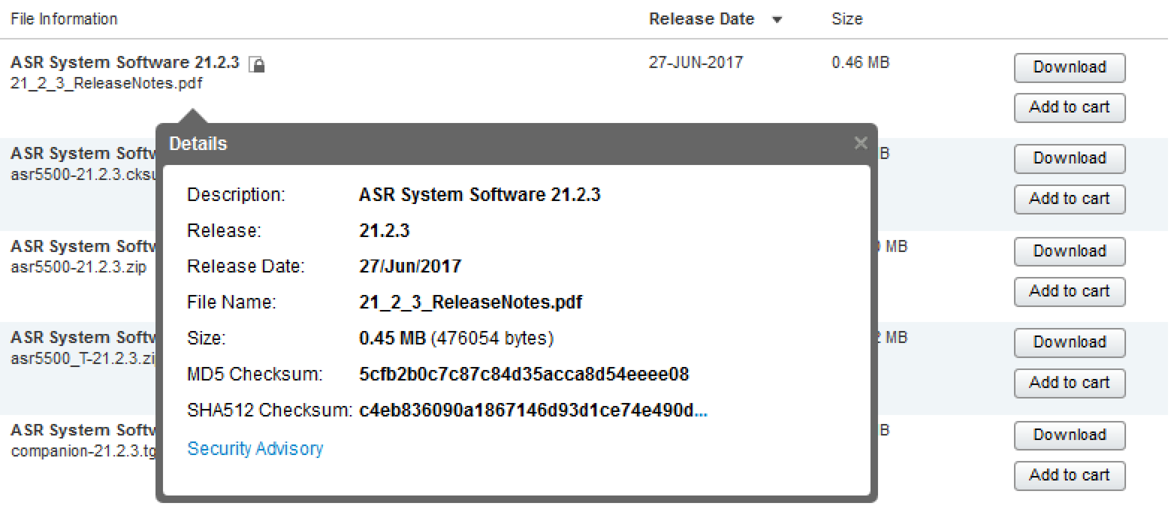
Firmware Updates

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		B
ASR System Softw asr5500-21.2.3.zip		MB
ASR System Softw asr5500_T-21.2.3.zi		MB
ASR System Softw companion-21.2.3.tg		B

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*
CSCwf33047	Observing UAANE state on CP , when CP and UP are loaded with different versions	cups-cp
CSCwe86228	cli display shows contradictory information for UP-Group name and UP-NODE-ID	cups-cp
CSCwa83375	[BP-CUPS] Observed sessmgr restart : snx_sgw_driver_handle_modify_rsp on CP in Longevity setup	cups-cp
CSCwc34754	Active call got disconnected during handoff from 4G to wifi on ICSR setup with Gx-Alias enabled.	cups-cp
CSCwd19554	[BP-CUPS] memory bloating at acsmgr_cups_allocate_charging_snapshot	cups-cp
CSCwc12852	[CUPS-BP] Admin Guide - Servers Unreachable - Specify non-support for after-timer-expiry	cups-cp
CSCwc81923	CUPS LI Admin guide needs to remove SaMOG and ePDG related support	cups-cp
CSCwd19379	[BP-CUPS] call drops on sessmgr task kill - recover_sgx_from_crr failed	cups-cp
CSCwd09301	RMMGR in Warn State on all Active SFs of CUPS-CP	cups-cp
CSCvu76574	[BP-CUPS] recovery-invalid-crr-clp-uplane-gtpu-session checkpoint error	cups-up
CSCwc29508	[BP-CUPS][sessmgr 12341 error][essmgr_uplane.c:36574][SXAB] UE IP Address is different in Traffic	cups-up
CSCwc53344	[BP-CUPS] Function: Assertion failure sessmgr_func.c:37116 Function: sessmgr_get_session_entry	cups-up
CSCwb83398	[BP-CUPS] Lots of error logs GTPU Recover Session Failed for GTP-u Peer on standby UP	cups-up

Bug ID	Headline	Product Found*
CSCwc82316	"Recovery after Gy bypass (SU for CCR-I/CCR-U), UP drops all subscriber packets"	cups-up
CSCvz03179	[BP-CUPS] Assertion failure @ func sessmgr_uplane_check_calls_on_rulebases	cups-up
CSCwc97902	[BP-CUPS] V6 peers not coming up due to cause PFCP_CAUSE_REQUEST_REJECTED	cups-up
CSCwc95490	Assertion failure at sess/sctrl/sessctrl_rcm.c:326-Func-sctrl_config_rcm_service()	cups-up
CSCwf30799	[CUPS UP] UP is not accounting packet in URR after UP switchover for dynamic rule with precedence 0	cups-up
CSCwe60630	CLI task restart during SSD collection	mme
CSCwe28302	PLR with only IMEI option is not working	mme
CSCwe94309	MME rejecting the service request from NBIoT device in case when eea3 and eia3 is enabled	mme
CSCwd19318	Enabling masked-imeisv only working for one mme-service when there are 2 mme-service	mme
CSCwc95163	"[NSO-MOB-FP] p2p plugin has since release 2.65, 4 sets of digits with one ER value"	nso-mob-fp
CSCwa79744	BP-ICUPS : CUSP Feature not working in 21.27.x builds	pdn-gw
CSCwf33189	Sessmgr task restart on sess/egtp/egtpc/egtpc_evt_handler_func	pdn-gw
CSCwc83287	[Smoke2-ICUPS] Undefined_Function_PC and hatsystem_process_card_fail_msg crash seen in regression	pdn-gw
CSCwb66185	Document: Removal of Step2 under the Generating SSH Client Key Pair	pdn-gw
CSCwf13981	show config errors showing Error message for IMSA config errors for no associate local policy .	pdn-gw
CSCwe17765	Sgi-reachability handling for permanent disappearance of sessmgr which handles sgi-reachability	pdn-gw
CSCwc10201	Race condition in informing RCM HA state from keepalived to controller	rcm
CSCwd91543	IKE notify packets are not responded after pod reload	rcm
CSCwd99902	Assertion Failures triggered during ADMF provisioning/auditing LI configuration	sae-gw
***** 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 4 - Resolved Bugs in this Release

Bug ID	Headline	Product Found*
CSCwc19603	Lower log level for "sessmgr 12241 error"	cups-cp

Bug ID	Headline	Product Found*
CSCwc21399	[BP-CUPS][sx 221332error<sessmgr:23>sx_db.c:1238]Tunnel_record local seid and Packet seid does not	cups-cp
CSCwc84548	[CUPS-CP] [ICSR] SRP Standby CP sending Sx Session Delete Request which is not expected	cups-cp
CSCwc39963	[Smoke2-Legacy] S8HR Intercepted calls not established after bbiff_trigger	cups-cp
CSCwc26069	[BP-CUPS] acsmgr_set_default_ul_far_for_dyn_rule_binding() multiple occ causing 81% call drops	cups-cp
CSCwb95670	[CUPS] Uplane received invalid far id in PDU	cups-cp
CSCwc15578	[CUPS CP] Sx Mod for Li Dup FAR missing when using GGSN Service and Selective LI Encryption	cups-cp
CSCwc50029	CUPS-CP sessmgr_sgw_handle_delete_req()	cups-cp
CSCwc97995	[CUPS CP]: WIFI to LTE handoff failure due to EBI mixing with dedicated bearer	cups-cp
CSCwb53858	ACSMGR 91432 Error	cups-cp
CSCwb94932	Sessmgr task restart on egtpc_release_pdn_conn_rec()	cups-cp
CSCwc00858	CP is not sending CCR-U during QHT expiry	cups-cp
CSCwc30297	"after initial chunk assinment to UPs, more chunks are assigned to UPs unexpectedly"	cups-cp
CSCwd33517	show apn statistics shows wrong value for GERAN and UTRAN users	cups-cp
CSCwd40148	[CUPS-CP] SessMgr restarts on Sec rat trigger hitting threshold with 2 def bearers for pure-S calls	cups-cp
CSCwb57352	[CUPS] Sx-Modify containing Usage-Report failed. Cause=64 OffendingIE Type=131	cups-cp
CSCwb69920	FHT is disappeared after removing diameter host-select table from ims-auth-service config	cups-cp
CSCwc80718	CUPS CP: Memory leak in sn_memblock_cache_alloc_new due to acsmgr_wrap_far_cache	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
CSCwb94772	session manager restart due to forwarding epsb request	cups-cp
CSCwc18836	[CUPS-CP] CP losing VoGx URR 0x8000000a after ICSR switchover.	cups-cp
CSCwc38090	Spurious error message [sessmgr 12241 error] Misc Error3: Internal Failure : SX_MODIFY_REQ failed	cups-cp
CSCwc42889	CUPS: SGW CDR containing wrong (future) timestamp in “record opening time”	cups-cp
CSCwd39782	[BP-CUPS] root-dir line in the local context sshd configuration is missing after reboot of StarOS	cups-cp
CSCwe24070	[BP-CUPS]: sessmgr crash at Function: acsmgr_collect_usage_for_all_monitoring_keys()	cups-cp
CSCwb45094	SX_ASSOCIATION_SETUP_REQUEST is rejected by CP after Demux SF unavailability	cups-cp
CSCwc20916	[CUPS CP] Assertion Failure @ sn_slist_lookup_by_key()	cups-cp
CSCwc88588	"CUPS-CP - After quota holding timer expiry, CP doesn't invoke Gy"	cups-cp
CSCwa54600	[BP-CUPS] Assertion failure @ PC: [08dc3801/X] fill_dyn_chrg_rule_name_info()	cups-cp

Bug ID	Headline	Product Found*
CSCwd20301	[BP-CUPS] SessMgr restart due to corruption when processing secondary RAT records	cups-cp
CSCwc07644	[BP-CUPS]AF at sess/smgr/sessmgr_gr_sess.c:1368 sessmgr_gr_handle_session_full_checkpoint on standby	cups-cp
CSCwc12794	[BP-CUPS] Observed sessmgr restart : snx_sgw_driver_handle_modify_rsp on CP in Longevity setup	cups-cp
CSCwc49447	CP not forwarding PCC dynamic rules to UP over Sx	cups-cp
CSCwd06686	[CUPS-CP] SessMgr restarts on Sec rat trigger hitting threshold with 2 def bearers for pure-S calls	cups-cp
CSCwd08502	[CUPS CP] MBR reduced to 1Kbps during 4G to 3G handoff if 4G AMBR is 4294968	cups-cp
CSCwb65661	[CUPS] Fatal signal 6 - sgwdrv_process_egtpc_change_notification_ind	cups-cp
CSCwb87081	[CUPS-CP] Discrepancy between Gy and Gz reporting when “exclude-packet-causing-trigger” configured	cups-cp
CSCwc87052	Sessmgr gtpu restart at gtpu_sess_abort_handler	cups-cp
CSCwa98422	[BP-CUPS]observed smgr restart “acsmgr_check_n_delete_pdrs_for_deleting_bearer” in Longevity run	cups-cp
CSCwc20048	Data browsing issue faced after CSFB	cups-cp
CSCwc66274	[CUPS-CP] “Requested-Service-Unit” AVP missing after receiving CCRI with 0 GSU and Redirection	cups-cp
CSCwc77597	High sessmgr utilization on CP due to memory leak from DNS NAPTR queries	cups-cp
CSCwe06468	CUPS CP: sessmgr restart seen in Function: sgwdrv_pdn_fsm_st_connected_evt_modify_bearer_ind()	cups-cp
CSCwc13887	Multiple sessmgr having high memory utilization	cups-cp
CSCwc28234	CUPS - ./sess/aaamgr/aaamgr_api_new_acct.c:282	cups-cp
CSCwc98188	sessmgr crash on CUPS-CP when UE is trying for more than 11 bearers	cups-cp
CSCwe01868	SX collision in Delete IDFT and logs Misc Error3: Internal Failure : SX_MODIFY_REQ failed for Trans	cups-cp
CSCwc78237	"[BP-CUPS] [sessmgr 10699 error]Misc Error:3G UE 0, error code 0,Misc Error: 2G UE 0,error code 0"	cups-cp
CSCwd39954	[CUPS-CP] Delay seen when CP handles 32 Sx associated UPs	cups-cp
CSCwc18750	ARP Request have wrong Sender IP set to network address instead of interface address	cups-up
CSCwb23704	QCI-QOS Mapping Table Copy-Outer Option for Pure-S Calls	cups-up
CSCwb17799	Pure-S call is not terminated by UP busy-out inactive-timeout option if configure APN-Profile.	cups-up
CSCwd67633	[BP-CUPS]libvnet.so.19.08.1/vlan_ip4_qos_mark_node_fn_avx2() with vpp restart	cups-up
CSCwc87274	"CUPS,VPP restart in vlan_ip4_qos_mark_node_fn_avx2"	cups-up

Bug ID	Headline	Product Found*
CSCwd93230	"[CUPS UP] When dynamic rule precedence is zero, UP is not accounting packet in URR "	cups-up
CSCwb54746	Sessmgr restarted on UP at uplane_check_modify_copy_orig_ip_packet()	cups-up
CSCwb83998	sessmgr_uplane_fill_event_record_sess_del()	cups-up
CSCwc54584	[CUPS][npumgr-drv 185001 error vpp_tcp_conn_bind_cb_v6_v4: VPP-LI: Fail to add socket with dhost	cups-up
CSCwb65384	pre-allocated calls becomes 0 in standby UP after user plane service restart	cups-up
CSCwc01038	VPP Panopticon debug tracing is unable to capture packet payload larger than 2K	cups-up
CSCwc23421	[CUPS-BP] ECSv2 - Slow browsing for certain URLs	cups-up
CSCwc26563	[CUPS-UP] standby SessMgr memory leak at sessmgr_uplane_allocate_dupl_param	cups-up
CSCwc30341	[CUPS UP] quota-exhausted pass is not applied if UP sessmgr has other session with other cc group	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
CSCwe00049	sessmgr memory usage is increasing while number of subscribers remains mostly the same	cups-up
CSCwe81754	VPP restart due to SIGBUS error	cups-up
CSCwc07806	[CUPS-UP] SRP standby SessMgr memory leak	cups-up
CSCwc07936	CUPS “pending-traffic-treatment quota-exhausted pass” is not working after back to back pfd push	cups-up
CSCwc53608	[(libvnet.so.19.08.1/ip4_rewrite_node_fn_avx2() [(libvlib.so.19.08.1/dispatch_pending_node	cups-up
CSCwc25704	[CUPS-UP] Some UP does not activate VPP correctly after upgrade or reload	cups-up
CSCwb34949	[CUPS UP]: sessmgr restart seen in uplane_populate_nbr_field_edr_charging_id()	cups-up
CSCwc76586	IPv6 src IP corruption for UDP LI in CUPS	cups-up
CSCwa85071	sessmgr restart while parsing uplane http header	cups-up
CSCwb22363	CUPS UP stuck ICMP NAT port chunks during TOPUP(rulebase change) 21.23.19	cups-up
CSCwd95901	"CUPS UP - After sessmgr crash, sessmgr is not showing p2p as loaded in 'show module'"	cups-up
CSCwd70361	Assertion failure at sess/sctrl/sessctrl_uplane_cfg_sync.c:23427	cups-up
CSCwb70785	"CUPS-UP: hatsystem crash due to VPP timeout, Assertion failure at hat/hatsystem_fail.c:2115"	cups-up
CSCwb93743	CUPS UP sesmgr restarted at specific time after timedef added on CP	cups-up
CSCwc44211	CUPS UP - Upgrade from 21.23.n9 to 21.23.n10 observed higher RTT/delay between S1U/SGi	cups-up
CSCwd33488	[CUPS UP] Large sx messages retransmission from CP if ipsec is used in Sx	cups-up
CSCwb99104	Multiple Sessmgr are in warn state due high memory usage by “epdg_allocate_uli_storage_in_sess” fun	epdg
CSCwd10414	OFR Requirement to enable DH Group 5 in 21.27	epdg

Bug ID	Headline	Product Found*
CSCwc08120	Incorrect Message Level [ipsec 55609 critical] [4/0/10468 <ipsecmgr:284>ipsecmgr_msg.c:1449]	epdg
CSCwb88450	Assertion failure at ../ipm/ipm/ipm_sad.c:	epdg
CSCwb51664	Need associating SMSC Service from specific context support under MME Service.	mme
CSCwb90376	MMEs is generating 00 values on the bulkstat for one of the VLRs	mme
CSCwb53675	[MME] release-due-to-pre-emption (39) S1AP radio network cause not implemented	mme
CSCwb55177	Assertion failure at mme_fsm_event_handler() - Expression: !fsm_data>mfl_in_eh	mme
CSCwa92047	MME: Authentication info to UE not sent during TAU when decor enabled.	mme
CSCwb83204	APN+TAC basic CLI for IMSI clearance.	mme
CSCwa52782	Node reloaded after LAG group port reconfiguration	pdn-gw
CSCwc60913	PGW initiates Gy session eventhough PCRF didnt enable online charging	pdn-gw
CSCwb38857	Release 21.26 removes (link-profile max-rate) config under (traffic-optimization-policy)	pdn-gw
CSCwc67866	Invalid container time of last-usage values	pdn-gw
CSCwb71744	Assume Positive (AP) files not generated when AP properly goes into effect due to any CCA-I failure	pdn-gw
CSCwc88038	MSCC AVP missing in retried Gy CCR-I message	pdn-gw
CSCwd02729	Continuous EGTPCPathFailClear traps after receiving echo requests during no session	pdn-gw
CSCvz68424	21.25:DNS Resolver statistics -overall attempts count is NOT matching with sum of success + failures	pdn-gw
CSCwc44793	Sessmgr task restart on acsmgr_config_acs_rule_options() during ECS config change	pdn-gw
CSCwd39197	E911 calls fail with GTPv2 Cause Code 73 - No Resources Available after PGW fails to send DNS Query	pdn-gw
CSCwc09456	Sessmgr instance restart due to assertion failure at acs/acsmgr/acsmgr	pdn-gw
CSCwc17331	LI encoding issue on HI2 IRI with location of target.	pdn-gw
CSCwd12198	[ICUPS-Smoke2] Assertion Failure @ acsmgr_config_acs_rule_options	pdn-gw
CSCwc80092	Flows are getting terminated even before the configured flow limit is reached	pdn-gw
CSCwc12692	HTTP Redirect sends a 302 Response with extra padding causing HTTP Parsing Errors in UE Web Browser	pdn-gw
CSCwc46023	CLI for Gy failure is not working for all offline cases	pdn-gw
CSCwc25574	[BP-CUPS]Planned UP switchover failing due to “Switchover timer on UPF timed out”	rcm
CSCwb73497	RCM VM manual reboot issue	rcm
CSCwb61900	SSH is sometimes not accessible after RCM VM boot	rcm

Bug ID	Headline	Product Found*
CSCwd17939	"In sGWRecord, changeTime appearing as before time from recordOpeningTime and duration showing zero"	sae-gw
CSCwc35815	AcsMgr error DNS snooping: unexpectedly p_hentry is NULL	sae-gw
CSCwb55423	[VPC-DI] Sessmgr process restart at sessmgr_pgw_fill_event_record_csr	sae-gw
CSCwd64943	[SAEGW] - ASR5500- - 21.23. 12 ICSR Standby sessmgr in Memory over state	sae-gw
CSCwb65556	Observing sessmgr crash:: sessmgr_get_num_mnc_digits	samog
CSCwb79049	Handover :Frozen sessions seen in SGSN after 2g-4g handover	sgsn
CSCwd41111	[S8HR] SGW increments “Apn Lookup Failed” wrongly for packets sent over non-s8hr bearers	sgw
CSCwc99662	SGW sessmgr task restart observed with bearerResourceCmd during S5 path failure	sgw
CSCwc42261	SGW is rejecting the attach even it is emergency apn/subscriber.	sgw
CSCwb75361	[S8HR] sessctrl restart sessctrl_handle_s8hr_apn_list	sgw
CSCwb65646	[S8HR]Malformed packets in IMS signalling/media message	sgw
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
CSCwc40876	NPU Utilization unevenness after MIO switchover and sessmgr restarts	staros
CSCwd17474	Trusted build: StarOS password encryption improvement feature new format saving issue	staros
CSCwb26816	vPC-DI: show card hardware <> does not show cpbond0 details	staros
CSCwb14971	License pid for 21.27	staros
CSCwd49072	Improve detection of invalid qem entry access	staros
CSCwd89468	Cisco StarOS Software Key-based SSH Authentication Privilege Escalation Vulnerability	staros
CSCwd65439	Password change option for user in warning period before expiration.	staros
CSCvw74614	[Combo-UPF]: Peer ID is not displayed correctly in show sx peers cli	upf
CSCwb35998	[UPF-SVI] :sessmgr restarted at sessmgr_uplane_set_teid_pdr_binding_info()	upf
CSCwb98069	[UPF-SVI] : VPP process restarted at sn_assert_signal_handler+0x1632	upf
CSCwb76554	UPF - standby sessmgr way over memory limit	upf
***** Information in the “Product Found” column identifies the product in which the bug was initially identified.		

Operator Notes

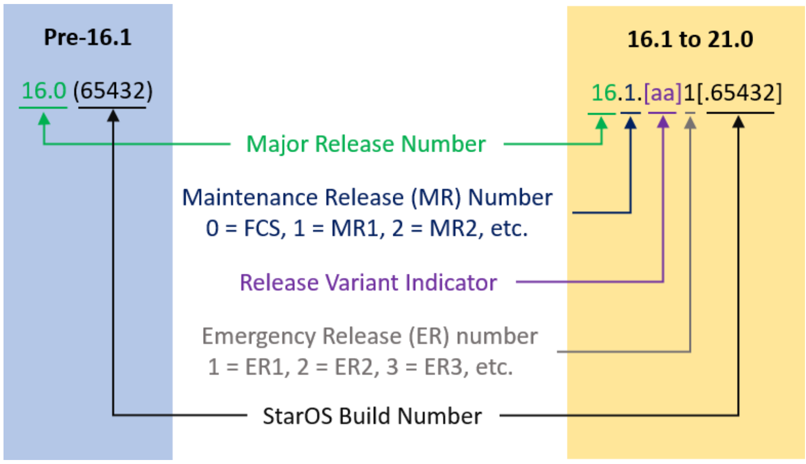
StarOS Version Numbering System

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.

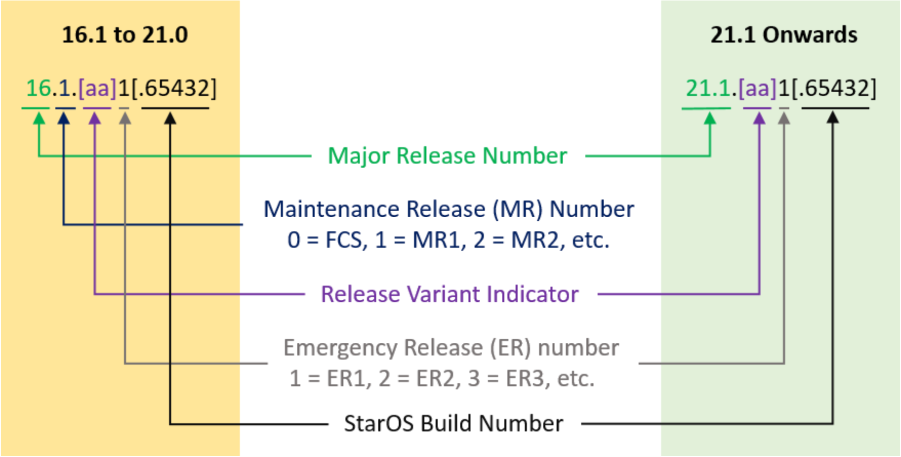
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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

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

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