Release Notes for StarOS™ Software Version 21.28.mh7

First Published: June 30, 2023
Last Updated: June 30, 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.mh6. 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.mh7, build 90399

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.

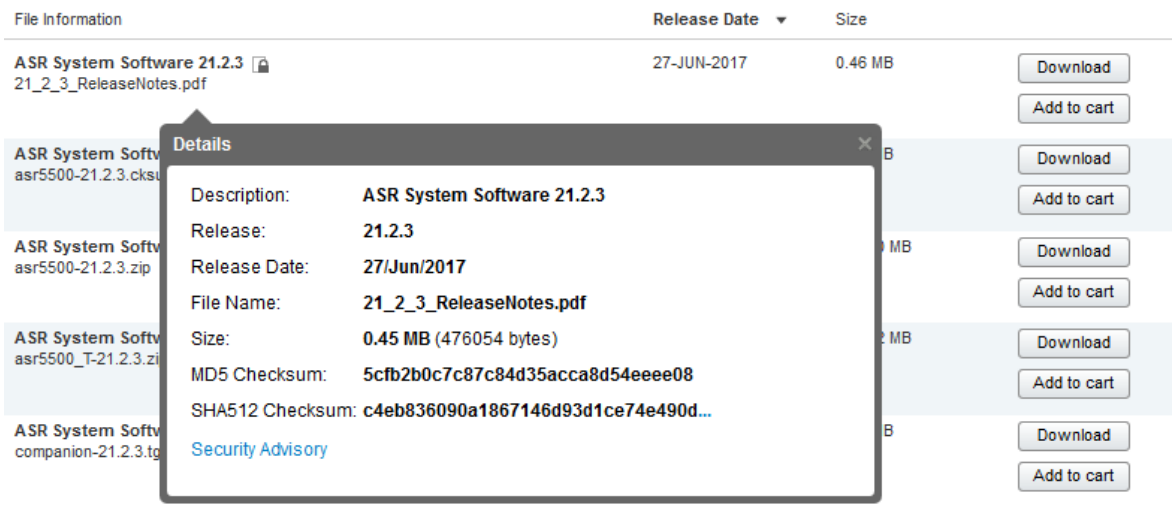
Firmware Updates

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.



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*
CSCwf01589	[CUPS-UP]UP send SX_mod_resp with PFCP_CAUSE_MANDATORY_IE_INCORRECT while doing handover	cups-cp
CSCwf26822	push config-to-up all takes longer than 5mins to finish	cups-cp
CSCwf42495	[CUPS-CP] [LI] Third target interception for the same subscriber NOT working as expected	cups-cp
CSCwf61026	"[21.28.m9.90248][cups-cp] aaamgr is going to warn and over state, when Cp is loaded with 300k subs"	cups-cp
CSCwf49223	Number of active subs in show saegw-service statistics all is greater than actual	cups-cp
CSCwf12125	CUPS: Discrepancy between the time SGW CDR and the time CGF log	cups-cp
CSCwf59752	'show snmp trap statistics verbose wide' command leads to cli crash	cups-cp
CSCwe08636	[BP-CUPS] Dynamic rule is not getting installed with no policy-control update-default-bearer	cups-cp
CSCwe86265	Behavior of command documentation in CUPS-CP User Guide	cups-cp
CSCwf26675	[BP-CUPS] Abnormal Release record closure for 3g call with custom38 dictionary	cups-cp
CSCwb83398	[BP-CUPS] Lots of error logs GTPU Recover Session Failed for GTP-u Peer on standby UP	cups-up
CSCwc99110	[BP-CUPS]: Assertion failure at sess/smgr/sessmgr_gtpu.c sessmgr_egtpu_signalling_routine()	cups-up
CSCwe73462	[BP-CUPS][sessmgr 10396 error]smgr_recovery.c:13989]Sessmgr-10Recover call from CRR failed post SR	cups-up
CSCvu76574	[BP-CUPS] recovery-invalid-crr-clp-uplane-gtpu-session checkpoint error	cups-up
CSCwf01800	[CUPS-UP]Stats mismatch rulebase change during HO with only predef rule	cups-up
CSCwf77251	[BP-CUPS]uplane_insert_tcp_ooo_in_list()uplane_handle_recvd_tcp_OOO_packet()uplane_analyze_tcp()	cups-up
CSCwf52474	[LI] Wrong timestamp format on content delivery interface	cups-up

Bug ID	Headline	Product Found*
CSCwf58640	[CUPS-UP]Need support for show user-plane-service gtpu statistics In SSD	cups-up
CSCwc29508	[BP-CUPS][sessmgr 12341 error][essmgr_uplane.c:36574][SXAB] UE IP Address is different in Traffic	cups-up
CSCwe51492	Sessmgr crash with function :: uplane_create_app_data_flow on Data UPs	cups-up
CSCwc73243	[BP-CUPS] Assertion failure at sess/sctrl/sessctrl_uplane_cfg_sync.c:23721	cups-up
CSCwd60551	"[BP-CUPS]: After task kill, sessmgr restart at function uplane_populate_nbr_field_edr_charging_id()"	cups-up
CSCwf03289	[CUPS-UP]UP not sending correct Uplink Volume in SX_SESSION_REPORT_REQUEST	cups-up
CSCwf58498	[CUPS-UP]DL Data packet getting drop while CBresponse is pending and DL data came	cups-up
CSCwf34386	vpp crash observed	cups-up
CSCwf55939	[BP-CUPS]: observed " sessmgr_uplane_send_sx_sess_modify_rsp_org()" crash on up	cups-up
CSCwf71126	An extra Sx Session Report is generated when moving network	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
CSCwe28302	PLR with only IMEI option is not working	mme
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
CSCwf57524	egtpinmg task restart egtpmgr_find_smgr_for_5G_sub_round_robin.cold	pdn-gw
CSCwe62325	Ubuntu 16.04 ESM/18.04LTS/20.04LTS/22.04LTS/22.10 : systemd vulnerability seen in RCM VM Nessus Scan	rcm
CSCwc53741	Checkpointed information lost after checkpointmgr pod restart	rcm
CSCwb74230	Switchover statistics info is missing in Switchover verbose statistics.	rcm
CSCwc10141	keepalived to controller notification fails but no retry	rcm
CSCwd91543	IKE notify packets are not responded after pod reload	rcm
CSCwe43183	Some UPF specific rcm-controller traps do not show UPF IP address	rcm
CSCwe74835	[SMF-MONSUB]CLI instance id should be same in START/STOP of Trace.	smf
CSCwf01246	[UPF-ST] : Sessmgr error logs "[N4] UE IP Address is different in PDR with PDR ID "	smf
CSCwc67766	[UPF_SVI] N4 Session Report request is getting assigned wrong peer IP addr ::ffff:192.10.25.23	smf
CSCwe79529	opscenter 2 container are crashing (confd & confd-notifications)	smi
CSCwd51484	Apache Tomcat 9.0.0-M1 Req Smuggling and Azul Zulu java (2022-10-18) Mulitple Vulnerabilities	smi
CSCwd81548	[5GaaS] Edge proxy NFs rely on NF restarts to apply config changes	smi
CSCwf79104	Junk values are appended with apn name in EDR record for the apn with no special characters	sgsn

Bug ID	Headline	Product Found*
CSCwe51959	v21.28.mx as the upstream branch :: RHEL-8 Build Issues fix in downstream Dev Branch v21.28.ZVx	staros
CSCwf08057	[UPF-SVI] : Seen Update FAR not found with FAR ID 0x11e with RCM planned/Unplanned SW	upf
CSCwf11828	[UPF-ST]: Error logs Invalid FAR with id 5 received in PDU. IMSI: 311480071230621 Interface: N4	upf
CSCwe33291	[UPF-SVI]: Continuous error logs on standby UPF "SMGR ID mismatch during recovery"	upf
CSCwf20631	[UPF-ST]: LI intercept for combo/Pure S call is not maintained post ICSR/N:M RCM SWO	upf
CSCwf71518	[UPF-ST]: Continuous error log seen on UPF "[N4] Uplane record not found for PDR with PDR ID 0x0"	upf
CSCwf00180	[UPF-SVI] : Seen Error logs "[CDR 1966 - URR ID -2147435417]" with ICSR SW	upf
CSCwf37593	[UPF-SVI] : cnUPF vpp_main in warn state with longevity	upf
CSCwe95648	[UPF-MONSUB]No fastpath(vpp) pcaps are generated for 4G SGWU only call.	upf
CSCwf04131	[UPF-MONSUB]Extra Sx report for MONSUB report.	upf
CSCwf08000	[SVI-UPF] Error logs Remove PDR PDR with ID observed	upf
CSCwe77481	[UPF-MONSUB]Incoming gtpu/GTPU error indication is not captured in slowpath pcap.	upf
CSCwf14455	[UPF-ST] : sessmgr restarted at smgr_is_proto_enabled_for_callid_cups()	upf
CSCwe80667	[UPF-MONSUB]Router advertisement/solicit packet is not captured on GTPU while egressing from sessmgr	upf
CSCwe80795	[UPF-MONSUB]GTPU end marker is not captured in slowpath pcap.	upf
CSCwd60981	[UPF] UPF does not initiate Sx_Session_Report_Req after receiving GTP_ERROR_IND_MSG	upf
CSCwf73165	slow cli and logs with resmgr warning The CPU 1/0 is running with a high 5-minute average cpu usage	upf
CSCwd99519	[UPF-ST] Error logs seen on UPF PDR not found with PDR ID 0x149 and Remove PDR PDR with ID 0x2ce	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 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*
CSCwd66766	cli display shows contradictory information for UP-Group name and UP-NODE-ID	cups-cp
CSCwd40162	[BP-CUPS] sesmgr crash: Assertion failure at sess/smgr/sessmgr_fsm_func.c:10998	cups-cp
CSCwe80883	Incorrect Max Sessions under UP reselection situation	cups-cp

Bug ID	Headline	Product Found*
CSCwe86228	cli display shows contradictory information for UP-Group name and UP-NODE-ID	cups-cp
CSCwe61210	“show subs ... tx-data ... rx-data ...” options not relevant from CP side	cups-cp
CSCwe71916	Sessmgr restart due to assertion failure in pgw_drv_fill_bearer_info_from_egtpc function.	cups-cp
CSCwf63483	CSCwb53858 ACSMGR 91432 Error -> Node prints unnecessary debug logs	cups-cp
CSCwf59908	SAEGW does NOT send CSResp even if SAEGW receives CCA-i with DIAMETER_AUTHORIZATION_REJECTED (5003)	cups-cp
CSCwf51104	[LI] Wrong timestamp format on event delivery interface	cups-cp
CSCwe94671	[CUPS-CP]CP not sending Used-Service-Unit in CCRT-GY message after clearing call	cups-cp
CSCwe79487	sessmgr restart at sessmgr_saegw_handle_cleanup_smgr_data	cups-cp
CSCwe94031	BP-CUPS] Assertion failure at sess/sx/sxc/sx_evt_handler_comm.c:625	cups-cp
CSCwc85511	Disconnect reason for PureS call is different between CSL and (Bulkstats)	cups-cp
CSCwe70452	[CUPS-CP] SessMgr restart while handling response for deletion	cups-cp
CSCwf36402	Sessmgr restart on CUPS CP at function - sessmgr_ggsn_sx_deallocate_trans_info_node	cups-cp
CSCwf63318	(CUPS) SGW incorrectly handling collision between MBR & CBR during N26 handover	cups-cp
CSCwf37463	[cups-cp][21.28.Fm6.89983] sessMgr crash at PC: [04110756/X] sessmgr_saegw_fill_subscriber_info()	cups-cp
CSCwe27814	[BP-CUPS]: [sessmgr 12325 error] Invalid FAR with id 8 received in PDU.	cups-cp
CSCwf15212	[BP-CUPS] egtp echo request not making it out of the CP	cups-cp
CSCwf40956	[BP-CUPS]MCPTT-[gtpc 47514 error] GTPC Misc error: Deactivation already in progress.Unexpected event	cups-cp
CSCwe19158	[BP-CUPS]: Assertion failure at sess/egtp/egtpc/egtpc_main.c:1477	cups-cp
CSCwe61204	Problem with “show subscribers saegw-only username” for Pure-S calls	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
CSCwf35332	F106852: Priority Between UP Groups UP-IP Association/De-association issue.	cups-cp
CSCwe91366	“URR node not found at CP for URR-id” of URR-id ended with 1 or 2	cups-cp
CSCwf11062	Sessmgr restart after GTP-C path failure	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
CSCwe50682	MCPTT flow not working after CUPS Upgrade to 21.28.m0	cups-cp
CSCwe91396	Duplicate TEP removal by CP.	cups-cp

Bug ID	Headline	Product Found*
CSCwf25021	Sessmgr restart at acsmgr_activate_predef_rule_or_group()	cups-cp
CSCwf09416	F138422: Show Subscribers display issue with user plane group filter for upgrade testing	cups-cp
CSCwf66330	Observed sessmgr crash observed with function :: sessmgr_sgw_send_abort_pdn_req_to_drv in CP	cups-cp
CSCwe61164	Problem with command “show subs saegw-only summary seid “	cups-cp
CSCwe93220	Modification required in syslog error on CUPS CP	cups-cp
CSCwf24855	CUPS CP incorrect stats	cups-cp
CSCwf27682	Sessmgr's memory is contiously increasing in KT corporation	cups-up
CSCwe28217	[CUPS UP] sessmgr restart is seen at uplane_free_icmp_session()	cups-up
CSCwf30799	[CUPS UP] UP is not accounting packet in URR after UP switchover for dynamic rule with precedence 0	cups-up
CSCwf44032	[BP-CUPS] Rule mis-match post the rule line modification which has ip server-domain-name	cups-up
CSCwf64710	[CUPS] eDNS enrichment with DNS request including UPP-size result in double UDP-size	cups-up
CSCwe83354	GTPU Test Echoes Received but not Reported to CLI	cups-up
CSCwf09429	VPP NSH Fastpath Tables Not Initialized	cups-up
CSCwf64696	[CUPS] Empty EDR and general drops incremented due to firewall drops	cups-up
CSCwf03759	CUPS UP sessmgr core file generated on SRP Standby node	cups-up
CSCwf57017	UP is not advertising static IP using explicit-route-advertise feature under VRF towards PE	cups-up
CSCwe70286	"ePDG PLMN handoff attempts,success counters having same values in CLI"	epdg
CSCwf23942	ePDG sends invalid S-NSSAI values in IKE_AUTH_RESPONSE even when 5G-IWK feature is not enabled	epdg
CSCwe51260	mmemgr crash	mme
CSCwf54298	[CP-MME]New statistics under Attach Reject category for hss abort except subscription withdrawn	mme
CSCwf57991	Clearing mismatched S1 context in sessmgr upon reception of Error Indication	mme
CSCwf19626	Backward compatibility of MME (supporting LTE-M) with SGW that does not support LTE-M	mme
CSCwf37226	Sessmgr restart in mme_abort_pdn_disconnect_procedure() post guard timer expiry	mme
CSCwe96936	Sessmgr process restarted at function “egtpc_handle_resume_proc_cmd_evt()”	mme
CSCwf52213	Assertion failure at sess/mme-hss/src/mme_hss_api.c:276	mme
CSCwf40583	Sessmgr process restarted at function “mme_egptc_set_pdn_state.isra.283()”	mme
CSCwf42224	HSS sending the access restriction 'NR as Secondary RAT Not Allowed' then why DCNR set flag=1 in MME	mme
CSCwf51538	MME sessmgr restart at egtpc_handle_del_bearer_cmd_req_evt()	mme
CSCwe94309	MME rejecting the service request from NBIoT device in case when eea3 and eia3 is enabled	mme

Bug ID	Headline	Product Found*
CSCwe54541	[MME] mmedemux recovery is not supported for ENDC SON feature	mme
CSCwe56039	[CP-MME] Mon pro to display IP with dual stack enabled for all s1-mme port	mme
CSCwf00038	Assertion failure at sess/mme/mme-app/app/mme_brr_proc.c:2400	mme
CSCwe83141	PGW Sends CCR-T when UE is in Assume Positive state and never established a Gy session	pdn-gw
CSCwf13981	show config errors showing Error message for IMSA config errors for no associate local policy .	pdn-gw
CSCwf17642	The PGW sends a CCR-U with no USU when the Tariff-Time-Change value expires)	pdn-gw
CSCwf28179	"STBY SRP PGW, Data-Rate APN KPIs Being Reported with no subscribers"	pdn-gw
CSCwe45652	PGW is not triggering UBR after RAR from PCRF for IP Filter Replace	pdn-gw
CSCwe64879	Bulkstats are reporting high utilization for DATARATE_IPPOOL schema	pdn-gw
CSCwd55745	Facility Mpls_sig is in over state continously	sae-gw
CSCwf27990	Line breaks in APN field causing SGSN/MME EDRs to fail parsing	sgsn
CSCwf08027	Ncurses CVEs Fixes in Legacy Branch StarOS	staros
CSCwf15613	glib CVEs Fixes in Legacy Branch StarOS	staros
CSCwe99045	Mx Critical CVEs Fixes in Legacy Branch StarOS	staros
CSCwf21408	Apply patches for critical security updates on hermes kernel	staros
CSCwf07806	Bash/rsync related CVEs Fixes in Legacy Branch StarOS	staros
CSCwe91848	Placeholder for libxml2/zlib related CVEs Fixes in Legacy Branch StarOS	staros
CSCwf10885	Glibc related CVEs Fixes in Legacy Branch StarOS	staros
CSCwe88330	[UPF-SVI] Continuous error logs on vpnmgr - RTNETLINK socket recv buffer under on hermes	upf
CSCwf15247	[ST-UPF] hold queue cli getting configured but not persistent on UPF	upf
CSCwf21120	UPF gtpumgr going to warn/over state with high memory usage	upf
CSCwf47748	[UPF] UL packet drop seen on UPF with IPv4 UE and V6 N3 Interface	upf
CSCwf52003	Hermes: incorrect isolcpus leading to boot loop.	upf
CSCwe96265	"[UPF-MONSUB]Exit code in case of converged 4G calls is not correct, monsub enabled using console/smf"	upf

***** Information in the “Product Found” column identifies the product in which the bug was initially identified.

Operator Notes

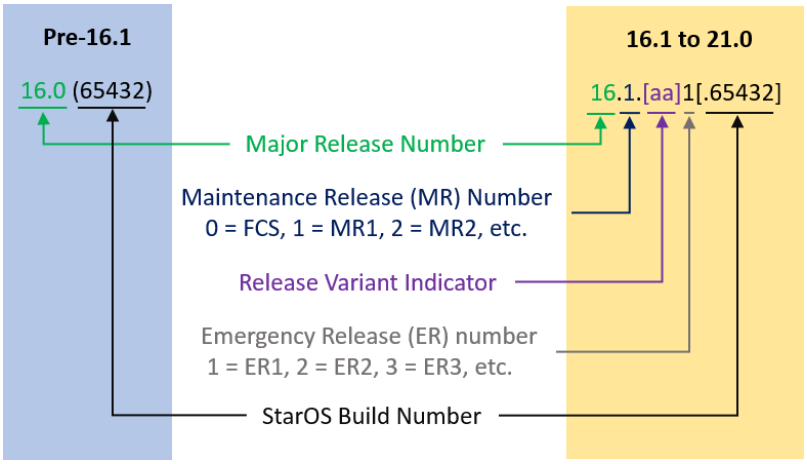
StarOS Version Numbering System

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.

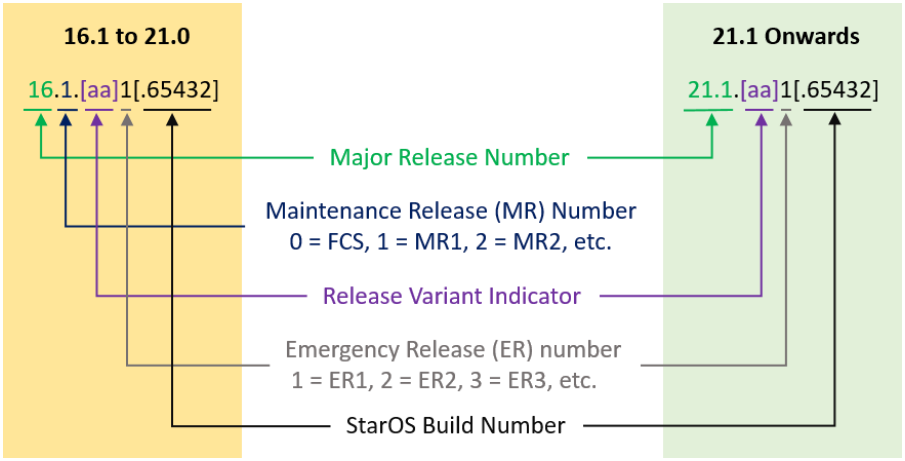
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example “16.0 (55435)”. Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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



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

Table 4 - 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 5 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 5 for descriptions of the specific bundles.
usp_rpm_verify_utils-<version>.tar		Contains information and utilities for verifying USP RPM integrity.

Table 5 - 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.