Release Notes for StarOS™ Software Version 21.26.5

First Published: May 23, 2022
Last Updated: May 23, 2022

Introduction

This Release Note identifies changes and issues related to this software release. This release is the next major feature release since 21.26.3. This release is deployment quality for all StarOS, RCM products other than CUPS.

Release Package Version Information

Table 1 - Release Package Version Information

Software Packages	Version
StarOS packages	21.26.5, build 85462

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.

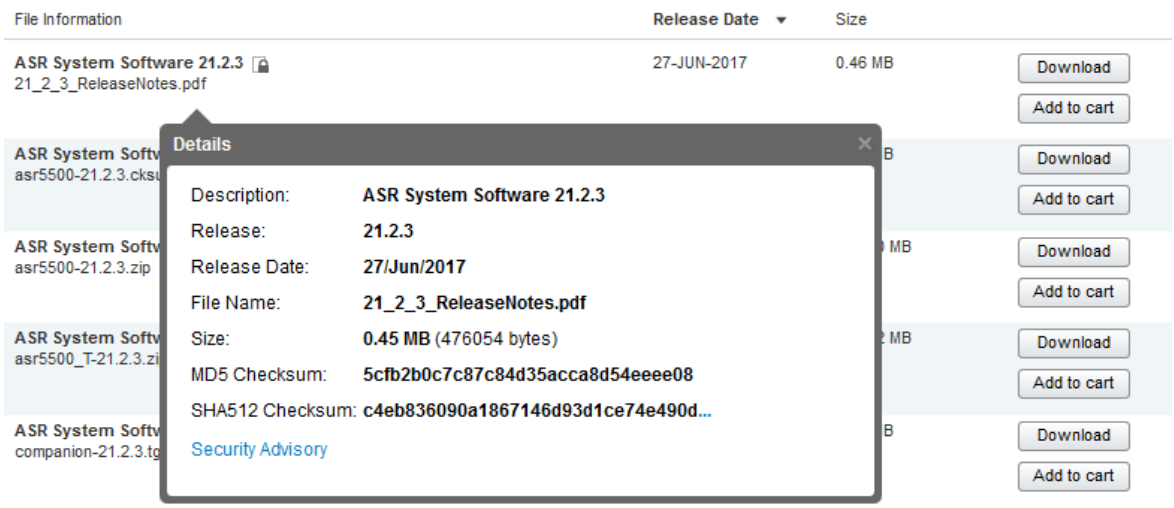
Firmware Updates

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*
CSCvz66300	[BP-CUPS]: Huge number of session disconnection observed related to sx	cups-cp
CSCwa83375	[BP-CUPS] Observed sessmgr restart : snx_sgw_driver_handle_modify_rsp on CP in Longevity setup	cups-cp
CSCvv13409	[BP-CUPS]URR node not found at CP for URR-id: 0x82 received in Usage Report	cups-cp
CSCvz92617	[BP-CUPS]:Huge number of error logs observed acsmgr_populate_chrg_info_from_urr failure	cups-cp
CSCvz90294	smgr_uplane_handle_config_timedef() restart is seen on ICSR UP	cups-up
CSCwa04551	[BP-CUPS]:Fatal Signal 6: Aborted Signal from: kernel	cups-up
CSCwa68097	[BP-CUPS] crash seen on smgr_uplane_opt_hash_table_deinit()	cups-up
CSCvu18163	Recovery mechanism is not working as expected for CIOT calls after session manager restart	mme
CSCwa39049	UBR Buffering is partially working	mme
CSCvu37233	Multiple Sessmgr restarts seen while doing service card migration from active to standby	mme
CSCwb09095	MME shall include Monitoring-Event-Report even when count of UEs is 0.	mme
CSCwa41573	BP-ICUPS: VPP restart seem during the callmodel run with redundancy events	pdn-gw
CSCwa46574	PLT-ICUPS-21.26: DNS_KPI_Enhancements - DNS client statistics output is inconsistent	pdn-gw
CSCwa44222	BP-ICUPS: VPP buffer were full while running callmodel when CUSP is enabled	pdn-gw
CSCwa56618	BP-ICUPS: VPP buffer usage is high even with CUSP disabled (due to missing LEAD packet)	pdn-gw
CSCwa40146	[LI-PGW] Observed un-expected content buffer stats output	sae-gw
CSCvz65453	[SGIR-Ph1] After MIO switchover sgi-reachability profiles status showing as DOWN	sae-gw
CSCwb69300	[UPF-SVI]: Assertion failure Function: sn_memblock_memcache_alloc()	smf

Bug ID	Headline	Product Found*
CSCwa88187	[F99512]Session Report for online URR quota exhaust not triggered for dynamic PCC rules	upf
CSCwa84825	[F99512]Session Report for quota exhaust not triggered post sessmgr restart with tariff time expiry	upf
CSCvz47574	[UPF SVI] :- PCF initiated Dedicated bearer creation is not working [EPSFB] on hSMF	upf
CSCwb69304	[UPF-SVI]: Assertion failure at sess/smgr/sessmgr_uplane_pdr_match.c:18429	upf
CSCwa49743	[UPF-VoN7] Static rules are not accounted for session level usage monitoring from PCF	upf
CSCwa79438	[F99512] UPF doesn't enable Monitoring time received from SMF for Tariff Time usage from CHF	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*
CSCwa51514	[CUPS] PGW should activate "start of traffic" event trigger when OCS grants 0 bytes	cups-cp
CSCwa53617	[CUPS CP] CP is not sending Update QER during 3G UPC (HLR initiated Qos change)	cups-cp
CSCwa57140	Gy down - SU URR ID seen as invalid by UP-new calls rejected with disc_reason:mandatory-ie-incorrect	cups-cp
CSCwb23375	"CP sends SX PFD messages, despite 'sx-pfd-push disabled' being configured under the user-plane-group"	cups-cp
CSCwb71157	PGW U-addr and SGW U addr for dedicated bearer should be IPv4 if it is created with IPv4 address	cups-cp
CSCvz95734	[CUPS CP] Collision scenario 4G UBR and CSR for WIFI handoff	cups-cp
CSCwa38828	[BP-CUPS] Assertion failure @ sx_tun_fsm_handle_sess_del_req_evt	cups-cp
CSCwa90459	[BP-CUPS]:Sessmgr restarts at sn_memblock_memcache_free() leads to call drops	cups-cp
CSCwb02662	[CUPS CP] sessmgr restart is seen in Function: sn_aaa_session_set_user_data()	cups-cp
CSCwb36835	sessmgr 11176 error: Unhandled Sx Modify Response in Connected state	cups-cp
CSCvz19221	UP response PFCP_CAUSE_REQUEST_REJECTED in SX_SESSION_MODIFICATION processing	cups-cp
CSCvz68141	CUPS rejecting sessions instead of disconnecting in out-of-credit prepaid scenario	cups-cp
CSCwa49671	sessmgr restart at sess/imsa/src/imsa_srvr.c	cups-cp
CSCwa57759	sessmgr restart at cups cp	cups-cp

Bug ID	Headline	Product Found*
CSCwb34440	Observing sessmgr crash::sessmgr_sgw_handle_get_peer_profile	cups-cp
CSCvy50239	Incorrect number of the active subscriber in show saegw-service statistics	cups-cp
CSCvz86460	sessmgr restart at acs_cups_fill_bucket_id_type	cups-cp
CSCwb07947	sessmgr crash | sessmgr_app_svr_event_control_dispatch()	cups-cp
CSCwb44877	sessmgr Assertion failure at sess/egtp/egtpc/egtpc_interface.c:246	cups-cp
CSCwb02037	CUPS CP : SGW sess current counter show abnormal increase after ICSR switchover	cups-cp
CSCwa19731	UP in busyout state get sessions assigned	cups-cp
CSCwa58375	Assertion failure @ sess/sx/sxc/sx_interface.c:235 func sx_handle_user_sap_event	cups-cp
CSCwb53858	ACSMGR 91432 Error	cups-cp
CSCwa22035	"mSTimeZone" and "servingNodePLMNIdentifie" fields are missing when using GTPP dictonary custom 24	cups-cp
CSCwa37735	[CUPS]: 'cc-profile any prepaid-prohibited' cli configured under APN is failing in CUPS setup	cups-cp
CSCwa64859	Assertion failure at sess/snx/drivers/sgw/sgw_pdn_fsm_util.c:17059	cups-cp
CSCwa78352	"[CUPS] SMGR_GGSN_SX_MODIFY_REQ_LI or SMGR_PGW_SGW_MODIFY_REQ_LI req to send Mod Req failed for LI,"	cups-cp
CSCwa86579	Observing sessmgr crash on CP | ggsnapp_process_snx_abort_sub_sess()	cups-cp
CSCwb00982	Observing sessmgr crash::sgwdrv_get_bearer_info_data	cups-cp
CSCwb03324	CUPS CP - Unexpected UPC request from CUPS GGSN after QOS change in 3G occurs	cups-cp
CSCwb39582	[CUPS CP] Monitoring key_CP is not reporting the final usage reporting in SX modify response to GX	cups-cp
CSCvz86548	sgw sessmgr restart when clearing new pdn event	cups-cp
CSCwa37702	[CUPS] Fatal signal 11 - smc_sx_pdn_fsm_unhandled_event	cups-cp
CSCwa61799	[CUPS] 4G->2G/3G->4G HO failures - double traffic endpoint deletion	cups-cp
CSCwa69208	CUPS CP LI X2 Event delivery problem after upgrade	cups-cp
CSCwa78138	[CUPS] CUPSSefCache free does not come back to 200 - Loss	cups-cp
CSCwa37818	CUPS: LI Duplicate Flag visible in show subs	cups-cp
CSCwa80683	[CUPS] Fatal Signal 11 - sn_memblock_cache_free_new / acsmgr_free_cups_sef_info	cups-cp
CSCwb06340	[CUPS] SGW does not always properly handle release access bearer with 2 sessions	cups-cp
CSCwb16706	[CUPS] sn_assert() egtpc_handle_rel_access_bearers_rsp_evt() egtpc_handle_user_sap_event()	cups-cp
CSCwa14260	"active counter for pure-S is still remained , though call is already purged due to sx-path-failure "	cups-cp

Bug ID	Headline	Product Found*
CSCwa82516	Assertion failure at sess/imsa/src/imsa_sgx.c:3075	cups-cp
CSCwb08731	[CUPS] CP does not request quota following "start-of-traffic" report from UP	cups-cp
CSCwb32201	CUPS CP imsa_handle_sgx_delete_notify_callback	cups-cp
CSCwb85916	CUPS-CP: Assertion failure at sess/smgr/sessmgr_snx.c:4645	cups-cp
CSCwa07945	[S8HR-CUPS] tracking SIP Signalling as IMSMEDIA li packets	cups-cp
CSCwa33658	sessmgr 12325 error "Uplane received invalid far id in PDU"	cups-cp
CSCwa41564	[BP-CUPS] Current "NAT IP" not cleared post call clear and NBR expiry	cups-cp
CSCwa56054	Complete Fix for Monitoring time chekpointing Issues	cups-cp
CSCwb35130	"CUPS CP : call-waiting service after the PGW <> GGSN handover , kills volte session"	cups-cp
CSCwa68973	Memory Leak Leading to Sessmgr Restarts in CUPS	cups-cp
CSCwb06211	CUPS CP :counter SAEGW.pgw-sesstat-pdn-rat-geran is never reset on 21.23	cups-cp
CSCwb42432	[BP-CUPS]: Fatal Signal 11: 11 PC: [03c4aea6/X] sessmgr_pcc_intf_free_cached_sef_evt()	cups-cp
CSCwa38971	[CUPS] PSF - Config "firewall icmp-fsm" block some ICMP responses expected (sollicited)	cups-up
CSCwa67585	[CUPS UP] UP is creating using each NAT port for every ICMP and never release [Stuck NAT Chunks]	cups-up
CSCwa87288	SIP invite not initiated from UPF to UE	cups-up
CSCvy75464	vpp restart is seen at function unix_signal_handler()	cups-up
CSCwb25436	[CUPS UP] sm restart at uplane_update_packet_stats_chunk()	cups-up
CSCvx13009	"In CUPS nodes IMS subs facing one way audio , intermittently"	cups-up
CSCwa22111	[CUPS UP] sessmgr restart is seen in function uplane_update_packet_stats_chunk()	cups-up
CSCwa72377	Multiple crashes with UP reboot	cups-up
CSCwb22220	Multiple sessmgr restart sn_sct_acs_set_gtpp_group_config() seen on ICSR UP	cups-up
CSCvz62621	Fatal Signal 11: 11 in PC: [04d9a45d/X] uplane_analyze_udp()	cups-up
CSCwa64576	ECGI in EDR is displayed in the decimal format instead of hex	cups-up
CSCwa77273	wrong detection for whatsapp traffic	cups-up
CSCwa38955	[CUPS] Active ftp fails with PSF (Personal statefull firewall)	cups-up
CSCwa41897	[CUPS] APN bulkstat data-touseravg-pps and data-fromuseravg-bps are counting SGW traffic	cups-up
CSCwa59721	[CUPS UP] - Bandwidth Policy not applied after UP Reload	cups-up
CSCwa41738	"LangSupp: Under Biased terminology feature, keyword under CF policy needs to be changed"	cups-up
CSCwa68337	[BP-CUPS] Crash at sessmgr_clear_teid_pdr_binding_info_list() on performing HO	cups-up

Bug ID	Headline	Product Found*
CSCvz50778	CUPS UP - Packets stuck in VPP queue under unknown conditions	cups-up
CSCwa80906	Observing sessmgr crash:sessmgr_uplane_set_teid_pdr_binding_info	cups-up
CSCwa87274	[UPF] Sessmgr crash : uplane_sfw_nat64_translate_ipv6_to_ipv4 during call running model	cups-up
CSCwb01365	[CUPS-UP] SessMgr task restart while generating partial CDR due to secRat reports	cups-up
CSCwb27606	[CUPS-UP]Crash at sx_tun_fsm_handle_sess_mod_rsp_evt	cups-up
CSCwa83817	[CUPS-UP] Some UP does not activate VPP correctly after upgrade or reload	cups-up
CSCwb07764	CUPS UP: nat-binding-timer is not respected strictly	cups-up
CSCwb08945	[BP-CUPS] Sessmgr crash @sessmgr_uplane_process_sx_remove_far () during the LTE to Wifi HO.	cups-up
CSCwb34009	Fatal Signal 11 in acsmgr_destroy_recorded_adc_flows_list()	pdn-gw
CSCwa15922	BP-ICUPS: sessmgr restart at sfw_nat_allocate_nat_ip ()	pdn-gw
CSCwb69047	Dedicated bearer creation between IPv4 only CUPS-UP as SGW-U and IPv4v6 VoLTE PGW is failed	pdn-gw
CSCwb71744	Assume Positive (AP) files not generated when AP properly goes into effect due to any CCA-I failure	pdn-gw
CSCwa56462	Accounting Request Interim Record sent before Validity Time Expired	pdn-gw
CSCwb38857	Release 21.26 removes (link-profile max-rate) config under (traffic-optimization-policy)	pdn-gw
CSCwa39302	sessmgr crashes sessmgr_rf_fill_service() Assertion failure at sess/smgr/sessmgr_rf.c	pdn-gw
CSCwa74502	BP-ICUPS: VPP restart seem during the callmodel run	pdn-gw
CSCwb15151	Difference between sessmgr and aaamgr Causes Rf messages to exceed 3400 limit	pdn-gw
CSCwa54994	BP-ICUPS: sm reload at sn_memblock_cache_block_flush.part.1()	pdn-gw
CSCwb60462	[UPF-RCM]Calls are incorrectly put in VOLTE Non active category and are not cleared as well.	rcm
CSCwb48335	RCM push corrupted config to UP after unplanned migration from UP	rcm
CSCwa05016	[UPF-SVI] :Sessmgr restarted at sessmgr_recover_add_sx_peer_info()	rcm
CSCwa81910	Upgrade packages in RCM	rcm
CSCwb19420	[PLT-RCM] RCM apply_config script giving errors	rcm
CSCvz90288	Running apply_config.sh from different directories	rcm
CSCwb24603	RCM HA S/O is triggered automatically on new masterr after keepalived pod is restarted on old mastr	rcm
CSCwb26274	RCM Ops-center pod needs restart in case of RCM HA s/o in CNDP Environmemt	rcm
CSCwb42558	Upgrade Spring Framework to version 5.2.20	rcm
CSCwb23196	RCM S/O via "rcm migrate primary" cli is failing on rcm.2022.01.1.i7	rcm

Bug ID	Headline	Product Found*
CSCwb12055	CLI to prevent multiple config push notifications towards NSO	rcm
CSCwb26977	Enable VPP full core in non-trusted build	staros
CSCvz28910	Supporting 25G link speed in staros linux kernel code for drivers(i40evf)	staros
CSCwa73707	ssh server config 'client-alive-countmax' is not working	staros
CSCwb11185	EDNS0 fields may not be encoding correctly IPv6 form ASR5500	staros
CSCwb26816	vPC-DI: show card hardware <> does not show cpbond0 details	staros
CSCwb35998	[UPF-SVI] :sessmgr restarted at sessmgr_uplane_set_teid_pdr_binding_info()	upf
CSCwa92472	Packet drop at sessmgr after atomic frag header removal	upf
CSCwb26632	[SVI] continuous crashes on CM run SegFault sessmgr_uplane_process_sx_update_far_update_tep_teid_n4	upf
CSCwa90877	[UPF] VPP crash observed during CUTO Elephant flow for TCP / UDP traffic	upf
CSCwb26397	[EDNS] TCP EDNS packets Drop	upf
CSCwb58450	[UPF-SVI]: PC: [04596802/X] sessmgr_uplane_process_sx_remove_pdr.constprop	upf
CSCwb72252	NYSMFI24 N4 session degradation - SMF sends Sx-rep-Resp with CC-69	upf
CSCwb75113	[SVI-UPF]:sessmgr restarted at uplane_drv_fsm_handle_invalid_evt	upf
CSCwb64090	[UPF]After switchover converged volte active call is showing as volte inactive in RCM.	upf
CSCwa90559	[UPF] CUTO - MBR/GBR values are 0 in TODR generated	upf
CSCvz72185	[UPF-IVT] GTP Peer/Path/Tunnel mgmt stats are missing in 'show user-plane-service gtpu statistics'	upf
CSCwb13828	UPF: 4G to 5G Post HO User-plane setup failure causing call termination due to media inactivity	upf
CSCwb33821	standby UPF in same deployment have vpnmgr in over state at same time	upf
***** Information in the “Product Found” column identifies the product in which the bug was initially identified.		

Operator Notes

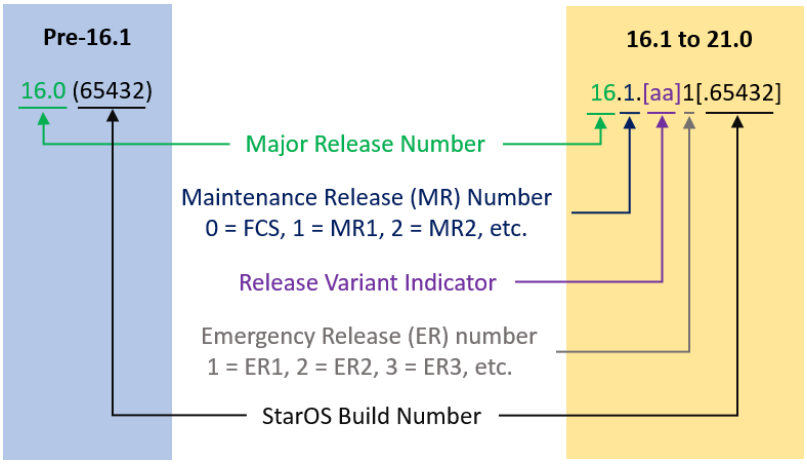
StarOS Version Numbering System

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.

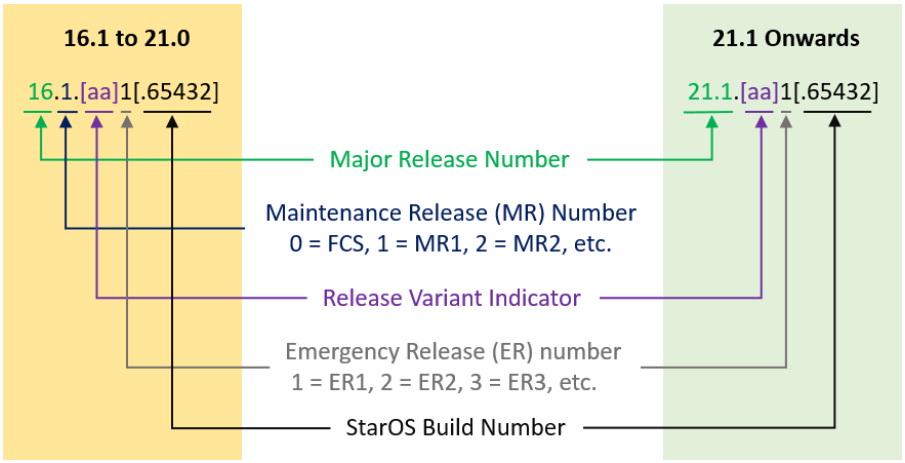
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example “16.0 (55435)”. Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)