



# Release Notes for StarOS™ Software Version 21.26.h4

**First Published:** October 11, 2022

**Last Updated:** October 11, 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.h0.

## Release Package Version Information

**Table 1 - Release Package Version Information**

Software Packages	Version
StarOS packages	21.26.h4, build 87207

## 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.

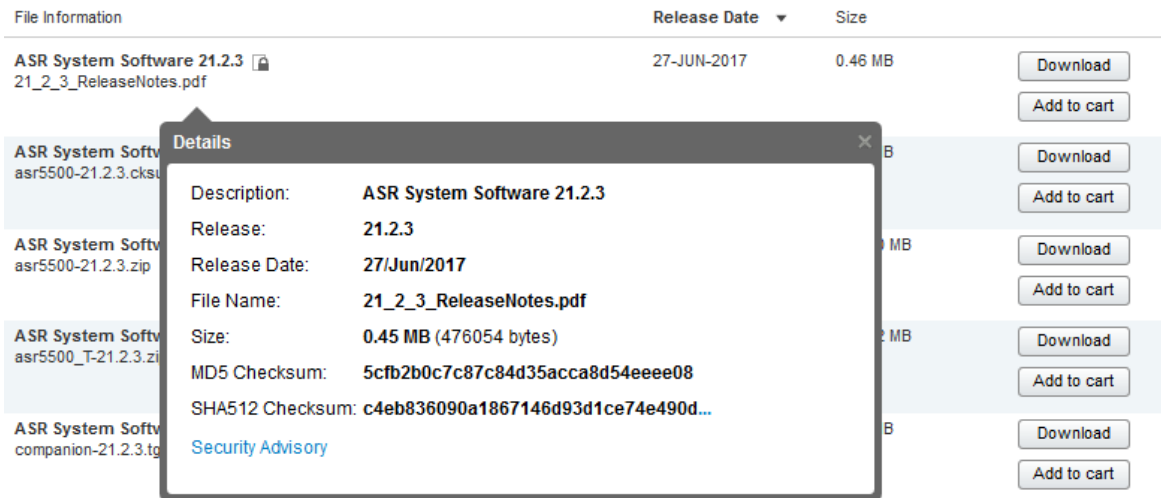
## Firmware Updates

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  <pre>&gt; certutil.exe -hashfile &lt;filename&gt;.&lt;extension&gt; SHA512</pre>
Apple MAC	Open a terminal window and type the following command  <pre>\$ shasum -a 512 &lt;filename&gt;.&lt;extension&gt;</pre>
Linux	Open a terminal window and type the following command  <pre>\$ sha512sum &lt;filename&gt;.&lt;extension&gt;</pre> <p>Or</p> <pre>\$ shasum -a 512 &lt;filename&gt;.&lt;extension&gt;</pre>
<p><b>NOTES:</b></p> <p>&lt;filename&gt; is the name of the file.</p> <p>&lt;extension&gt; is the file extension (e.g. .zip or .tgz).</p>	

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*
CSCvz44140	[BP-CPUS] mostly all aaamgr goes in warn state while running BYT call model	cups-cp
CSCwc95182	SGW doesn't send DBR/DSR triggered by GTPU path failure	cups-cp
CSCwa83375	[BP-CUPS] Observed sessmgr restart : snx_sgw_driver_handle_modify_rsp on CP in Longevity setup	cups-cp
CSCwb57352	[CUPS] Sx-Modify containing Usage-Report failed. Cause=64 OffendingIE Type=131	cups-cp
CSCwc83349	[sgw 140014 error] Failure dispatching event <SNX_MSGTYPE_SGW_ADD_PDN_REQ> during longevity test	cups-cp
CSCwa16910	[BP-CUPS] Assertion failure @ sess/sx/sxc/sx_interface.c:235 func sx_handle_user_sap_event	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
CSCwc59454	slow response for new calls to existing apn / ip pool at "push config" and "update ip-pool"	cups-cp
CSCwa61385	Hermes: show ipv6 neighbors vpp has no output in HX	cups-up
CSCvz99295	[CUPS-TACACS-IPSEC] Crypto map is in Incomplete after configuring	cups-up
CSCwa98318	[BP-CUPS] Assertion failure at Function: sn_memblock_memcache_alloc()	cups-up
CSCwa04551	[BP-CUPS]:Fatal Signal 6: Aborted Signal from: kernel	cups-up
CSCvw79600	"loopXX create failed" when recreate VRF on UP.	cups-up
CSCwd10265	[5GaaS] MME sending wrong destination realm resulting in 3002 from DRA	mme
CSCwa39049	UBR Buffering is partially working	mme
CSCwb09095	MME shall include Monitoring-Event-Report even when count of UEs is 0.	mme
CSCwa41640	BP-ICUPS: fragmentation doesn't work properly with CUSP enabled	pdn-gw

## Resolved Bugs in this Release

Bug ID	Headline	Product Found*
CSCwa44222	BP-ICUPS: VPP buffer were full while running callmodel when CUSP is enabled	pdn-gw
CSCwa52583	ICUPS : Session Manager restarts on PGW	pdn-gw
CSCwc80092	Flows are getting terminated even before the configured flow limit is reached	pdn-gw
CSCwa49391	[BP-CUPS] Traffic Optimization UP stats not getting incremented/decremented properly	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
CSCwc29694	BFD Down due to BFD pkts sent to wrong port post recovery	staros
CSCwa37867	GRE Tunnel with KA not coming up after Card Migration	staros
CSCwc78328	"When UPF detects Sx path failure with no Standby to failover, purge IP chunks and associated subs. "	upf
CSCwa84825	Session Report for quota exhaust not triggered post sessmgr restart with tariff time expiry	upf
CSCwa88187	Session Report for online URR quota exhaust not triggered for dynamic PCC rules	upf
CSCwa79438	UPF doesn't enable Monitoring time received from SMF for Tariff Time usage from CHF	upf
CSCwb99802	UPFs sending unexpected Session Event Records (SERs)	upf
CSCvz47574	[UPF SVI] :- PCF initiated Dedicated bearer creation is not working [EPSFB] on hSMF	upf
CSCwd17799	[UPF-SVI] : Client-ID : n/a in sho sub user-plane-only callid 042cf7f5 flows full	upf
CSCwd18400	configurable CLI for hold-queue-size change to be persistent.	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*
CSCwa53617	[CUPS CP] CP is not sending Update QER during 3G UPC ( HLR initiated Qos change )	cups-cp
CSCwb23375	"CP sends SX PFD messages, despite 'sx-pfd-push disabled' being configured under the user-plane-group"	cups-cp
CSCwb38173	[BP-CUPS]sessmgr 10396 errors on standby CP.	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
CSCwc80718	CUPS CP: Memory leak in sn_memblock_cache_alloc_new due to acsmgr_wrap_far_cache	cups-cp

## Resolved Bugs in this Release

Bug ID	Headline	Product Found*
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
CSCwb33013	Random CRBN/RG mismatch in CDRs	cups-cp
CSCwb36835	sessmgr 11176 error: Unhandled Sx Modify Response in Connected state	cups-cp
CSCwc28234	CUPS - ./sess/aaamgr/aaamgr_api_new_acct.c:282	cups-cp
CSCwa49671	sessmgr restart at sess/imsa/src/imsa_svr.c	cups-cp
CSCwb34440	Observing sessmgr crash::sessmgr_sgw_handle_get_peer_profile	cups-cp
CSCwb95670	[CUPS] Uplane received invalid far id in PDU	cups-cp
CSCwc97995	[CUPS CP ]: WIFI to LTE handoff failure due to EBI mixing with dedicated bearer	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
CSCwc85511	Disconnect reason for PureS call is different between CSL and CLI(65288;Bulkstats)	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
CSCwc42889	CUPS: SGW CDR containing wrong ( future) timestamp in "record opening time"	cups-cp
CSCwb89717	Crash seen at acsmgr_create_urrs_for_static_predef_rule()	cups-cp
CSCwa22035	"mTimeZone" and "servingNodePLMNIdentifie" fields are missing when using GTPP dictionary custom 24	cups-cp
CSCwa37735	[CUPS]: 'cc-profile any prepaid-prohibited' cli configured under APN is failing in CUPS setup	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
CSCwa19731	UP in busyout state get sessions assigned	cups-cp
CSCwb41247	[BP-CUPS] Observed smgr restart "smgr_fsm_newstate" on CP on Longevity execution	cups-cp
CSCwb53858	ACSMGR 91432 Error	cups-cp
CSCwc30297	"after initial chunk assinment to UPs, more chunks are assigned to UPs unexpectedly"	cups-cp
CSCwa82550	[CUPS-CP] Discrepancy between Gy and Gz reporting when	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

## Resolved Bugs in this Release

Bug ID	Headline	Product Found*
CSCwb02037	CUPS CP : SGW sess current counter show abnormal increase after ICSR switchover	cups-cp
CSCwc20916	[CUPS CP ] Assertion Failure @ sn_slist_lookup_by_key()	cups-cp
CSCwa33658	sessmgr 12325 error "Uplane received invalid far id in PDU"	cups-cp
CSCwb35130	"CUPS CP : call-waiting service after the PGW <> GGSN handover , kills volte session"	cups-cp
CSCwb41424	CUPS CP sessmgr task restart smc_sx_copy_sef_pdu_to_sx_pdu	cups-cp
CSCwb63921	sessmgr crash - Assertion failure at sess/smgr/sessmgr_sgw.c:11881	cups-cp
CSCwb80543	CUPS CP sessmgr restart at smgr_fsm_state_connected()	cups-cp
CSCwc12794	[BP-CUPS] Observed sessmgr restart : snx_sgw_driver_handle_modify_rsp on CP in Longevity setup	cups-cp
CSCwc67008	CDR is not sent after unplanned SF card migration.	cups-cp
CSCwd06686	[CUPS-CP] SessMgr restarts on Sec rat trigger hitting threshold with 2 def bearers for pure -S calls	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
CSCwb87081	[CUPS-CP] Discrepancy between Gy and Gz reporting when "exclude-packet-causing-trigger" configured	cups-cp
CSCwb83998	sessmgr_uplane_fill_event_record_sess_del()	cups-up
CSCwb95179	[BP-CUPS] CUTO library is Uninitialized	cups-up
CSCwb25436	[CUPS UP] sm restart at uplane_update_packet_stats_chunk()	cups-up
CSCwa41738	"LangSupp: Under Biased terminology feature, keyword under CF policy needs to be changed"	cups-up
CSCwc01038	VPP Panopticon debug tracing is unable to capture packet payload larger than 2K	cups-up
CSCwc26563	[CUPS-UP] standby SessMgr memory leak at sessmgr_uplane_allocate_dupl_param	cups-up
CSCwa90698	UP-CSL are generated inspite of no related cli config(session-event-module) present in the UP node	cups-up
CSCwb93743	CUPS UP sessmgr restarted at specific time after timedef added on CP	cups-up
CSCwb94113	CUPS: Active UP reload due to NPU-VPP keepalive timeout	cups-up
CSCwb22220	Multiple sessmgr restart sn_sct_acs_set_gtp_group_config() seen on ICSR UP	cups-up
CSCvx13009	"In CUPS nodes IMS subs facing one way audio , intermittently"	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
CSCwb61411	SX Peer doesn't recover even after reconfigure sx_association from UP	cups-up
CSCwc97902	[BP-CUPS] V6 peers not coming up due to cause PFCP_CAUSE_REQUEST_REJECTED	cups-up
CSCwa83817	[CUPS-UP] Some UP does not activate VPP correctly after upgrade or reload	cups-up

## Resolved Bugs in this Release

Bug ID	Headline	Product Found*
CSCwb07764	CUPS UP: nat-binding-timer is not respected strictly	cups-up
CSCwb34009	Fatal Signal 11 in acsmgr_destroy_recorded_adc_flows_list()	pdn-gw
CSCwc12692	HTTP Redirect sends a 302 Response with extra padding causing HTTP Parsing Errors in UE Web Browser	pdn-gw
CSCwa15922	BP-ICUPS: sessmgr restart at sfw_nat_allocate_nat_ip ()	pdn-gw
CSCwb42809	Nat call object list length going wrong when Insertion failed on NAT call obj list	pdn-gw
CSCwa39302	sessmgr crashes sessmgr_rf_fill_service() Assertion failure at sess/smgr/sessmgr_rf.c	pdn-gw
CSCwa83203	Observing sessmgr restart::sessmgr_egtpu_receive_gtpu_v6_packet	pdn-gw
CSCwb76901	We are not adjusting the SACK options correctly in the TCP when we modify the HTTP header.	pdn-gw
CSCwc07472	Optimized changes for adjusting the SACK options correctly in the TCP while modify the HTTP header.	pdn-gw
CSCwc31700	"ecs-rbase-sess-cur" in ECS schema has abnormal value	pdn-gw
CSCwc61468	In staros 21.26.6 - Flows not properly offloaded to VPP resulting in throughput degradation	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
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
CSCwb15151	Difference between sessmgr and aaamgr Causes Rf messages to exceed 3400 limit	pdn-gw
CSCwc44793	Sessmgr task restart on acsmgr_config_acs_rule_options() during ECS config change	pdn-gw
CSCwc25574	[BP-CUPS]Planned UP switchover failing due to "Switchover timer on UPF timed out"	rcm
CSCwa79949	[soltest]: M6 UPF Sessmgr instances stuck in SERVER Mode after SWO	rcm
CSCwc35815	AcsMgr error DNS snooping: unexpectedly p_hentry is NULL	sae-gw
CSCwb59156	Assertion failure at acs_copy_to_rule_defn()	sae-gw
CSCwb26977	Enable VPP full core in non-trusted build	staros
CSCwc18985	Autoconfirm to be enabled from exec mode instead of config mode	staros
CSCwc40876	NPU Utilization unevenness after MIO switchover and sessmgr restarts	staros
CSCwb26816	vPC-DI: show card hardware &lt;&gt; does not show cpbond0 details	staros
CSCwb73319	21.26.1.83746 - crashes not transferred when "filename-pattern" is configured	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
CSCwa44118	Most of the service flows vanished after SF switch	staros

Bug ID	Headline	Product Found*
CSCwb35998	[UPF-SVI] :sessmgr restarted at sessmgr_uplane_set_teid_pdr_binding_info()	upf
CSCwb21297	Sx TX HB Request count not increasing on CNDP DATA UPFs	upf
CSCwc03312	[UPF] AssertFail sx_tun_fsm_handle_sess_estab_req_msg	upf
CSCwa90559	[UPF] CUTO - MBR/GBR values are 0 in TODR generated	upf
CSCvz92788	[UPF] SNMP traps have incorrect data types for IP address and timestamps	upf
CSCwb64090	[UPF]After switchover converged volte active call is showing as volte inactive in RCM.	upf
CSCwd05061	EDNS readdress is not working	upf
CSCwb75113	[SVI-UPF]:sessmgr restarted at uplane_drv_fsm_handle_invalid_evt	upf
CSCwb76554	UPF - standby sessmgr way over memory limit	upf
CSCwd12668	DL packets held within UPF after stream offload/onload	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
CSCwb87895	[UPF-SVI]: SM restart at sessmgr_uplane_periodic_process_urr_queue on UPF	upf
CSCvw74614	[Combo-UPF]: Peer ID is not displayed correctly in show sx peers cli	upf
CSCwa90877	[UPF] VPP crash observed during CUTO Elephant flow for TCP / UDP traffic	upf
CSCwb26397	[EDNS] TCP EDNS packets Drop	upf
CSCwc06639	[UPF] SegFault sessmgr_uplane_populate_CreateUrr() sessmgr_uplane_process_sx_create_urr()	upf
CSCwc35917	Buffered RTP/RTCP pkts forwarded with incorrect IP/TEID before dedicated bearer is created	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

## 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.

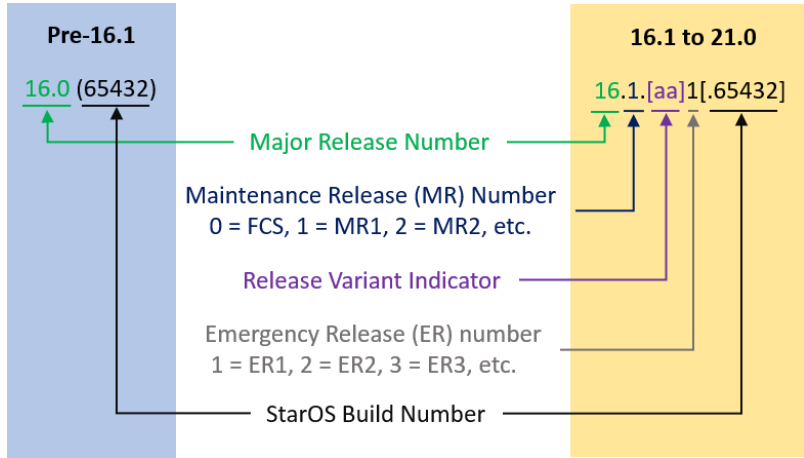
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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

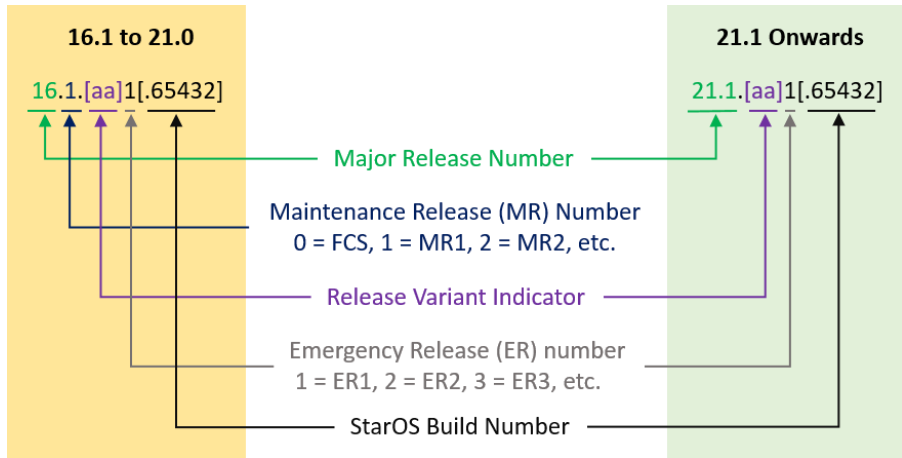


Operator Notes

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
<b>ASR 5500</b>		
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.
<b>StarOS Companion Package</b>		
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.
<b>VPC-DI</b>		
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
qvmc-di-template-vmware-<release>.zip	qvmc-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.
qvmc-di-template-vmware_T-<release>.zip	qvmc-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.
qvmc-di-template-libvirt-kvm-<release>.zip	qvmc-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.
qvmc-di-template-libvirt-kvm_T-<release>.zip	qvmc-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.
qvmc-di-<release>.qcow2.zip	qvmc-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.
qvmc-di_T-<release>.qcow2.zip	qvmc-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.
<b>VPC-SI</b>		
qvmc-si-<release>.bin.zip	qvmc-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.
qvmc-si_T-<release>.bin.zip	qvmc-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
qvmc-si-<release>.iso.zip	qvmc-si-<release>.iso	<p>Contains the VPC-SI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image.</p> <p>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.</p>
qvmc-si_T-<release>.iso.zip	qvmc-si_T-<release>.iso	<p>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.</p> <p>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.</p>
qvmc-si-template-vmware-<release>.zip	qvmc-si-template-vmware-<release>.ova	<p>Contains the VPC-SI binary software image that is used to on-board the software directly into VMware.</p> <p>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.</p>
qvmc-si-template-vmware_T-<release>.zip	qvmc-si-template-vmware_T-<release>.ova	<p>Contains the trusted VPC-SI binary software image that is used to on-board the software directly into VMware.</p> <p>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.</p>
qvmc-si-template-libvirt-kvm-<release>.zip	qvmc-si-template-libvirt-kvm-<release>.tgz	<p>Contains the same VPC-SI ISO identified above and additional installation files for using it on KVM.</p> <p>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.</p>
qvmc-si-template-libvirt-kvm_T-<release>.zip	qvmc-si-template-libvirt-kvm_T-<release>.tgz	<p>Contains the same trusted VPC-SI ISO identified above and additional installation files for using it on KVM.</p> <p>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.</p>
qvmc-si-<release>.qcow2.zip	qvmc-si-<release>.qcow2.gz	<p>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.</p> <p>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.</p>
qvmc-si_T-<release>.qcow2.zip	qvmc-si_T-<release>.qcow2.gz	<p>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.</p> <p>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.</p>

## Operator Notes

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
<b>VPC Companion Package</b>		
companion-vpc-<release>.zip	companion-vpc-<release>.tgz	<p>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.</p> <p>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.</p>
<b>Ultra Service Platform</b>		
usp-<version>.iso		<p>The USP software package containing component RPMs (bundles).</p> <p>Refer to <a href="#">Table 5</a> for descriptions of the specific bundles.</p>
usp_T-<version>.iso		<p>The USP software package containing component RPMs (bundles). This bundle contains trusted images.</p> <p>Refer to <a href="#">Table 5</a> for descriptions of the specific bundles.</p>
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.

## Obtaining Documentation and Submitting a Service Request

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](http://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](http://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)

© 2022 Cisco Systems, Inc. All rights reserved.