Release Notes for StarOS™ Software Version 21.19.11

First Published: July 16, 2021
Last Updated: July 16, 2021

Introduction

This Release Note identifies changes and issues related to this software release. This emergency release is based on release 21.19.10. These release notes are applicable to the ASR5500, VPC-SI and VPC-DI platforms.

Release Package Version Information

Table 1 - Release Package Version Information

Software Packages	Version
StarOS packages	21.19.11, build 81270

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.

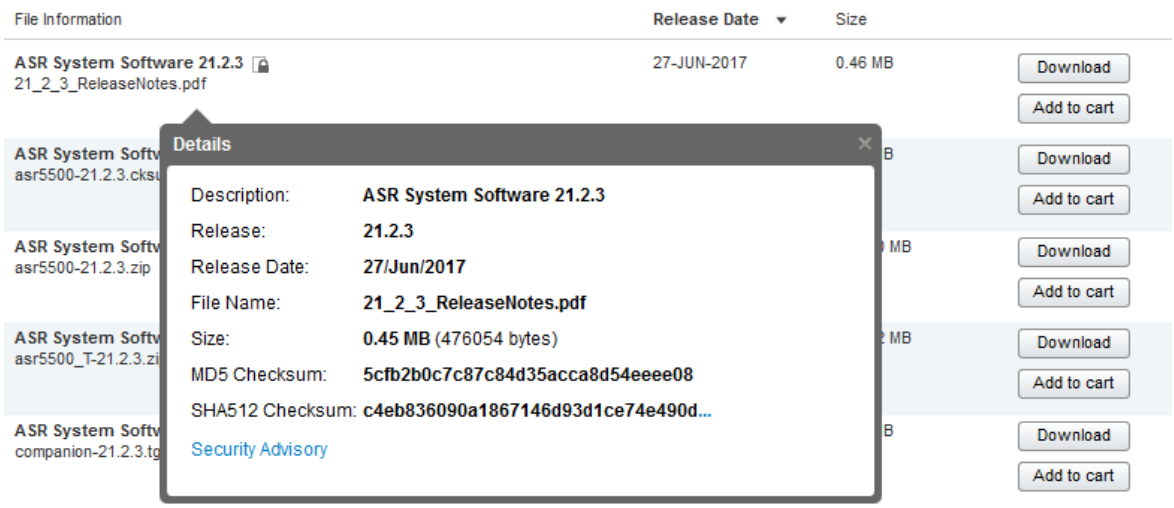
Firmware Updates

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*
CSCvu34579	show crypto statistics not display encode and decode data statics in SI and ASR55K	cups-cp
CSCvy76037	[BP-CUPS]:Assertion failure at sxctrlmgr_recollect_ip_context_info_for_peer_list()	cups-cp
CSCvt26865	sessmgr task restart with fn: sessmgr_ggsn_cups_remove_sx_trans_node()	cups-cp
CSCvu70527	“Replay Errors” observed after perform switch over on CP	cups-cp
CSCvs05924	[URR] [SXAB] Updated URR doesn't exist	cups-up
CSCvu36561	Crash observed on UP at smgr_uplane_update_edr_references_in_all_rbases	cups-up
CSCvw97015	"Sessmgr installing wrong TEP version in VPP, hence packets are dropped"	cups-up
CSCvu14090	[BP-CUPS] sessmgr restart at add_chunk() function	cups-up
CSCvu19385	[BP-CUPS] ICSR - Fatal SIgnal 11 uplane_sfw_nat_gr_handle_nat_realm_update	cups-up
CSCvu35075	IPSec SA rekey happens only if 'keepalive' is also configured	cups-up
CSCvy74044	[BP-CUPS]aaamgr in warn state on IMS UP	cups-up
CSCvv14996	[BP_CUPS] Timedef rule matches if no timedef is configured	cups-up
CSCvy59148	[CUPS-UP] Sessmgr failures occur when “flow action readdress” CLI is configured inside “smtp_all_ca”	cups-up
CSCvu00150	[PLT-CUPS]: The p2p app-identifier tls-sni related CLIs failing at UP	cups-up
CSCvt97779	"[BP_CUPS] CF: sessmgr recovery when done in a particular sequence, call gets dropped"	cups-up
CSCvu19454	MME doesn't return the UE count in a geographical area when imsi-group is configured in hex-format	mme
CSCvu40373	MONTE: MME doesn't send ?Supported-Services? AVP in ISDA S6a	mme
CSCvu18163	Recovery mechanism is not working as expected for CIOT calls after session manager restart	mme

Bug ID	Headline	Product Found*
CSCvu20041	Delete counter not incremented proeprly for Monte	mme
CSCvu70861	[MONTE] RIR is not sent in case if eDRX activated not during Attach but in TAU	mme
CSCvv34694	Sessmgr restarts seen at mme_hss_checkpoint_internal	mme
CSCvu35147	MONTE: eDRX Device: MME is not sending RIR when UE becomes reachable	mme
CSCvu70881	[MONTE] Missing AVP 3142 Monitoring-Event-Config-Status in IDA from MME	mme
CSCvu81405	Revert back CSCvr34106	mme
CSCvx97860	IMEI-TAC matching criteria failing during service request	mme
CSCvu20626	[MONTE] bulkstats counter issue for num-of-ues-in-geographical-area	mme
CSCvu35160	MONTE: MME sends RIR with a weird AVP User-Name value	mme
CSCvq71949	Task restart while handling li session	mme
CSCvu69504	sessmgr restart occurred at diabase_peer_conn_res_info	mme
CSCvx23843	MONTE: S6a IDR NPC timers not sent to T6a in RIR and not sent to UE in TAU_ACCEPT	mme
CSCvu67421	MONTE : MSISDN value is wrongly enclosed into User-Name AVP instead of MSISDN AVP in RIR message	mme
CSCvy03998	Extend the Peer/IMS server status check mechanism to also include peer-host check	pdn-gw
CSCvx66200	[BP-ICUPS]:SM crashes observed on active and standby with “acsmgr_deallocate_call_obj()”	pdn-gw
CSCvw03127	Frequent sessmgr restart on acs_flush_ttl_aged_entries_from_ip_pools	pdn-gw
CSCvv59640	sessmgr_ipv4_process_inet_pkt_part3_pgw_ggsn	pdn-gw
CSCvw76775	Many sessmgr restarts seen on virtual PGW	pdn-gw
CSCvg20133	Segmentation fault at PC: [0d8e2647/X] EZprmSER_CheckError()	staros
CSCvu05306	"After rekey, IPSec SA Pkts count not reset with IKEv2 SA re-establishment triggered by peer"	staros
CSCvw18493	Evaluation of staros for Treck ip stack vulnerabilities - 2nd batch - VU#114986	staros
* 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*
CSCvu76661	[BP-CUPS] crash "vpnmgr_srp_send_to_socket" observed on active CP.	cups-cp
CSCvv64787	UE is not on CP but on UP causing DLDR session report rejection from CP	cups-cp
CSCvx59968	CP sends wrong APN-AMBR (MBR) in QER in PFCP session modification request messages	cups-cp
CSCvx68269	CUPS: LI info visible in monitor protocol	cups-cp
CSCvu87236	"[BP-CUPS]AF,reload at sess/egtp/egtpc/egtpc_evt_handler_func.c:756 egtpc_handle_abort_proc_cmd_evt()"	cups-cp
CSCvx00246	[CUPS / Sx] Unexpected Offending IE: UPDATE_PDR when switching rulebase	cups-cp
CSCvx08962	[CUPS SX] - Unexpected "LINKED URR ID" value (0x00000000) after Rulebase Change	cups-cp
CSCvy00866	Zero quota preemptively-request scenario CP is sending SX modify for PDR which was never created #2	cups-cp
CSCvy95539	[CUPS-CP] "show lawful-intercept full all" output is not displaying CC related information	cups-cp
CSCvv55109	[BP-CUPS]: Assertion failure at ggsnapp_fill_pdp_info_from_egtpu while clearing the calls	cups-cp
CSCvv66631	[BP-CUPS] Assertion at sn_memblock_memcache_alloc()	cups-cp
CSCvx11934	[CUPS ECS] - "flow limit-for-flow-type" and "flow limit-for-bandwidth id" are used together	cups-cp
CSCvx13647	CP rejects DLDR session report by PDR is not present	cups-cp
CSCvx74438	TCP state is INACTIVE in the output of the CLI 'show lawful-intercept full imsi xx' on CP side	cups-cp
CSCvy95216	[CUPS Pure-S] CUPS SGW is not including SGW S1-U TEIDs during piggyback CSR+CBR	cups-cp
CSCvv94329	[CUPS CP] [N+2 UP Redundancy] - (MonPro) Impossible to delete a Monitor Group	cups-cp
CSCvy02620	[CUPS] [PGWCDR] - causeForRecClosing set to "Normal Release" when Sx Path Failure occurs in 3G/2G	cups-cp
CSCvy36038	CUPS CP Adds Null Value 0.0.0.0 as the servingNodeAddress in PGW-CDR	cups-cp
CSCvv74525	Non fatal vpnmgr restart on standby CP - seen every 24 hours	cups-cp
CSCvw02743	[STC CUPS] 3G call fail and session manager restart	cups-cp
CSCvw94565	[BP-CUPS] Inconsistency behavior in handling Predefined Rule and Group-of-Ruledef at control plane	cups-cp
CSCvw99517	[CUPS] Unexpected combinations of CRBN value and PLMN value in CDRs	cups-cp
CSCvx01746	[CUPS] sessmgr restart Fatal Signal 11: 11 : acsmgr_allocate_cups_sef_info()	cups-cp
CSCvx62382	[CUPS-CP] Stale session on CP after Gx rule install failure in 3G	cups-cp
CSCvx72095	[BP-CUPS]: SessMgr restart @ sessmgr_snx_send_drop_call()	cups-cp
CSCvu59278	Cisco CUPS C-plane restart seen when Session Report Indication is rejected on SxA	cups-cp
CSCvw27942	[Smoke2-Legacy] show acs session charging update RG state "Final Unit"	cups-cp

Bug ID	Headline	Product Found*
CSCvy66117	CUPS Gy Failure-Handling for cause-4999	cups-cp
CSCvq81083	[PLT-CUPS-VPN] same USED address are displayed multiple time in show ip pool command.	cups-cp
CSCvx45677	[CUPS] [SGWCDR] - Missing "RANSecondaryRATUsageReport" inside SGWCDR	cups-cp
CSCvx56945	[BP-CUPS] CDR not getting generated upon context replacement	cups-cp
CSCvy63788	Loss of LI X1 connection after CP reboot	cups-cp
CSCvw65523	[CUPS CP] - CP fails to allocate a Peer-ID to UP following the UP Reload	cups-cp
CSCvy33190	No CCR-U from CP after reception of Sx_Session_Report_Request with usage volume for VoGx	cups-cp
CSCvs52657	[SOL TEST] SRP recovery-access-side-failure counters incremented	cups-cp
CSCvt46570	[BP-CUPS]: Huge checkpoint failure at Standby micro-checkpoint failures recovery record not found	cups-cp
CSCvu48856	[BP-CUPS]: [gtpc 47514 error] GTPC Misc error: Deactivation already in progress.	cups-cp
CSCvu86949	[BP-CUPS]: sessmgr restart at acsmgr_allocate_far_id()	cups-cp
CSCvv80358	[BP-CUPS] sx-path-failure after ICSR switchback	cups-cp
CSCvx45708	[CUPS] [PGWCDR] - causeForRecClosing set to "Normal Release" when Sx Path Failure occurs	cups-cp
CSCvx54858	[CUPS CP] GGSN sends CPC Response with Tunnel ID Data I: 0x00000000	cups-cp
CSCvx69017	Assertion failure at sess/smgr/sessmgr_saegw.c:8912 @ Function: sessmgr_delete_pending_timeout()	cups-cp
CSCvu24136	Sessmgr reloaded due to sn_memblock_memcache_free()	cups-up
CSCvv82165	"After double-fault, sxdemux has incorrect view of sessmgr instances."	cups-up
CSCvw45972	Maximum QGRs supported over Sx should be 20. Currently they are 16	cups-up
CSCvw47662	[BP-CUPS]sessmgr_uplane_action_prioritization() uplane_http_pkt_inspection()	cups-up
CSCvw76282	[CUPS-UPF] Multiple sessmgr crashes on UP	cups-up
CSCvu19838	[BP-CUPS] Error Log SEID: Ê Non-zero Correlation id while sending Sx session report request	cups-up
CSCvw83244	Uplink packet drops after 4g->3G handover on CUPS UP with this error: ADF UL TEID/QFI key mismatch	cups-up
CSCvw99852	[BP-CUPS]: Crash observed at smgr_uplane_fapi_config_change_timer_callback()	cups-up
CSCvx22765	CUPS UP sessmgr restart at acsmgr_process_get_grp_of_rdefs_stats	cups-up
CSCvw70447	CUPS continuous sessctrl restart on standby-UPIMS Pure-S following ECS config update on the fly	cups-up
CSCvx32800	[CUPS / UPF-DATA] Fatal Signal 11 at sessmgr_uplane_readdr_adf_compare_hash_entry	cups-up
CSCvx97927	[CUPS UP] - UP stuck in "UAANEPU" state after CP Reload	cups-up

Bug ID	Headline	Product Found*
CSCvw04208	show subscribers user-plane-only callid <id> qos-group statistics not giving correct o/p on v21.x.gx	cups-up
CSCvw71600	[CUPS] vpp_output.log size growing to 1GB - causes no space left on device - sessmgr crash observed	cups-up
CSCvx73933	CUPS UP - Packets stuck in VPP queue during OOO condition if stream is in config/pre-active state	cups-up
CSCvt89273	CUPS-UP : 'show subscribers all' starOS CLI command causes Sessmgr task restarts	cups-up
CSCvw22375	[BP-CUPS] issue observed at sessmgr uplane_process_ruledef_deletion	cups-up
CSCvx60660	Task restart @ libc.so.6/__strlen_sse2_bsf()	cups-up
CSCvo47185	[BP-CUPS]Tos marked downlink pkts are counted twice in show sub cli.	cups-up
CSCvs30808	[BP-CUPS] calls disconnected with reason graceful-cleanup-on-audit-fail after srp switchover	cups-up
CSCvw25328	[BP-CUPS] Predef rule match is not happening and the corresponding pkts/bytes are getting dropped	cups-up
CSCvw73684	[CUPS UP] - Traffic Dropped with cause “R7Gx Rule-Matching Failure”	cups-up
CSCvw97725	CUPS sessmgr restart on UPFdata - smgr_uplane_config_qos_gor	cups-up
CSCvy39181	inner-fragmentation support is required if DF bit is set in the received packet	cups-up
CSCvw77581	[BP-CUPS] ruledef priority change and sx config push results in peering loss and outage	cups-up
CSCvs23558	[BP-CUPS] PC: [048dd1d7/X] smgr_uplane_handle_config_chrg_action()	cups-up
CSCvw94672	VPP restart leading to reload of node and ICSR switchover	cups-up
CSCvv87427	4G CUPS Bad behavior for ACL in SGi context	cups-up
CSCvv90937	CUPS-UP: sessmgr restart at sess_udp_mtree_lookup	cups-up
CSCvw43171	[CUPS] [PFD Management] - Inconsistent rulebase configuration between CP & UP	cups-up
CSCvw54270	CUPS sessmgr restart on UPFData sessmgr_connproxy_client_state_cb	cups-up
CSCvu27887	suppress-nrupc didn't works after upgrade to 21.17.4	ggsn
CSCvw61491	[CP-MME] Sessmgr restarts seen at sn_list_contains_element	mme
CSCvu61088	Traffic drop in certain SF cards after Nexus switch multi port failures	pdn-gw
CSCvx79042	Unexpected debug logs are observed during ICSR switchover with L2TP subscribers	pdn-gw
CSCvx80308	[BP-ICUPS]:SM restart observed on active/standby with plain callmodel	pdn-gw
CSCvy30776	Wrong CDRs are generated by PGW on receiving Secondary RAT Usage Reports in CNR	pdn-gw
CSCvy47655	Corrupted values of total/output octets displayed in CCR-U on Gy	pdn-gw
CSCvt47005	[BP-Legacy] Traffic allowed despite CCR failure with FHT continue discard traffic post recovery	pdn-gw
CSCvv90925	PGWCDRs reported with higher volume than configured limit	pdn-gw

Bug ID	Headline	Product Found*
CSCvw47620	sessmgr restart seen after upgrade to 21.17.14 on acs_remove_learnt_cname_n_ip_addresses	pdn-gw
CSCvw34433	[BP-ICUPS]Call cleared when CCRI towards OCS is sent mid-session	pdn-gw
CSCvs09553	[BP-ICUPS]: Monsub pcap file's call id not changed after context replacement	pdn-gw
CSCvq31796	[BP-ICUPS] Incorrect session count under “show gtpu stat”	pdn-gw
CSCvu51831	Not all sessmgrs came up after upgrading to 21.15.37.75871	pdn-gw
CSCvu93710	Bearer inactivity idle timer is triggered incorrectly causing incorrect idle timeout for subscribers	pdn-gw
CSCvw58221	[BP_PCT PGW] Diameter data fragmentation not working as expected	pdn-gw
CSCvv20352	[PLT-ICUPS] npumgr restart at dh_api_get_sockets_handler	pdn-gw
CSCvv64672	[BP-ICUPS]: HTTP Traffic issue observed during FOA tesing on the 21.15.x latest builds.	pdn-gw
CSCvw64863	[Smoke2-Legacy] TCP FIN/Reset are not sent post readdress rule install.	pdn-gw
CSCvw77989	Sessmgr restart while processing Secondary RAT Usage CDR records #2	pdn-gw
CSCvu85001	Cisco ASR 5000 Series Software TACACS Authorization Bypass Vulnerability	pdn-gw
CSCvv14103	vlan-npu Bulkstats data missing for all the interface except the first interface 21.19	pdn-gw
CSCvy29768	Diameter peers go down even though there is an operational LAG port due to EZChip LPM tree issue	pdn-gw
CSCvv52504	PGW not setting the IPv6 Layer Hop Limit	pdn-gw
CSCvu55467	[BP-ICUPS] Session Controller restart observed during data_backup_read_abort	pdn-gw
CSCvv02711	PGW sends APN AMBR as 1Kbps in UBReq	pdn-gw
CSCvw95793	[Smoke2-ICUPS] In Monsub fastpath pcap files are not generated as expected.	pdn-gw
CSCvu87645	Wrong value of RX counter on 'show port utilization table'	sae-gw
CSCvx62561	Observer High CPU on multiple cards with HO since 21.18.5 upgrade	sgw
CSCvy12988	Wrong CDRs are generated by SGW on receiving Secondary RAT Usage Reports	sgw
CSCvv43175	Changes inside route-map does not take effect	staros
CSCvw51050	21.14: Port speed OID changes after port up/down	staros
CSCvx07298	[CUPS / UPF / OAM / SR-IOV] Bonding not working	staros
CSCvx59032	Failure while trying to assign IPv6 127-bit prefix to interface	staros
CSCvw04670	DPC2 card failure due to IPS_ParityErrInt takes long to recover on ASR5500 node	staros
CSCvu44031	npumgr Fatal Signal 11: Segmentation fault following NPU memory error	staros
CSCvy11353	Blackholed traffic for IPv6 shared subnet without BFD (when IPv6 NS not established)	staros
CSCvy63440	Port Tx traffic not balanced across MIO cards	staros

Bug ID	Headline	Product Found*
CSCvx98495	[UPF-SVI] : sessmgr restarted at uplane_p2p_update_stats()	upf
* Information in the "Product Found" column identifies the product in which the bug was initially identified.		

Operator Notes

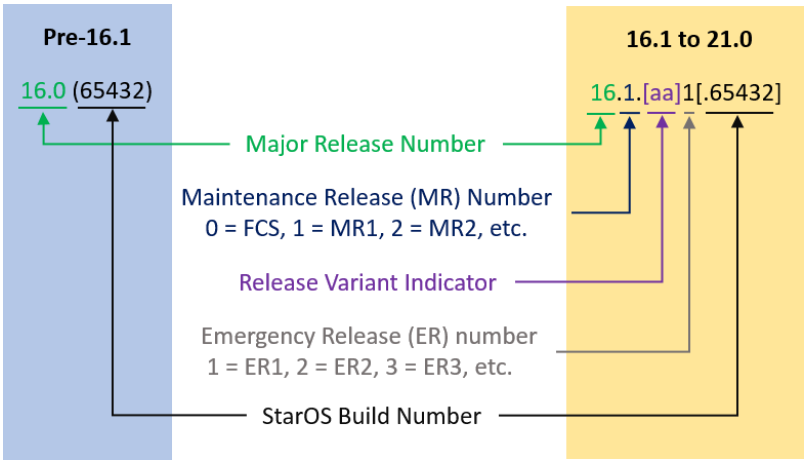
StarOS Version Numbering System

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.

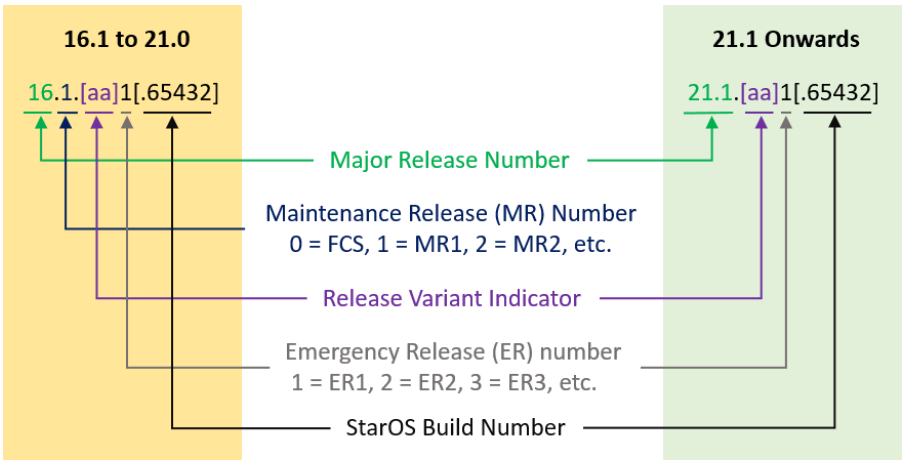
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployme nt releases also differed only in build 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 e xample "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 number ing format is a contiguous sequential number that represents incremental changes between releases. This format will facilitate identifying the changes between releases when using Bug Search Tool to research software releases.

Release Package Descriptions

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

Table 5 - Release Package Information

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
ASR 5500		
asr5500-<release>.zip	asr5500-<release>.bin	Contains the signed ASR 5500 software image, the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
asr5500_T-<release>.zip	asr5500_T-<release>.bin	Contains the signed, trusted ASR 5500 software image, the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
StarOS Companion Package		
companion-<release>.zip	companion-<release>.tgz	Contains numerous files pertaining to this version of the StarOS including SNMP MIBs, RADIUS dictionaries, ORBEM clients. These files pertain to both trusted and non-trusted build variants. In 21.12.0 and later releases, the StarOS companion package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
VPC-DI		
qvpc-di-<release>.bin.zip	qvpc-di-<release>.bin	Contains the VPC-DI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di_T-<release>.bin.zip	qvpc-di_T-<release>.bin	Contains the trusted VPC-DI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di-<release>.iso.zip	qvpc-di-<release>.iso	Contains the VPC-DI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di_T-<release>.iso.zip	qvpc-di_T-<release>.iso	Contains the trusted VPC-DI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qvpc-di-template-vmware-<release>.zip	qvpc-di-template-vmware-<release>.tgz	Contains the VPC-DI binary software image that is used to on-board the software directly into VMware. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di-template-vmware_T-<release>.zip	qvpc-di-template-vmware_T-<release>.tgz	Contains the trusted VPC-DI binary software image that is used to on-board the software directly into VMware. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di-template-libvirt-kvm-<release>.zip	qvpc-di-template-libvirt-kvm-<release>.tgz	Contains the same VPC-DI ISO identified above and additional installation files for using it on KVM. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di-template-libvirt-kvm_T-<release>.zip	qvpc-di-template-libvirt-kvm_T-<release>.tgz	Contains the same trusted VPC-DI ISO identified above and additional installation files for using it on KVM. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di-<release>.qcow2.zip	qvpc-di-<release>.qcow2.tgz	Contains the VPC-DI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di_T-<release>.qcow2.zip	qvpc-di_T-<release>.qcow2.tgz	Contains the trusted VPC-DI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
VPC-SI		
qvpc-si-<release>.bin.zip	qvpc-si-<release>.bin	Contains the VPC-SI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qvpc-si_T-<release>.bin.zip	qvpc-si_T-<release>.bin	Contains the trusted VPC-SI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-<release>.iso.zip	qvpc-si-<release>.iso	Contains the VPC-SI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si_T-<release>.iso.zip	qvpc-si_T-<release>.iso	Contains the trusted VPC-SI ISO used for new deployments a new virtual machine is manually created and configured to boot from a CD image. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-template-vmware-<release>.zip	qvpc-si-template-vmware-<release>.ova	Contains the VPC-SI binary software image that is used to on-board the software directly into VMware. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-template-vmware_T-<release>.zip	qvpc-si-template-vmware_T-<release>.ova	Contains the trusted VPC-SI binary software image that is used to on-board the software directly into VMware. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-template-libvirt-kvm-<release>.zip	qvpc-si-template-libvirt-kvm-<release>.tgz	Contains the same VPC-SI ISO identified above and additional installation files for using it on KVM. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-template-libvirt-kvm_T-<release>.zip	qvpc-si-template-libvirt-kvm_T-<release>.tgz	Contains the same trusted VPC-SI ISO identified above and additional installation files for using it on KVM. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-<release>.qcow2.zip	qvpc-si-<release>.qcow2.gz	Contains the VPC-SI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qvpc-si_T-<release>.qcow2.zip	qvpc-si_T-<release>.qcow2.gz	Contains the trusted VPC-SI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
VPC Companion Package		
companion-vpc-<release>.zip	companion-vpc-<release>.tgz	Contains numerous files pertaining to this version of the VPC including SNMP MIBs, RADIUS dictionaries, ORBEM clients. These files pertain to both VPC-DI and VPC-SI, and for trusted and non-trusted build variants. In 21.12.0 and later releases, the VPC companion package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
Ultra Service Platform		
usp-<version>.iso		The USP software package containing component RPMs (bundles). Refer to Table 6 for descriptions of the specific bundles.
usp_T-<version>.iso		The USP software package containing component RPMs (bundles). This bundle contains trusted images. Refer to Table 6 for descriptions of the specific bundles.
usp_rpm_verify_utils-<version>.tar		Contains information and utilities for verifying USP RPM integrity.

Table 6 - USP ISO Bundles

USP Bundle Name	Description
usp-em-bundle-<version>-1.x86_64.rpm*	The Element Manager (EM) Bundle RPM containing images and metadata for the Ultra Element Manager (UEM) module.
usp-ugp-bundle-<version>-1.x86_64.rpm*	The Ultra Gateway Platform (UGP) Bundle RPM containing images for Ultra Packet core (VPC-DI). There are trusted and non-trusted image variants of this bundle.
usp-yang-bundle-<version>-1.x86_64.rpm	The Yang Bundle RPM containing YANG data models including the VNFD and VNFR.
usp-uas-bundle-<version>-1.x86_64.rpm	The Ultra Automation Services Bundle RPM containing AutoVNF, Ultra Web Services (UWS), and other automation packages.
usp-auto-it-bundle-<version>-1.x86_64.rpm	The bundle containing the AutoIT packages required to deploy the UAS.
usp-vnfm-bundle-<version>-1.x86_64.rpm	The VNFM Bundle RPM containing an image and a boot-up script for ESC (Elastic Service Controller).
ultram-manager-<version>-1.x86_64.rpm*	This package contains the script and relevant files needed to deploy the Ultra M Manager Service.

* These bundles are also distributed separately from the ISO.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.