Release Notes for StarOS™ Software Version 21.20.14

First Published: April 22, 2021
Last Updated: April 22, 2021

Introduction

This Release Note identifies changes and issues related to this software release. This emergency release is based on release 21.20.13. 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	21.20.14, build 80226

Descriptions for the various packages provided with this release are located in Release Package Descriptions.

Feature and Behavior Changes

The following features and/or behavior changes have been introduced in this emergency release.

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 installation and upgrade instructions. Refer to the existing installation documentation for specific installation and upgrade considerations.

Firmware Updates

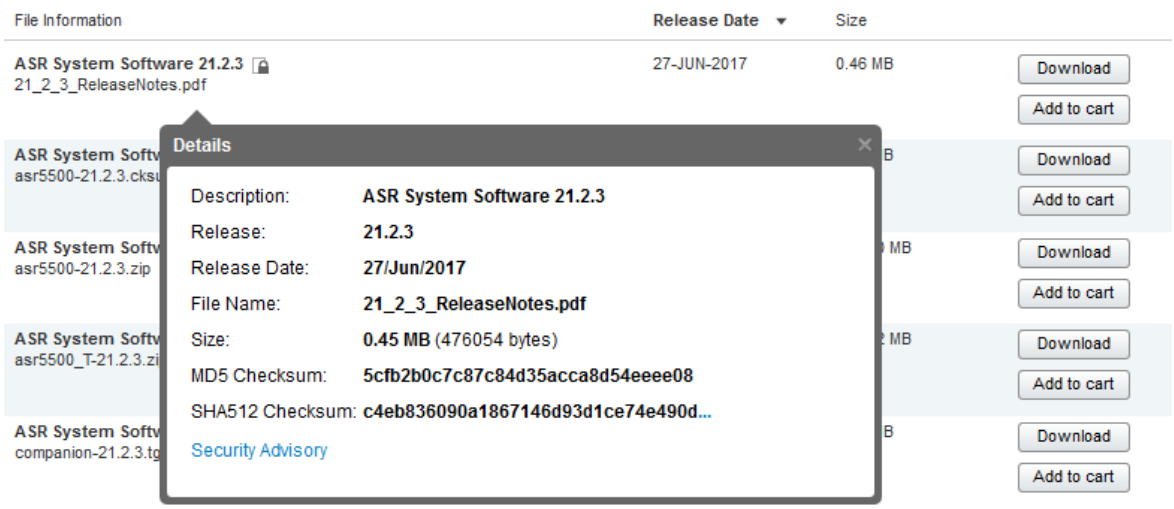
There are no firmware upgrades required for this release.

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 the following mechanisms:

- **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.

- **.cksums file:** A file containing software image checksum information is distributed with the image files. The naming convention for this file is:

  <product>-<version>.cksums

  Example: asr5500-21.4.0.cksums

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 please see the table below.

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>*

Operating System	SHA512 checksum calculation command examples

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/or that 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*
CSCvu81900	[PLT-CUPS]: huge CRR recovery failures on back-to-back SRP-Switchover leading to call-drop	cups-cp
CSCvu96189	"[BP-CUPS] After CP ICSR, USU is not encoded if there was no GSU for the MSCC"	cups-cp
CSCvu45618	[BP-CUPS] huge number of session disconnects with reason sxfail-opr-get-usagereport	cups-cp
CSCvv03378	"[BP-CUPS]: 12241: sessmgr_ggsn_fill_sub_sess_recovery_info: sgsn gtpu addr NULL callid 99c0d4,"	cups-cp
CSCvx28193	[BP-CUPS]:Assertion failure at sn_memblock_memcache_alloc() on UP ICSR	cups-up
CSCvv52658	[RCM] UP reboot didn't switchover to Stby. Instead RCM kept rebooting UPs(Act and Stby) cyclically	cups-up

Bug ID	Headline	Product Found*
CSCvv56994	[RCM] 2 Active PGW UP's reboot did not lead to Standby coming up for 1 Active UP	cups-up
CSCvu37233	Multiple Sessmgr restarts seen while doing service card migration from active to standby	mme
CSCvu81405	Revert back CSCvr34106	mme
CSCvv88515	DSReq for SOS bearers not triggered when cancel location is received	mme
CSCvu65266	Assertion failure while configuring Diameter destination realm under mme-service with context MME	mme
CSCvu81466	[MONTE Roaming] On VPC-DI while doing mmemgr restart seen 18K subs drop from total 1.4M	mme
CSCvw55120	bulkstats MME counter TAU-PERIODIC-ATTEMPTED is constantly ZERO after upgrade	mme
CSCvu80679	MME doesn't handle the Exp Result Code 5511 when received from IWK-SCEF in CIA message	mme
CSCvu82139	[CP-MME]- Post unplanned card failure diamproxy/diactrl instances went to over state	mme
CSCvv74288	N26 - TAU Reject due to E-RAB Modification Indication - Collision	mme
CSCvw62681	MME does not respond to n/w initiated dedicated Bearer creation request after ERAB Modification Ind.	mme
CSCvx98833	[CP-MME] Session manager restart at mme_app_destroy_ue_ctxt	mme
CSCvw74939	Multiple SESSMGRs in WARN/OVER state	mme
CSCvx79042	Unexpected debug logs are observed during ICSR switchover with L2TP subscribers	pdn-gw
CSCvx66200	[BP-ICUPS]:SM crashes observed on active and standby with acsmgr_deallocate_call_obj()	pdn-gw
CSCvw25217	BP-ICUPS : sessctrl crashes during boot up at acs_sanitize_a_single_tdb	pdn-gw
CSCvw76775	Many sessmgr restarts seen on virtual PGW	pdn-gw
CSCvx22943	Monitor DCH FIFO Discards in the FE600 health check	Staros
CSCvw72152	Task Resources - Session Manager and bulkstats in Warn Status on UPF.	Upf
CSCvw65922	[UPF-SVI] Negative case - Removing ip vrf <vrf-name> cli --> huge no of continuous VPNMGR restarts	Upf
CSCvw56143	UPF cpu utilization at 100% with 230K calls and close to 8Gbps throughput	Upf
CSCvw48604	[UPF-SVI] Active UPF is losing IP Chunks allocated by SMF after ICSR Switchover but recovering later	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*
CSCvu22351	[BP-CUPS] CLI process restarts when configuring default timeout for LI tcp connection-retry-timer	cups-cp
CSCvx56945	[BP-CUPS] CDR not getting generated upon context replacement	cups-cp
CSCvx59968	CP sends wrong APN-AMBR (MBR) in QER in PFCP session modification request messages	cups-cp
CSCvx60660	Task restart @ libc.so.6/__strlen_sse2_bsf()	cups-up
CSCvu59361	TEID Collision with ULI Change feature triggered during 4G->3G handoffs when subscriber is roaming	ggsn
CSCvv31388	Frequent Sessionmgr Assertion failure	mme
CSCvx47164	Restart for function mme_app_hss_if_cb_func()	mme
CSCvv49652	EIA3/EEA3 broken	mme
CSCvw53493	MME sends MBCmd for incorrect bearer after ISDR	mme
CSCvv44990	Wrong appiarance order of Ext-APN-AMBR IE leds to inability to recognise PCO	mme
CSCvu65256	MME is sending cause misc: Unspecified for e-RAB ID 7 in PathSwitch Req Ack message during X2 HO	mme
CSCvv28217	Session manager restart wile encoding QOS on PDP	mme
CSCvw74939	Multiple SESSMGRs in WARN/OVER state	mme
CSCvu90470	Fatal Signal 11: Segmentation fault mme_hss_request_fill_data_UPDATE_LOCATION	mme
CSCvv64138	sessmgr restart in function: egtpc_allocate_new_bearers	mme
CSCvv82191	Multiple paging/CS serv notific from MME after receiving Ext Serv Req with cause CSFB Reject from UE	mme
CSCvt34756	"EPC: MME, Reversed_message_order_ULR_CSReq_In_case_GUTI_Attach"	mme
CSCvw51877	[BP-ICUPS]:Sessmgr carshes observed on active and standby chassis	pdn-gw
CSCvx96693	VPP buffer leak when drops due to interna 1973 is seen	pdn-gw
CSCvy05857	BP-ICUPS: Sessmgr reloads observed when LI related show commands are executed on a loaded chassis	pdn-gw
CSCvt05716	Sessmgr process restart in TCP packet processing path	pdn-gw
CSCvu77779	PGW didn't send CCR-U when user moves from Eutran to WLAN	pdn-gw
CSCvv36310	IP Bad checksum with Rewrite TTL on Downlink Packets feature	pdn-gw

Bug ID	Headline	Product Found*
CSCvu72697	aaamgr restart with PC: [ffffe430/X] __kernel_vsyscall()	pdn-gw
CSCvx80308	[BP-ICUPS]:SM restart observed on active/standby with plain callmodel	pdn-gw
CSCvx45748	sessmgr allocates Chg-ID from start after smgr restart if old PDN with close to max value exists	sae-gw
CSCvw45500	S4 association configuration disappeares after demux card restart	sgsn
CSCvx44868	sessmgr restart seen with Function: SmGenSuspendReq	sgsn
CSCvu23258	Sessctrl restart observed at fuction sctr_handle_smgr_msg_xfr_failure_internal()	sgsn
CSCvv69506	ASR5500 - SGSN/MME - map-service name is truncated to 8 characters	sgsn
* Information in the "Product Found" column identifies the product in which the bug was initially identified.		

Operator Notes

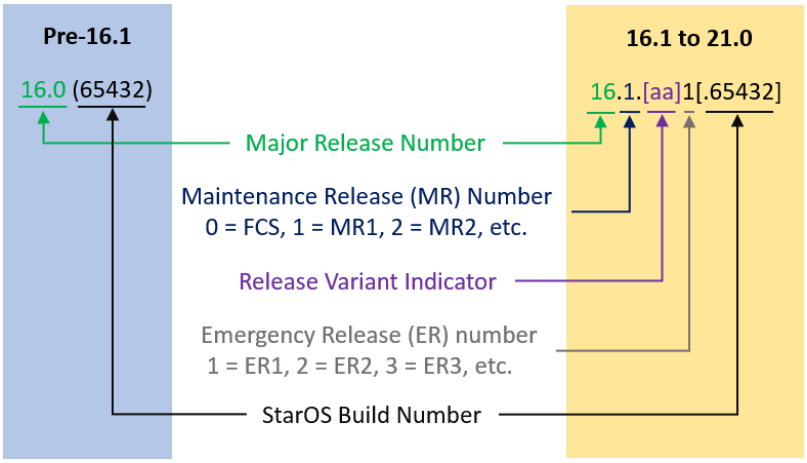
StarOS Version Numbering System

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.

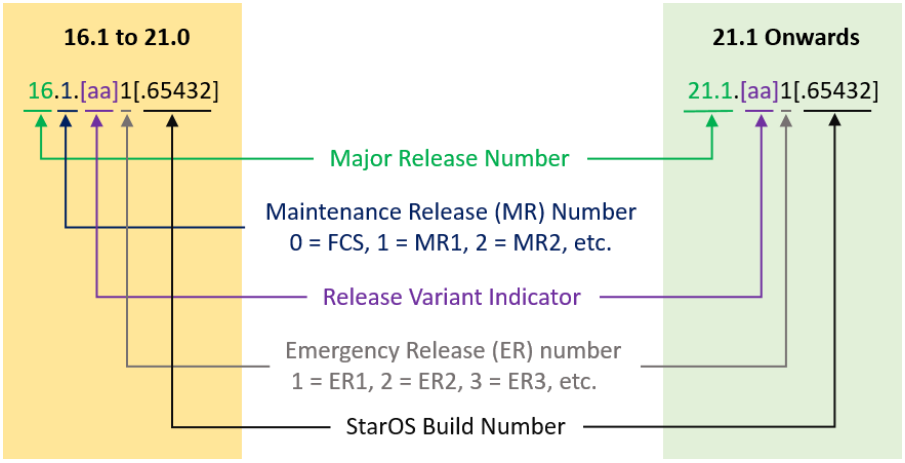
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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

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

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

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

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.