Release Notes for StarOS™ Software Version 21.11.9

First Published: November 11, 2019
Last Updated: November 11, 2019

Introduction

This Release Notes identify changes and issues related to this software release. This emergency release is based on release 21.11.8. This Release Notes is applicable to the ASR5500, VPC-SI, and VPC-DI platforms.

Release Package Version Information

Software Packages	Version
StarOS packages	21.11.9, build 73403

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

Feature and Behavior Changes

Ther 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 the software release on which this emergency release is based.

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

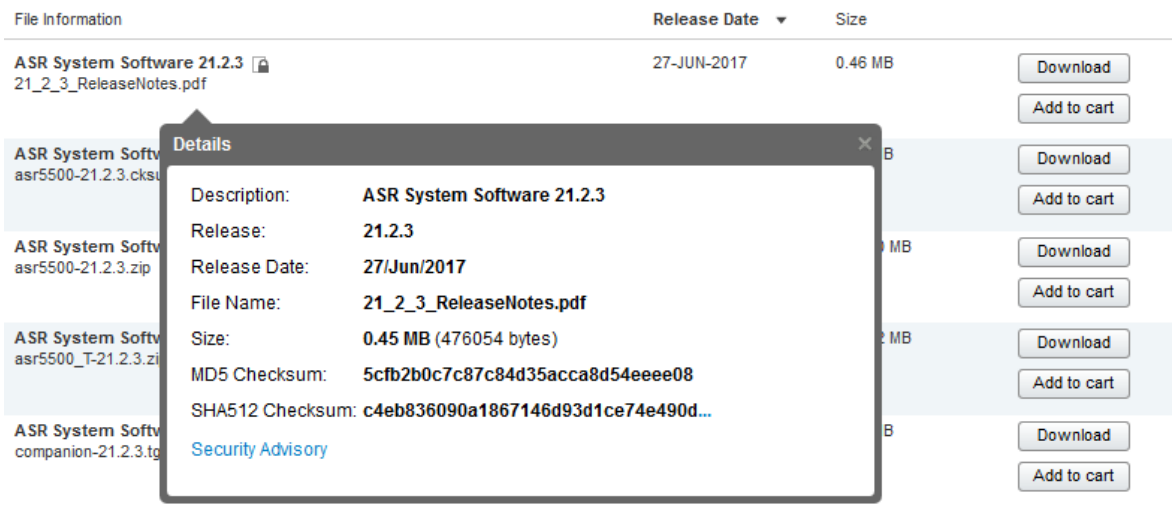
There are no firmware upgrades required for this release.

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 1 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 1 – 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>*

Operating System	SHA512 checksum calculation command examples
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 th e Cisco Technical Assistance Center.

Certificate Validation

StarOS software images are signed via x509 certificates. Please view the .README file packaged with the software for informat ion and instructions on how to validate the certificates.

NOTE: Image signing is not currently supported for VPC-SI and/or VPC-DI software packages.

Open Bugs for This Release

The table below highlights 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.

Bug ID	Headline	Product Found*
CSCvm83524	[BP-CUPS] Assert failure at egtpc_handle_user_sap_event()	cups-cp
CSCvk63958	[PLT-CUPS-ICUPS-VPP]Single user performance blocked due to VPP_MAIN is in over state	cups-up
CSCvn14097	[BP-CUPS] Access Type of Pure-S call is displayed as 'Unknown'	cups-up
CSCvn14202	[BP-CUPS-VPP]Delay charging is having issues with Tear Down packets.	cups-up
CSCvn39767	Unexpected session manager restart- _do_acs_usertcp_event_handler()	pdn-gw
CSCvo32237	[BP-ICUPS]: some UDP streams going to passive post ICSR switchover	pdn-gw
CSCvm65884	PGW-Around 5% increase in sessmgr memory in 21.11.M0.70658 wrt 21.9.M0.69679 baseline CEPS test	pdn-gw
CSCvm83968	[CUSP] need to handle interworking of URL-readdressing and CUSP feature.	pdn-gw
CSCvp03633	'Accounting-Request' counter is not getting pegged if response from RADIUS server is missing	pdn-gw
CSCvm82008	[BP-ICUPS]:HTTP volume based offload is not happening after PDN update	sae-gw
CSCvn35333	[BP-ICUPS] uplinkdata and downlinkdata volume values are not correct in PGWCDR after XHDR insertion	sae-gw
CSCvn76706	Sessmgr restarts observed in Cisco ASR5500 after starting the callmodel	sae-gw

Bug ID	Headline	Product Found*
CSCvi12541	bfdlc facility instances in warn state on active and standby chassis	sae-gw
CSCvr99166	[MME-SGSN]- Frequent Sessmgr restart seen with sgsn_app_sm_config	sgsn
CSCvn23275	[PLT-ICUPS] Both DPC2 rebooted upon planned migration	staros
CSCvm98426	[PLT-ICUPS-VPP] Not able to send fragmented packet through VPP.	staros
CSCvp63312	confdmgr restart on DI reload	staros
* Information in the "Product Found" column identifies the product in which the bug was initially identified.		

Resolved Bugs for This Release

The table below highlights 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.

Bug ID	Headline	Product Found*
CSCvo74521	MME isn't handling properly APN Configuration received in ISD from HSS	mme
CSCvq63501	MME does not send MME Config Update after active SF card migration	mme
CSCvq77876	Assertion Failure in sn_aaa_session_set_user_data()	mme
CSCvk54439	MME doesn't send ESM Notification for IMS session re-establishment	mme
CSCvq03879	Single-registration-indication flag not set in case of 4G->3G->4G PS-HO	mme
CSCvq17864	Multiple sessmgr restart with function mme_app_apply_sgw_blacklist()	mme
CSCvr43199	sgw blacklisting deleting pgw pair by error	mme
CSCvn09785	sessmgr restart after modify ECS configuration	pdn-gw
CSCvp35767	SRP connection fluctuations and continuous restart of Orbs task	pdn-gw
CSCvq00562	[VPC-DI] Demux IPv6 TCP large packet handling broken.	pdn-gw
CSCve75890	CCR-I message not failing over with session-failover configured	pdn-gw
CSCvp37159	Duplicated sessstat-pdn-dcnr-cumulative-activated instead of sessstat-pdn-dcnr-cumulative-dectivated	pdn-gw
CSCvp91000	SM fail due to Fatal Signal on s4_smn_handle_srns_new_sgsn_abort_mbr	sgsn
CSCvq63005	Gbmgr restart seen on gbmgr_rx_gns_pdu	sgsn
CSCvr05830	session manager restarts during egtp handling	sgsn
CSCvr34833	sessmgr assertion failure in pmm_ms_fsm_invalid_event_handler	sgsn
CSCvo42076	SM fail due to Fatal Signal on s4_smn_handle_srns_new_sgsn_abort_mbr	sgsn
CSCvo64397	Invalid Event NTWK-MODIFY-REQUEST from SM-APP in NTWK-REMOTE-HANDOFF-IN-PROGRESS-IN-INACTIVE state	sgsn
CSCvr00128	Assertion failure at sess/aaamgr/aaamgr_api.c	sgsn

Bug ID	Headline	Product Found*
CSCvo37389	sessmgr/diamproxy mapping mismatch after DPC migration	staros
CSCvo46728	random BFD sessions do NOT comeup at time of VNF reload - Flap peer leaf interface to re-cover	staros
CSCvo70530	SAEGW-VPC-DI- Sw Version 21.12.0 - MTU higher than Default value not working correctly	staros
CSCvp06026	VPC-DI NAT keepalive packets should be dropped.	staros
CSCvp23541	[VPC-DI] CF switchover failure due to cspctrl assert.	staros
CSCvp27624	[VPC-DI] Unnecessary CF hatcpu failure	staros
CSCvp75465	[VPC-DI] Restrict use of transparent huge pages on CFC	staros
CSCvq11482	QVPC-DI-Disable Multi Segment mbuf	staros
CSCvq19559	Wrong values on show port utilization table - StarOS VPC-DI	staros
CSCvr45783	Most of Service ports showing zero traffic after StarOS reload	staros
CSCvq46641	AFIO is leaking a file descriptor whenever it collects a register dump from a device	staros
* Information in the "Product Found" column identifies the product in which the bug was initially identified.		

Operator Notes

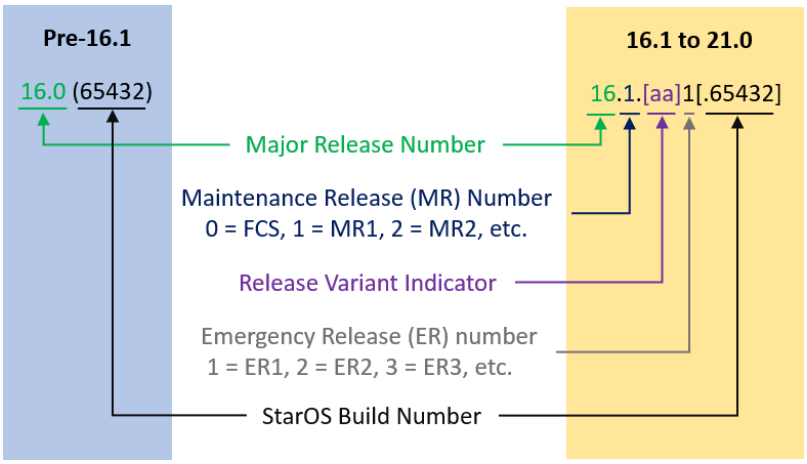
StarOS Version Numbering System

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.

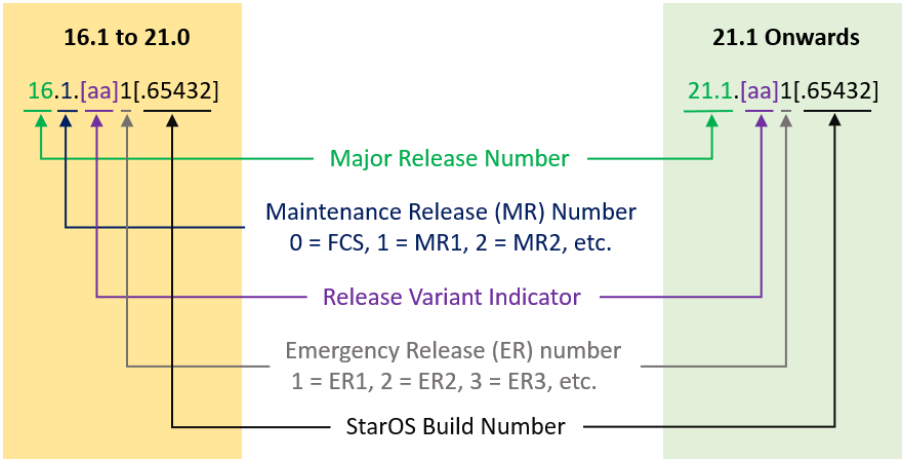
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build 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 identifyi ng the changes between releases when using Bug Search Tool to research software releases.

Release Package Descriptions

Table 2 lists provides descriptions for the packages that are available with this release.

Table 2 - Release Package Information

Package	Description
ASR 5500	
asr5500-<release>.bin	A zip file containing 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>.bin	A zip file containing 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.
VPC-DI	

Package	Description
qvpc-di-<release>.bin	The VPC-DI binary software image which is used to replace a previously deployed image on the flash disk in existing installations.
qvpc-di_T-<release>.bin	The trusted VPC-DI binary software image which is used to replace a previously deployed image on the flash disk in existing installations.
qvpc-di-<release>.iso	The VPC-DI ISO used for new deployments a new virtual machine is manually created and configured to boot from a CD image.
qvpc-di_T-<release>.iso	The trusted VPC-DI ISO used for new deployments a new virtual machine is manually created and configured to boot from a CD image.
qvpc-di-template-vmware-<release>.tgz	The VPC-DI binary software image that is used to on-board the software directly into Vmware.
qvpc-di-template-vmware_T-<release>.tgz	The trusted VPC-DI binary software image that is used to on-board the software directly into Vmware.
qvpc-di-template-libvirt-kvm-<release>.tgz	This is an archive that includes the same VPC-DI ISO identified above, but additional installation files for using it on KVM.
qvpc-di-template-libvirt-kvm_T-<release>.tgz	This is an archive that includes the same trusted VPC-DI ISO identified above, but additional installation files for using it on KVM.
qvpc-di-<release>.qcow2.tgz	The VPC-DI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack.
qvpc-di_T-<release>.qcow2.tgz	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.
VPC-SI	
qvpc-si-<release>.bin	The VPC-SI binary software image which is used to replace a previously deployed image on the flash disk in existing installations.
qvpc-si_T-<release>.bin	The trusted VPC-SI binary software image which is used to replace a previously deployed image on the flash disk in existing installations.
qvpc-si-<release>.iso	The VPC-SI ISO used for new deployments a new virtual machine is manually created and configured to boot from a CD image.
qvpc-si_T-<release>.iso	The trusted VPC-SI ISO used for new deployments a new virtual machine is manually created and configured to boot from a CD image.
qvpc-si-template-vmware-<release>.ova	The VPC-SI binary software image that is used to on-board the software directly into Vmware.
qvpc-si-template-vmware_T-<release>.ova	The trusted VPC-SI binary software image that is used to on-board the software directly into Vmware.
qvpc-si-template-libvirt-kvm-<release>.tgz	This is an archive that includes the same VPC-SI ISO identified above, but additional installation files for using it on KVM.
qvpc-si-template-libvirt-kvm_T-<release>.tgz	This is an archive that includes the same trusted VPC-SI ISO identified above, but additional installation files for using it on KVM.
qvpc-si-<release>.qcow2.gz	The VPC-SI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack.

Package	Description
qvpc-si_T-<release>.qcow2.gz	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.
StarOS Companion Package	
companion-<release>.tgz	An archive containing 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.

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.