Release Notes for StarOS™ Software Version 21.9.3

First Published: Oct 16,2018
Last Updated: Oct 16, 2018

Introduction

These Release Notes identify changes and issues related to this software release. This emergency release is based on release 21.9.2. These release notes are applicable to the ASR 5500,VPC-SI and VPC-DI platforms.

Release Package Version Information

Software Packages	Version
StarOS packages	21.9.3 build 70453

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 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

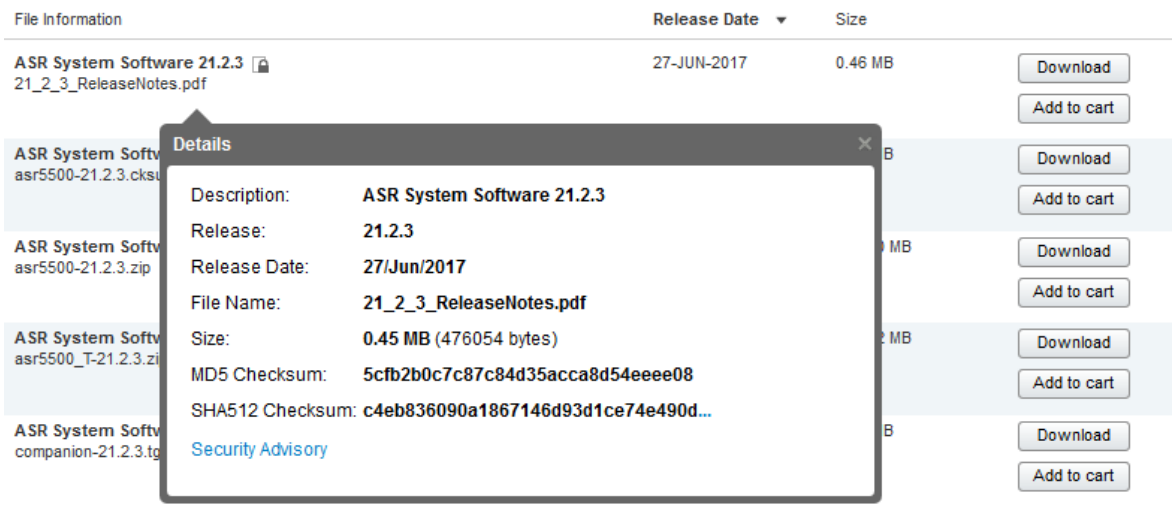
There are no firmware upgrades required for this release.

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 the Cisco Technical Assistance Center.

Certificate Validation

StarOS software images are signed via x509 certificates. Please view the .README file packaged with the software for information 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*
CSCvk13379	[BP-CUPS]Sessmgr reload is observed on PGW Control Plane while sending Sx Session Reporting Request	cups-cp
CSCvk13391	[BP-CUPS] Sessmgr in over state with dedicated bearer	cups-cp
CSCvk48006	[BP-CUPS]: Behaviour on Sx PFD messages timeout - UP stuck in Not configured state	cups-cp
CSCvk17716	[BP-CUPS] On UBRes failure for Dynamic rule modification URRs getting removed for default Bearer	cups-cp
CSCvk42558	[BP-CUPS-VPP] Facility sessctrl restart: sn_msg_call_internal()	cups-cp
CSCvj90659	[BP-CUPS]sponsorIdentity parameter not populated in GTPP Custom35 CDR.	cups-cp
CSCvj93186	BP-CUPS: AFCID not seen in CDR for custom35 dictionary	cups-cp
CSCvk54440	StarOS 21.9 release does not contain the unittest for the traps with ifIndexes from 1357 to 1360	cups-cp

Bug ID	Headline	Product Found*
CSCvi53376	[BP-CUPS]: Session Manager reload at smgr_uplane_config_rule_options on Cisco PGW	cups-up
CSCvk21427	[BP-CUPS-VPP] Seg Fault at sessmgr_up_fapi_handle_stats_update()	cups-up
CSCvk27851	[BP-CUPS-VPP]: sxdemux process restarts every 6 mins	cups-up
CSCvk29167	[PLT-CUPS-VPP]: vpp stops on UP with 24 sessmgr	cups-up
CSCvk39591	[BP-CUPS-VPP] Segmentation fault at uplane_reset_saved_pdr_match_info on VPP Testbed	cups-up
CSCvk47500	[BP-CUPS-VPP] RS packet handling is incorrect in VPP fastpath.	cups-up
CSCvj76251	[PLT-CUPS-VPP]: vpp_main in 'over' state with single subscriber 8Mbps data	cups-up
CSCvj77802	[BP-CUPS]: show subscriber data-rate not showing correct values	cups-up
CSCvj81306	[BP-CUPS]: [sessmgr 12341 error] [SXAB] Update PDR not found with PDR ID 0x7	cups-up
CSCvj90571	[BP-CUPS] USAGE REPORT not sent in SxModResp even if QUERY URR is received in SxModReq	cups-up
CSCvk05490	[PLT-CUPS-VPP]: [sessmgr 0 error] Timeout Processing: Time out, MSG ID: 8790, wheel Slot Id: 68	cups-up
CSCvk37888	[BP-CUPS-VPP] Post rule modification all packets come to smu, stream is passive.	cups-up
CSCvk39031	[BP-CUPS-VPP] TOS not getting applied on d/l inner packet from qci qos mapping table.	cups-up
CSCvk40097	[BP-CUPS]: Sessmgr restarted with sn_slist_remove_by_key	cups-up
CSCvk42806	[BP-CUPS-VPP] Drop stream is not getting onloaded on installing high priority rule.	cups-up
CSCvk46857	[PLT-CUPS-VPP]: vpnmgr restart while removing crp config	cups-up
CSCvj93176	BP-CUPS: packetCount is not incremented for R10 ULI change or Qos change	cups-up
CSCvk53594	mmemgr Restart at free_acct	mme

Bug ID	Headline	Product Found*
CSCvm83704	egtpinmgr restart when MIO switchover happened	pdn-gw
CSCvk13327	SRP service not working when traffic is routed via two default route, 2nd default not reachable	pdn-gw
CSCvk34087	NAT IPs lost after session recovery when port-chunk-size is configured with higher values	pdn-gw
CSCvk36855	Sessmgr Restart at access_get_nw_to_ms_gmm_stats_type	sgsn
CSCvk05521	21.9_69629_5GNSA: Activate DCNR counters incrementing for Non-5GNSA PDP contexts	sgsn
CSCvk07083	21.9.69633 Assertion Failure in Function: s4_sessmgr_gprs_fsm_pdp_cleanup_with_egtp_abort	sgsn
CSCvk54113	Assertion failure at sess/sgsn/sgsn-app/gtp_c/gtapp_enc_ie	sgsn
CSCvk43563	Indirect Data tunnelling stats not updating after call is cleared on SGW.	sgw
CSCvm73155	Unable to update module p2p after unplanned DPC migration	staros
CSCvj77813	show active-charging edr-udr-file statistics causing cli task restart	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*
CSCvm67581	sessmgr restart at tfTcpCompleteClose during Callmodel run testing	pdn-gw
CSCvm57152	P2P: acsmgr_p2p_init_statistics_counters - Setting Up P2P Stats Resource failed	pdn-gw
CSCvm63606	VPNMGR restarts observed when TACACS is not reachable.	sae-gw
CSCvm34045	Few SF cards in booting state in VNFs in C2.1 deployment model	staros
CSCvm58137	SF stuck in booting state - DI-Net bonding not functioning	staros

Bug ID	Headline	Product Found*
CSCvm81402	SFTP Public Key authentication is failing.	staros
* Information in the "Product Found" column identifies the product in which the bug was initially identified.		

Operator Notes

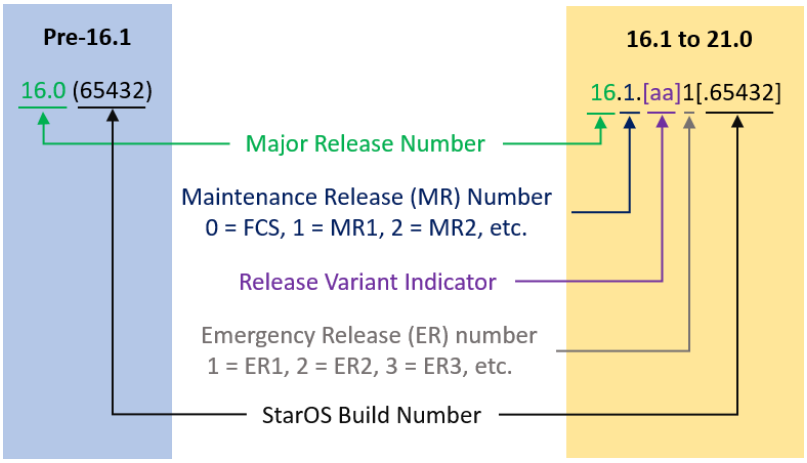
StarOS Version Numbering System

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.

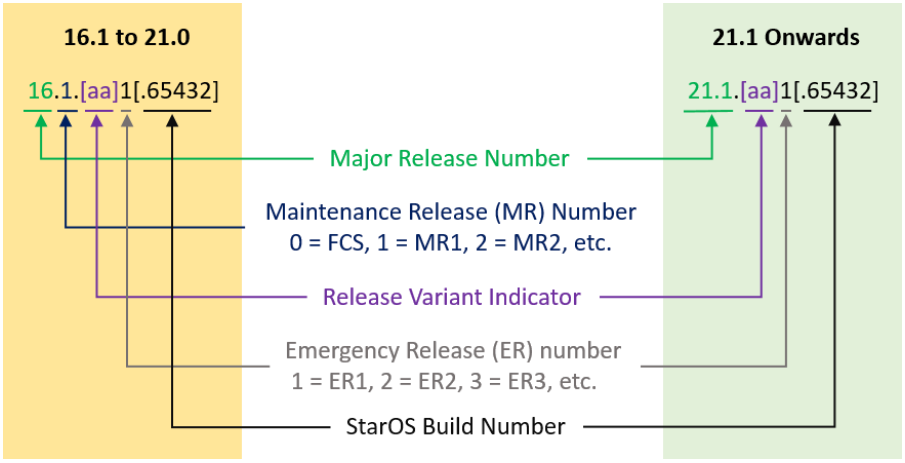
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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

Package	Description
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.
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.

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 are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.