Release Notes for StarOS™ Software Version 21.6.13

First Published: Jan 31,2019
Last Updated: Jan 31, 2019

Introduction

These Release Notes identify changes and issues related to this software release. This emergency release is based on release 21.6.12. These release notes are applicable to the ASR 5500, VPC-SI and VPC-DI platforms.

Release Package Version Information

Software Packages	Version
StarOS packages	21.6.13 build# 71139

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

Feature and Behavior Changes

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

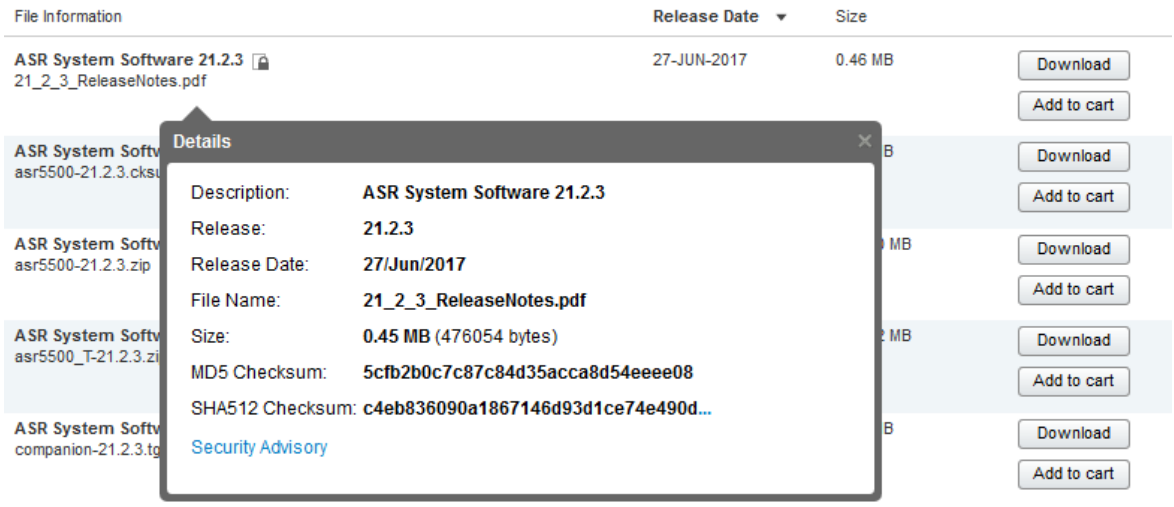
There are no firmware upgrades required for this release.

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*
CSCvk10055	Task restart while handling delete bearer.	epdg
CSCvh67114	sessmgr restarts at function egtpc_validate_context_ack_rsp_evt	mme
CSCvh82217	sessmgr task restart during MME start Auth procedure.	mme
CSCvj40660	MME to support 10KB pkt size on Sbc interface	mme
CSCvm21245	Ghost enodeB associations after CSCvf74768	mme
CSCvo06510	MME assert in Forward Relocation Complete procedure	mme
CSCvi06043	aaamgr restarted multiple times on srp switch-over	pdn-gw
CSCvg95957	Single instance of Bulkstat facility restart seen on active CISCO ASR5500	pdn-gw
CSCvh67681	20% SM CPU increase when Traffic Optim is enabled with 100% heavy session in single event perf test	pdn-gw
CSCvk29371	bgtpc peer-salvation keyword is missing under context level configuration	pdn-gw

Bug ID	Headline	Product Found*
CSCvk52505	"Crypto map configuration on interface rejected, when maximum number of ikev1 ipsecmgr tasks reached"	pdn-gw
CSCvm47811	Adding debug info to understand restart counter change from SGW causing PGW to mark sessions down	pdn-gw
CSCvm93977	Inconsistency between AAAAccServerUnreachable and AAAAccSvrUnreachable causing SNMP trap issues	pdn-gw
CSCvi06491	The default behaviour of diameter encode-supported-features has changed in 21.7	pdn-gw
CSCvm19430	NAT64 ipv6 fragment header identification field always zero	pdn-gw
CSCvi66788	VPC-DI incorrectly reports Standby SF when N+1 count is less	sae-gw
CSCvg77087	XL - GGSN/SAE-GW on VPC-DI - aaamgr in Active CF card in Memory warn state	sae-gw
CSCvh64982	Planned SRP switchover followed by switchover due to BGP failure - aaamgr restarts	sae-gw
CSCvj48443	Cisco SAEGW sends incorrect ARP value after a IDFT procedure in DDN towards MME	sae-gw
CSCvi50398	core file size limited to 2048 bytes in VPC resulting in core file transfer failure	staros
CSCvh54162	[ePDG] performing iftask restart is causing SF to restart on ultraM with servicemode as epdg	staros
CSCvh68111	The beakerd process has a memory leak	staros
CSCvi65014	Restart of vpnmgr task adversely affecting the connectivity.	staros
CSCvh84131	defaut mcdma latency is 0 leading to inefficiency	staros
CSCvh99381	SDR cli output shows all Enaled/Disabled command at all times.	staros
CSCvi44228	Incorrect time format for msg-format rfc5424	staros
CSCvm73155	Unable to update module p2p after unplanned DPC migration	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*
CSCvk35798	Sessmgr task restart at egtpc_handle_bearer_res_cmd_req_evt	mme
CSCvm76444	SM restart occured due to Assertion failure on sn_gt_encode_bss_container_ie	mme
CSCvm78020	SM fail due to Assertion failure at egtpc_validate_evt	mme
CSCvm94595	SM fails at egtpc_handle_user_sap_event	mme
CSCvn74172	SM restarts due to Segmentation fault at egtpc_get_ebi_info_from_pdu during S1 HO	mme
CSCvj72476	sm restarts on assert at mme_abort_procedure	mme
CSCvj92869	sessmgr restart due to assertion failure at sess/mme/mme-app/app/mme_msg_utils.c	mme
CSCvm44685	Framed-Route not added in the routing table	pdn-gw
CSCvn33779	nexthop-forwarding-address in charging-action does not work for L4 OOO packets	pdn-gw
CSCvk34024	CLI process in loop and restarts after the command show ip bgp vpnv4 all	sae-gw
CSCvk30462	sessmgr restart on function egtpc_handle_user_sap_event	sgsn
CSCvm87438	SM restarts while getting subscriber summary	sgsn
CSCvn31717	sessmgr restart on s4_smn_send_egtpc_pdn_local_purge	sgsn
CSCvh03512	Task restart while handling bearer info command	sgsn
CSCvn06408	sessctrl restart when configuring and unconfiguring 'imsi-range' frequently	sgsn
CSCvi63286	Throughput capped at 9.6 Gbps in SI	staros
CSCvm94917	iftask out of memory	staros
CSCvn02827	On DeMux Host reboot two additional SFs reset in the VNF	staros
CSCvn02929	3 digit MNC with specific MCC are incorrectly treated in NAI of user-name in AAR	staros
CSCvn18519	StarOS DNS Client Issue with Fragmented Packets	staros
CSCvn19507	IPv6 BFD - cross - sessions down after triggering EEM script on leaf	staros
CSCvn49958	sf card migration takes more than 600 seconds	staros

* Information in the “Product Found” column identifies the product in which the bug was initially identified.

Operator Notes

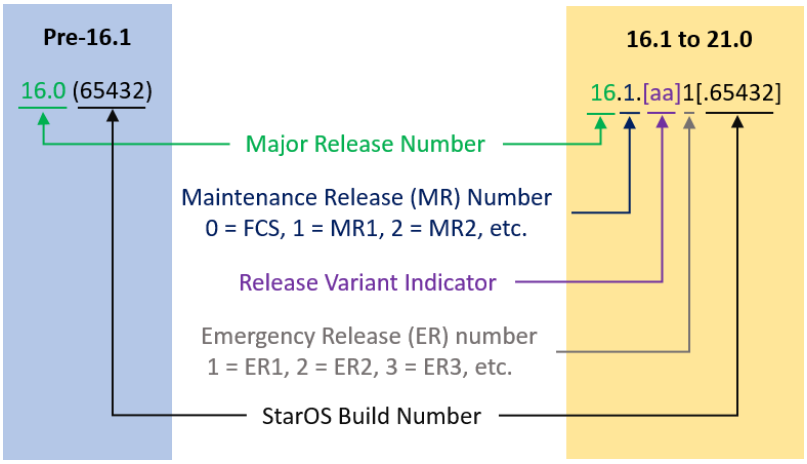
StarOS Version Numbering System

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.

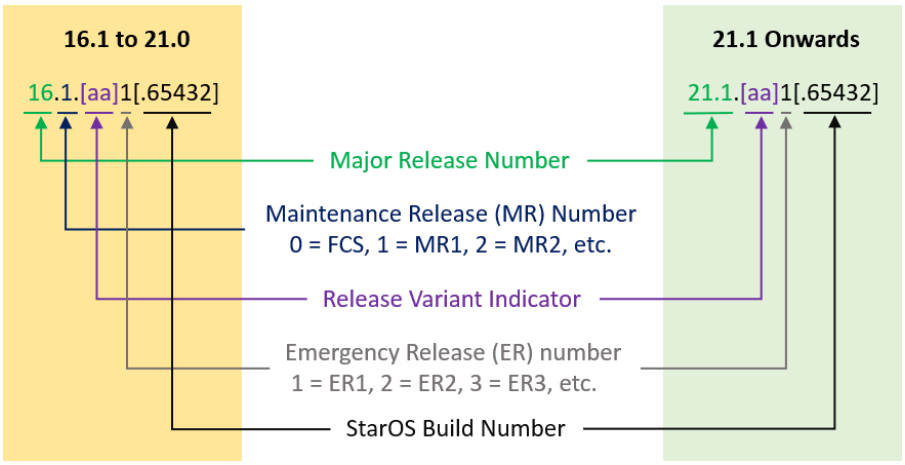
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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

Package	Description
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.