Release Notes for StarOS™ Software Version 21.6.14

First Published: May 30, 2019
Last Updated: May 30, 2019

Introduction

This Release Note identifies the resolved/fixed and unresolved/open bugs that are related to 21.6.14 StarOS Release.

Release Package Version Information

Software Packages	Version
StarOS packages	21.6.14, build 72024

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 this software release.

Related Documentation

For a complete list of documentation available for this release, go to:

- StarOS: https://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

This software release includes a firmware upgrade for the Board Control FPGA (BCF) on the ASR 5500 MIO card.

- Previous BCF version: 4.1.0

- New BCF version: 4.8.0

The new BCF firmware version provides:

- A 60 second lockout upon lowering the ejector sub-handle (interlock). Failures were observed in the field where an MIO that was being removed attempted to become Active as it was being removed. The remaining MIO would then go Standby causing a chassis failure. Now after the front panel ejector subhandle (interlock) is moved to the down position, the MIO is locked out for a period of 60 seconds and cannot become Active from the Standby state.

- A MIO reset and power down sequence when a BCF firmware upgrade is requested. A field failure was observed when an MIO with a lower revision of BCF firmware was installed in a chassis. The process of upgrading this BCF firmware on the new MIO caused inconsistencies on the chassis fabric signals which lead to other cards being reset. Upon receiving a request to reload the BCF firmware image from a newly programmed PROM, the BCF now first triggers a reset of all devices on the MIO card. After a short period of time the BCF powers the MIO card down for several seconds before the request to reload from PROM is performed.

- Improved the use of MIO presence pins to reduce the chance of incorrect Active state changes. This change affected the use of both the MIOs presence pins. Additionally, a signal filter was added to both MIOs presence pins to prevent false MIO state changes, such as during removal of inserts.

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.
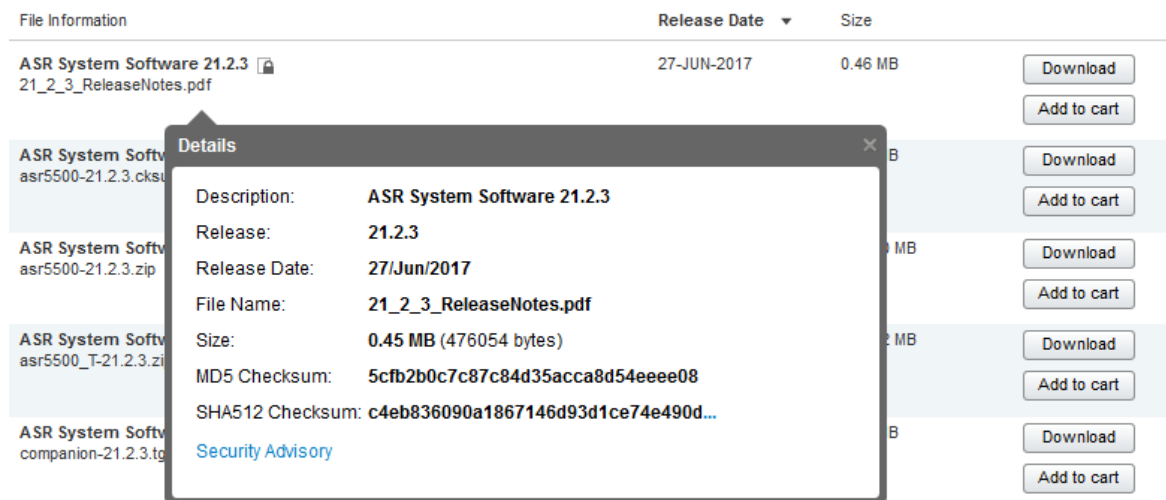
At the bottom you find the SHA512 checksum, if you do not see the whole checksum you can expand it by pressing the "..." at the end.

To validate the information, calculate a SHA512 checksum using the information in Table 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>*

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. USP ISO images are signed with a GPG key. 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 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*
CSCvh67114	sessmgr restarts at function egtpc_validate_context_ack_rsp_evt	mme
CSCvh82217	sessmgr task restart during MME start Auth procedure.	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

Bug ID	Headline	Product Found*
CSCvi06491	The default behaviour of diameter encode-supported-features has changed in 21.7	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
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
* 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*
CSCvn98394	SaMOG not sending 'Mobile-Node-Identifier' or 'EAP-Identity' for mn-nai AVP	samog
CSCvh23199	S4 SGSN rejecting forward relocation request for non standard QCI	sgsn
CSCvo42076	SM fail due to Fatal Signal on s4_smn_handle_srns_new_sgsn_abort_mbr	sgsn
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
CSCvn67152	VPC-DI/XL710: Fix port statistic collection time intervals.	staros
CSCvo70948	"push 133076 error; vpnmgr Error reading socket -1,errno 9: Bad file descriptor"	staros
CSCvp23541	[VPC-DI] CF switchover failure due to cspctrl assert.	staros
CSCvp27624	[VPC-DI] Unnecessary CF hatcpu failure	staros

| Bug ID	Headline	Product Found*
CSCvp75465	[VPC-DI] Restrict use of transparent huge pages on CFC	staros
CSCvn94836	VPC-DI: iftask double count for di_tx traffic	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".
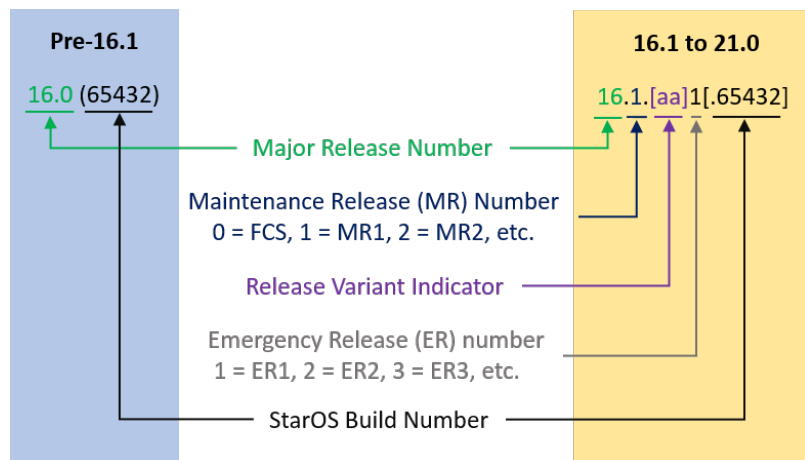
The Version Build Number for releases 21.1 and later include a major and emergency release number, for example, "21.1.1".
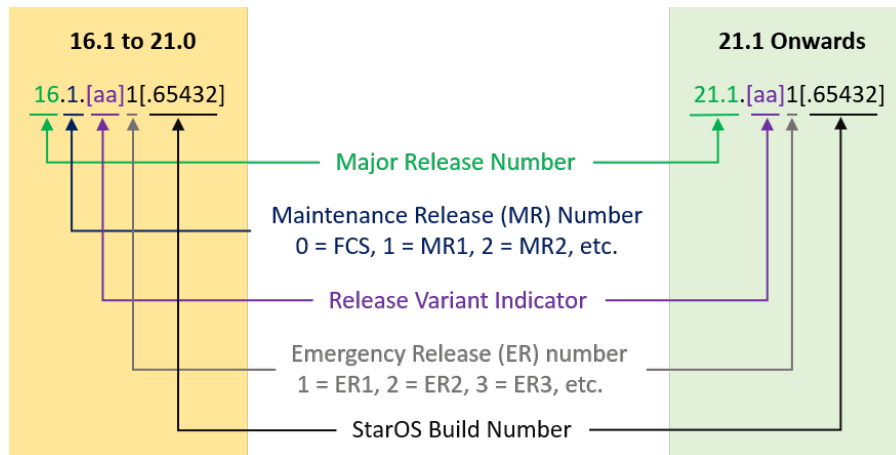
In either scenario, the appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format will facilitate identifying the changes between releases when using 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.

Package	Description
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.
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.