Release Notes for StarOS™ Software Version 21.10.1

First Published: November 5, 2018
Last Updated: November 5, 2018

Introduction

This Release Notes identify changes and issues related to this software release. This emergency release is based on release 21.10.0. This Release Notes is applicable to the ASR5500, VPC-SI, and VPC-DI platforms.

Release Package Version Information

Software Packages	Version
StarOS packages	21.10.1, build 70607

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

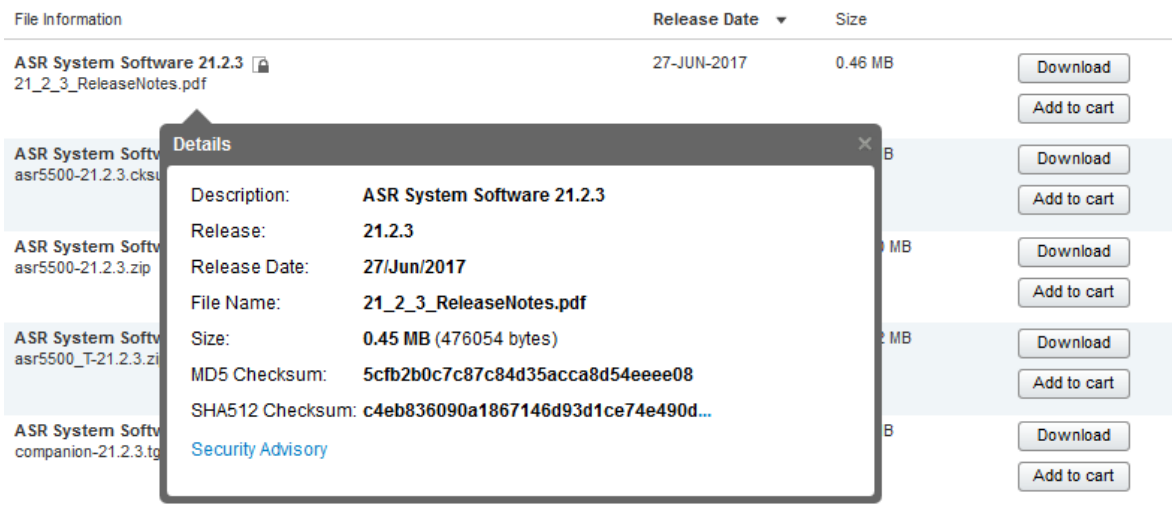
There are no firmware upgrades required for this release.

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 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*
CSCvk52151	[BP-CUPS]: Huge session disconnect with reason sx-cntxt-not-found	cups-cp
CSCvm48160	[PLT-CUPS] chmgr restart unhandled sn_event_file's in migrating proclet chmgr	cups-cp
CSCvi53376	[BP-CUPS]: Session Manager reload at smgr_uplane_config_rule_options on Cisco PGW	cups-up
CSCvk52159	[BP-CUPS]: huge session disconnect with reason sx-mand-ie-incorrect	cups-up
CSCvk56280	[BP-CUPS-VPP]: sessmgr restart at uplane_policing_charging	cups-up
CSCvk62265	[BP-CUPS]: UP never re-initiate SX association if it comes back before SX faillure detected in UP	cups-up
CSCvk66464	[BP-CUPS]: Sessmgr reload at smgr_match_dyn_rule_filter	cups-up
CSCvm54234	[PLT-CUPS-VPP] Call is getting dropped after performing shutdown-noshutdown-shutdown interface	cups-up
CSCvm72250	[PLT-CUPS-ICUPS] sessmgr and vpp crashes and DPC2 cards in Offline state on 21.10.M0.70328	cups-up
CSCvk46857	[PLT-CUPS-VPP]: vpnmgr restart while removing crp config	cups-up
CSCvm47437	[BP-ICUPS]:Analyser/RB statistics are not counting DL dropped offloaded packets.	cups-up
CSCvm56058	[BP-ICUPS]: Streams created with state PASSIVE and packets pass through slow path.	cups-up

Bug ID	Headline	Product Found*
CSCvm56190	[BP-ICUPS]: packets sent through slow path after PDN-UPDATE.	cups-up
CSCvm57966	[BP-ICUPS] First DL pkt of UDP flow creating stream in passive state instead of active state	cups-up
CSCvm50353	[BP-ICUPS] : SGW sends TEP entry Updation with IPV6 remote and local address during HO	pdn-gw
CSCvm55782	[BP-ICUPS]:Dynamic Rule flow status change from Discard to Allow All is not working	pdn-gw
CSCvm63590	[PLT-ICUPS-VPP]: Update to DCCA triggered 1 pkt later then expected.	pdn-gw
CSCvm79365	[BP-ICUPS]: Data over new dedicated bearer after gngp-collapsed HO sent through slow path.	pdn-gw
CSCvm91229	[BP-ICUPS] : sessmgr restart at fapi_tp_process_incoming_local_row_req() sp=0xffccd588()	pdn-gw
CSCvm19671	US38613 [PGW-NSA] PRA-Info received in MBReq is not sent in CCRU in inter RAT case	pdn-gw
CSCvm75776	[BP-ICUPS]:Policer table is deleted,created twice on Dynamic Rule deletion, bearer movement for GBR	pdn-gw
CSCvm83968	[CUSP] need to handle interworking of URL-readdressing and CUSP feature.	pdn-gw
CSCvn03518	Idle timer expires 10 seconds earlier than it ideally should when data sent.	pdn-gw
CSCvm82008	[BP-ICUPS]:HTTP volume based offload is not happening after PDN update	sae-gw
CSCvn09483	21.10_70287_SGSN: Subscriber IMEI check frequency config not working properly during InterSRAU event	sgsn
CSCvm93185	[SGSN] DNS Naptr weight based load balancing not taking place	sgsn
CSCvm45981	[PLT-ICUPS]:TCP & UDP Packets drop observed at VPP for Single PGW at 500+ Mbps with 5 & 2 flows	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*
CSCvn13800	sessmgr restart at function dh_api_delete_handle	pdn-gw
CSCvn11028	vpnmr restart at vpnmgr_audit_ip4_by_session_taskid()	staros

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

Operator Notes

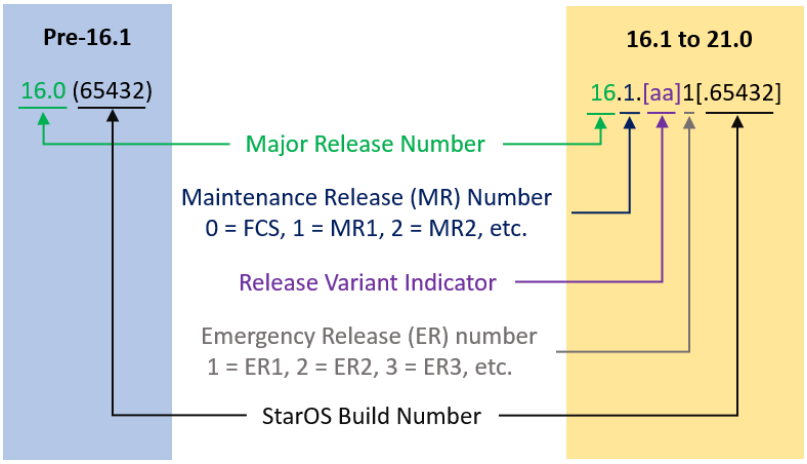
StarOS Version Numbering System

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.

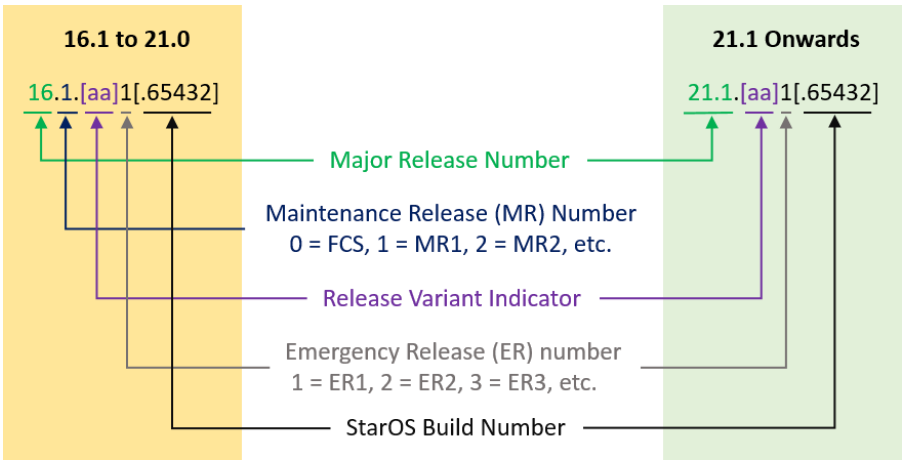
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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