Release Notes for StarOS™ Software Version 21.10.6

First Published: Sept 2, 2020
Last Updated: Sept 2, 2020

Introduction

This Release Notes identify changes and issues related to this software release. This emergency release is based on release 21.10.5. This Release Notes is applicable to the ASR5500, VPC-SI, and VPC-DI platforms.

Release Package Version Information

Software Packages	Version
StarOS packages	21.10.6, build 77068

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

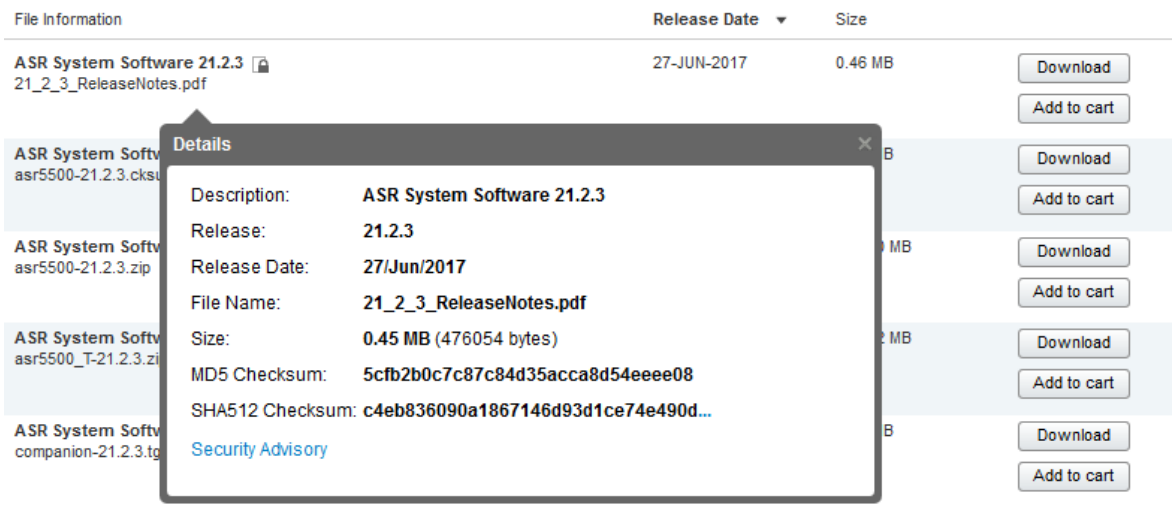
There are no firmware upgrades required for this release.

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*
CSCvm83524	[BP-CUPS] Assert failure at egtpc_handle_user_sap_event()	cups-cp
CSCvk56280	[BP-CUPS-VPP]: sessmgr restart at uplane_policing_charging	cups-up
CSCvk46857	[PLT-CUPS-VPP]: vpnmgr restart while removing crp config	cups-up
CSCvk62265	[BP-CUPS]: UP never re-initiate SX association if it comes back before SX faillure detected in UP	cups-up
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
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
CSCvm59761	[PLT-CUPS-VPP]IPv6 fragmentation issue	cups-up
CSCvq76355	"[ePDG]To change the event ID of Unknown Encryption Type 12, Attribute Value 192"	epdg
CSCvn59038	Segmentation fault mme_start_procedure() while handling Delete Bearer.	mme
CSCvs26952	"qVPC-DI, MME: SGS schema has generates more entries than sgs services"	mme
CSCvq03879	Single-registration-indication flag not set in case of 4G->3G->4G PS-HO	mme

Bug ID	Headline	Product Found*
CSCvs01456	Cisco Mobility Management Entity Denial of Service Vulnerability	mme
CSCvo33689	inter-rat-nnsf mme-codes parameter missing after reload	mme
CSCvv57453	Sessmgr restarts seen at egtpc_get_ebi_info_from_pdu	mme-app
CSCvm82106	[BP-ICUPS] : Packets drop seen at vpp for TEP entries marled with DeferDel as "yes".	pdn-gw
CSCvn27653	IP source violation should support L2TP allocated IP + Framed route combinations	pdn-gw
CSCvo08450	21.10.1: PGW is adding extra character "19" in MSISDN PCO on CSResp during SIM activation scenario.	pdn-gw
CSCvo25833	SM fail due to Segmentation fault on snx_pgw_driver_recreate_pdn	pdn-gw
CSCvr30611	ASR5500: "Transmit stalled" messages were seen in console	pdn-gw
CSCvp80850	sessmgr restart at tftcpsendpacket()	pdn-gw
CSCvo09517	VPP related logs appear during DPC migration even if VPP function is disabled.	pdn-gw
CSCvm55782	[BP-ICUPS]:Dynamic Rule flow status change from Discard to Allow All is not working	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
CSCvm91229	[BP-ICUPS-VPP] : sessmgr restart at fapi_tp_process_incoming_local_row_req() sp=0xffccd588()	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
CSCvo64893	[saegw-gn] LI interception of calltype saegw does not intercept 2G/3G calls	sae-gw
CSCvg77087	XL - GGSN/SAE-GW on VPC-DI - aaamgr in Active CF card in Memory warn state	sae-gw
CSCvp09454	session manager restart due to RABassign request	sgsn
CSCvn31717	sessmgr restart on s4_smn_send_egtpc_pdn_local_purge	sgsn
CSCvn01449	Syslog messages missing hostname after evlogd kill	staros
CSCvm96218	"ASR5K device sends wrong objects for the traps with ifIndex 1343, 1344, 1345, 1346."	staros
CSCvm98426	[PLT-ICUPS-VPP] Not able to send fragmented packet through VPP.	staros
CSCvn23275	[PLT-ICUPS] Both DPC2 rebooted upon planned migration	staros
CSCvn67152	VPC-DI/XL710: Fix port statistic collection time intervals.	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*
CSCvu68945	Evaluation of staros for Treck ip stack vulnerabilities	staros
* Information in the "Product Found" column identifies the product in which the bug was initially identified.		

Operator Notes

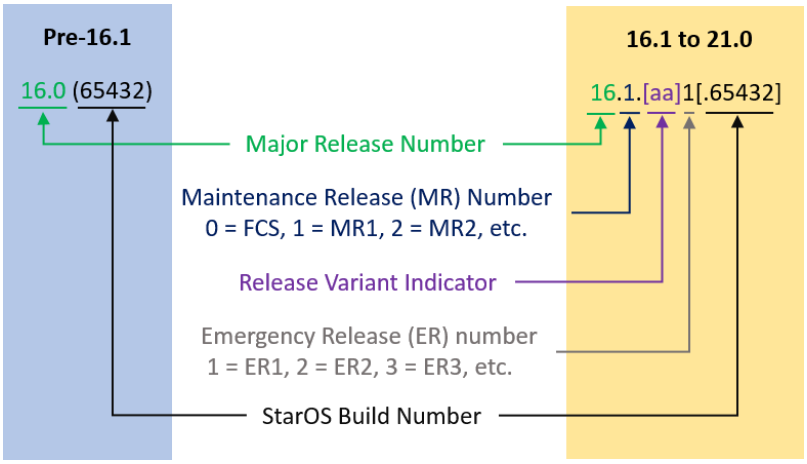
StarOS Version Numbering System

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.

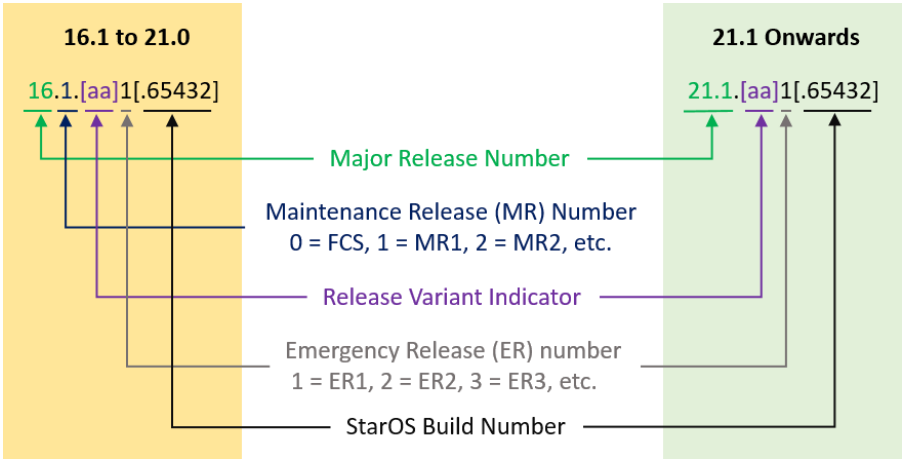
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2020 Cisco Systems, Inc. All rights reserved.