Release Notes for StarOS™ Software Version 21.17.17

First Published: Jan 29, 2021
Last Updated: Jan 29, 2021

Introduction

This Release Notes identify changes and issues related to this software release. This emergency release is based on release 21.17.16. This Release Notes is applicable to the ASR5500, VPC-SI, and VPC-DI platforms.

Release Package Version Information

Software Packages	Version
StarOS packages	21.17.17, build 79107

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

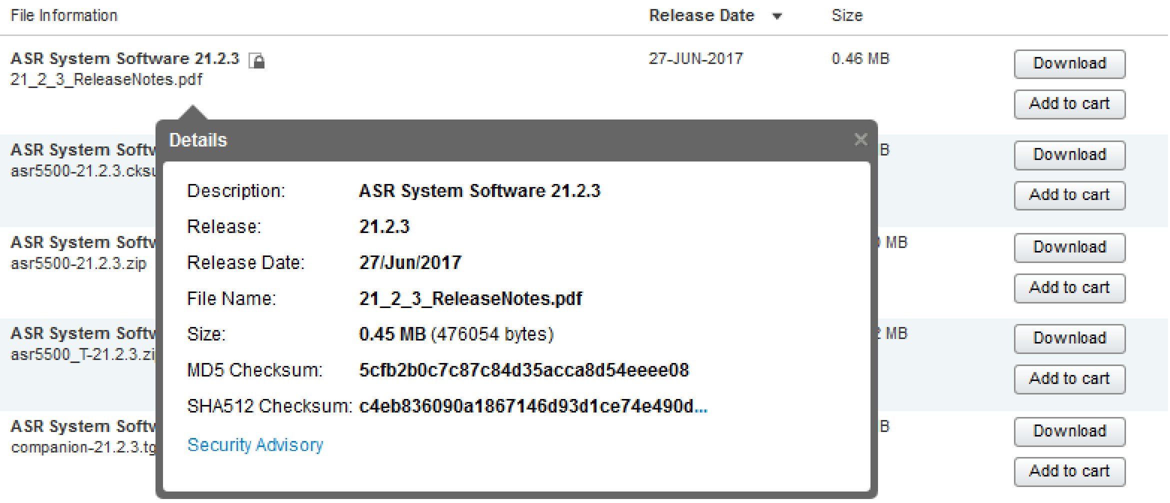
There are no firmware upgrades required for this release.

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.



File Information	Release Date	Size
ASR System Software 21.2.3 21_2_3_ReleaseNotes.pdf	27-JUN-2017	0.46 MB
ASR System Softw asr5500-21.2.3.cksu		B
ASR System Softw asr5500-21.2.3.zip		MB
ASR System Softw asr5500_T-21.2.3.zi		MB
ASR System Softw companion-21.2.3.tg		B

Details

Description: ASR System Software 21.2.3
Release: 21.2.3
Release Date: 27/Jun/2017
File Name: 21_2_3_ReleaseNotes.pdf
Size: 0.45 MB (476054 bytes)
MD5 Checksum: 5cfb2b0c7c87c84d35acca8d54eeee08
SHA512 Checksum: c4eb836090a1867146d93d1ce74e490d...

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*
CSCvs72199	CUPS CP :PGW-CP node spits continuous log events acsmgr 91699 error CUPS: Charging Snapshot with key	cups-cp
CSCvs40215	[BP-CUPS] resultCode IE missing in CDR in CUPS	cups-cp
CSCvu81900	[PLT-CUPS]: huge CRR recovery failures on back-to-back SRP-Switchover leading to call-drop	cups-cp
CSCvt49488	In Monsub fastpath packets are captured twice in vpp pcap	cups-up
CSCvt15349	Recovery failed on 10:2 testbed after RCM VM reload	cups-up
CSCvu00150	[PLT-CUPS]: The p2p app-identifier tls-sni related CLIs failing at UP	cups-up
CSCvt82639	VPP cannot handle MTU size &gt; 2K	cups-up
CSCvs23558	[BP-CUPS] PC: [048dd1d7/X] smgr_uplane_handle_config_chrg_action()	cups-up
CSCvs29569	[sol test] Gtpumgr is in over state due to over memory usage on SAEGW-UP	cups-up
CSCvu18163	Recovery mechanism is not working as expected for CIOT calls after session manager restart	mme
CSCvt75377	Assert at mme_app_fill_s1_bearer_values	mme

Bug ID	Headline	Product Found*
CSCvv57424	SGd MT-Forward-Short-Message-Request handling when the req is received outside PTW is wrong	mme
CSCvw05731	mmedemux restart in mme_get_ta_info_from_tlv	mme
CSCvw22685	MME is sending TEID 0 in Modify-Bearer-Request to SGW	mme
CSCvw30489	S1-AP messages are not decoded in Monitor Subscriber next call	mme
CSCvv17110	SessMgr restart while handling MME bearer abort procedure	mme
CSCvt33632	"EPC: MME, Collision: NR add &amp; UBReq, MME send with the ESM cause"	mme
CSCvt34756	"EPC: MME, Reversed_message_order_ULR_CSReq_In_case_GUTI_Attach"	mme
CSCvt90897	Segmentation fault when decoding nas message	mme
CSCvu24212	Unable to delete TAI Group related configuration from MME	mme
CSCvw51536	[I-CUPS] PC: [09e96246/X] acs_assign_data_session()	pdn-gw
CSCvs88144	[PGW] PCRF monitoring-key range must allow any 4 bytes range value	pdn-gw
CSCvw51563	[I-Cups] acsmgr_fp_handle_tep_version_modify()	pdn-gw
CSCvs53948	Override control not working after HSUE to 4G transition with VPP	pdn-gw
CSCvw03127	Frequent sessmgr restart on acs_flush_ttl_aged_entries_from_ip_pools	pdn-gw
CSCvr96436	[CUSP] sessmgr Segmentation fault - tfTcpSendPacket	pdn-gw
CSCvw85418	[BP-Legacy] EDR's created for ULI CGI_RAI and SGI_RAI contains only MCC MNC info	pdn-gw
CSCvv74924	Assertion failure at gtapp_enc_ie.c:1618	sgsn
CSCvs62416	[SGSN]- sessmgr restarts at egtpc_handle_user_sap_event s4_smn_egtp_send_modify_bearer_command	sgsn
CSCvv60952	SGSN not send re-attach required when Cancel Location Request with Reattach-Required bit=1 received	sgsn
CSCvv69506	ASR5500 - SGSN/MME - map-service name is truncated to 8 characters	sgsn

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*
CSCvw58221	[BP_PCT PGW] Diameter data fragmentation not working as expected	pdn-gw
CSCvx08359	WiFi to VoLTE handover failure cause as CONTEXT_NOT_FOUND (0x40)with different pdn types	pdn-gw
CSCvw51050	21.14: Port speed OID changes after port up/down	staros
CSCvu29089	E-RAB Modification Indication collision scenario with Create Bearer response	mme
CSCvv28217	Session manager restart wile encoding QOS on PDP	mme
CSCvu55467	[BP-ICUPS] Session Controller restart observed during data_backup_read_abort	pdn-gw
CSCvv02711	PGW sends APN AMBR as 1Kbps in UBReq	pdn-gw
CSCvw45500	S4 association configuration disappeares after demux card restart	sgsn
CSCvw95793	[Smoke2-ICUPS] In Monsub fastpath pcap files are not generated as expected.	pdn-gw
CSCvv66919	MIPv6 Binding update not including Default Router after ICSR	pdn-gw
CSCvs83392	Cisco ASR 5000 Enhanced Charging Service Rule Bypass Vulnerability	sgw
***** Information in the “Product Found” column identifies the product in which the bug was initially identified.		

Operator Notes

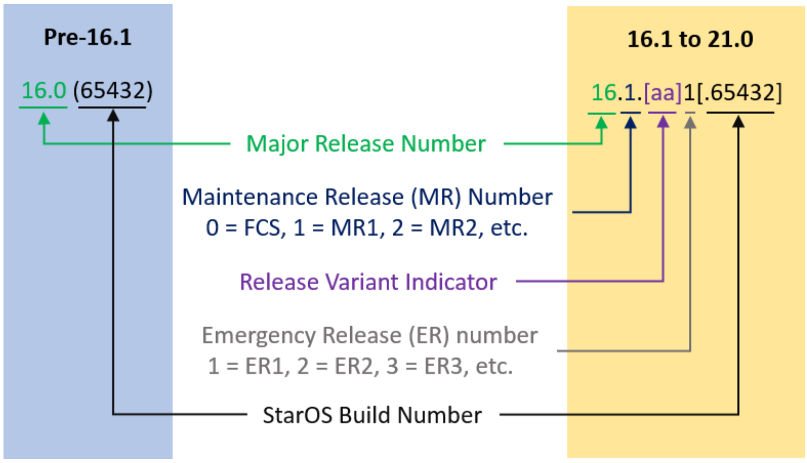
StarOS Version Numbering System

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.

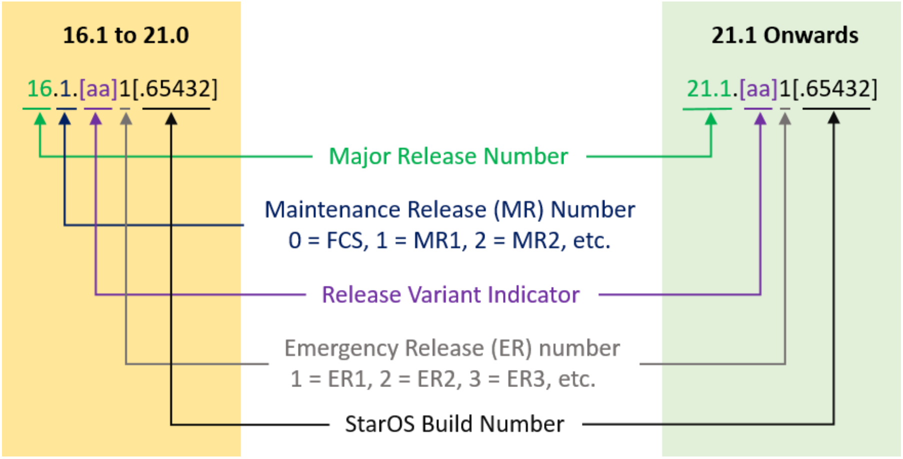
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example “16.0 (55435)”. Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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


Pre-16.1
16.0 (65432)
16.1 to 21.0
16.1.[aa]1[.65432]
Major Release Number
Maintenance Release (MR) Number
0 = FCS, 1 = MR1, 2 = MR2, etc.
Release Variant Indicator
Emergency Release (ER) number
1 = ER1, 2 = ER2, 3 = ER3, etc.
StarOS Build Number

The Version Build Number for releases 21.1 and later include a major and emergency release number, for example, "21.1.1".


16.1 to 21.0
16.1.[aa]1[.65432]
21.1 Onwards
21.1.[aa]1[.65432]
Major Release Number
Maintenance Release (MR) Number
0 = FCS, 1 = MR1, 2 = MR2, etc.
Release Variant Indicator
Emergency Release (ER) number
1 = ER1, 2 = ER2, 3 = ER3, etc.
StarOS Build Number

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	

Package	Description
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.
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.

Package	Description
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.