



Release Notes for StarOS™ Software Version 21.17.19

First Published: Sept 22, 2021

Last Updated: Sept 22, 2021

Introduction

This Release Notes identify changes and issues related to this software release. This emergency release is based on release 21.17.18. This Release Notes is applicable to the ASR5500, VPC-SI, and VPC-DI platforms.

Release Package Version Information

Software Packages	Version
StarOS packages	21.17.19, build 82079

Descriptions for the various packages provided with this release are located in [Release Package Descriptions](#).

Feature and Behavior Changes

The 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

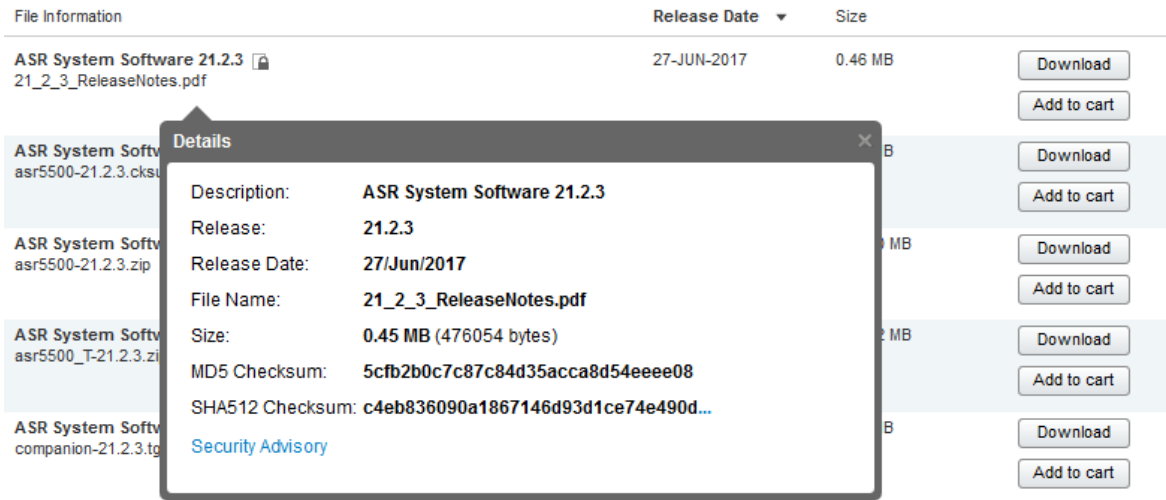
There are no firmware upgrades required for this release.

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 <pre>> certutil.exe -hashfile <filename>.<extension> SHA512</pre>
Apple MAC	Open a terminal window and type the following command <pre>\$ shasum -a 512 <filename>.<extension></pre>
Linux	Open a terminal window and type the following command <pre>\$ sha512sum <filename>.<extension></pre> <p>Or</p> <pre>\$ shasum -a 512 <filename>.<extension></pre>

Open Bugs for This Release

Operating System	SHA512 checksum calculation command examples
<p>NOTES:</p> <p><filename> is the name of the file.</p> <p><extension> is the file extension (e.g. .zip or .tgz).</p>	

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*
CSCvu34579	show crypto statistics not display encode and decode data statics in SI and ASR55K	cups-cp
CSCvu81900	[PLT-CUPS]: huge CRR recovery failures on back-to-back SRP-Switchover leading to call-drop	cups-cp
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
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
CSCvt49488	In Monsub fastpath packets are captured twice in vpp pcap	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
CSCvu55658	"[ICSR] Sx Peers are not getting cleared , when peers un-configured after UPswitchover"	cups-up
CSCvt82639	VPP cannot handle MTU size > 2K	cups-up
CSCvu18163	Recovery mechanism is not working as expected for CIOT calls after session manager restart	mme

Open Bugs for This Release

Bug ID	Headline	Product Found*
CSCvw81248	Abnormal high counter values in MME tai schema counters after upgrade	mme
CSCvx16478	ASR5500 21.17.6 SNMP TRAPS sent with different varbinds when a valid 2nd address is not configured	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
CSCvw17110	SessMgr restart while handling MME bearer abort procedure	mme
CSCvt75377	Assert at mme_app_fill_s1_bearer_values	mme
CSCvw57424	SGd MT-Forward-Short-Message-Request handling when the req is received outside PTW is wrong	mme
CSCvq68326	mmemgr restart is seen in memmgr_aggregate_msg_to_sessmgr()	mme
CSCvt33632	"EPC: MME, Collision: NR add & 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
CSCvz12548	Value for counter esm-msgtx-pdncon-rej-auth-failed not increasing	mme
CSCvw05731	mmedemux restart in mme_get_ta_info_from_tlv	mme
CSCvw13552	Echo req seen for gtp peers even when echo is not configured in MME.	mme
CSCvy29396	NB-IoT UE isn't receiving SMS via SGd when the device is in idle	mme
CSCvy81424	X2 Handover does not work due to possible incorrect NextHop in PathSwitchReqAck	mme
CSCvw87220	Handle E-RAB MODIF of EBI=5 when PDN-connectivity req for EBI=6 process is ongoing	mme
CSCvu24212	Unable to delete TAI Group related configuration from MME	mme
CSCvy89382	WRITE-REPLACE WARNING RESPONSE messages not received by MME after enabling WRWI	mme
CSCvw96092	session manager restarts at pgw_drv_clear_drv_clp_due_to_gnnp_ctxt_replacement	pdn-gw
CSCvs88144	[PGW] PCRF monitoring-key range must allow any 4 bytes range value	pdn-gw
CSCvr96436	[CUSP] sessmgr Segmentation fault - tfTcpSendPacket	pdn-gw
CSCvs53948	Override control not working after HSUE to 4G transition with VPP	pdn-gw
CSCvt05716	Sessmgr process restart in TCP packet processing path	pdn-gw
CSCvw85418	[BP-Legacy] EDR's created for ULI CGI_RAI and SGI_RAI contains only MCC MNC info	pdn-gw
CSCvx22350	Sessmgr restart with fatal signal tftCplIncomingPacket()	pdn-gw
CSCvx15261	Sessmgr crash at PC: [08a14140/X] egtpc_encode_imsi_ie()	sae-gw
CSCvv74924	Assertion failure at gtapp_enc_ie.c:1618	sgsn
CSCvy98376	5G-NSA: SGSN: MAP nrAsSecondaryRATNotAllowed encoding	sgsn

Open Bugs for This Release

Bug ID	Headline	Product Found*
CSCvy09744	[CP-SGSN] sessmgr restart seen with function egtpc_handle_del_bearer_cmd_req_evt	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
CSCvx44868	sessmgr restart seen with Function: SmGenSuspendReq	sgsn
CSCvx49375	Following Error after node upgrade " initial-config file has not finished loading";	staros

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*
CSCVy45030	Sessmgr memory increasing on ASR5500 due to smc_sx_allocate_subsession_sx_data()	cups-up
CSCvt66372	sessmgr restart at sess/mme/mme-app/app/mme_fw.c	mme
CSCVy90143	Auto recovery for "Failed to send Diameter Message" issue	mme
CSCVv24823	sessmgr restarted at the function egtpc_send_req_msg()	mme
CSCVz39725	DCN id is incorrectly sent in ATTACH ACCEPT	mme
CSCVx66200	[BP-ICUPS]:SM crashes observed on active and standby with "acsmgr_deallocate_call_obj()"	pdn-gw
CSCVy98310	BP-ICUPS: sessmgr restart while running callmodel with SRP switchovers at 30 mins interval	pdn-gw
CSCVx79042	Unexpected debug logs are observed during ICSR switchover with L2TP subscribers	pdn-gw
CSCVx80308	[BP-ICUPS]:SM restart observed on active/standby with plain callmodel	pdn-gw
CSCVy29768	Diameter peers go down even though there is an operational LAG port due to EZChip LPM tree issue	pdn-gw
CSCVy63440	Port Tx traffic not balanced across MIO cards	staros
CSCVv33622	Cisco ASR 5000 Series Software nocli Authorization Bypass Vulnerability	staros
* Information in the "Product Found" column identifies the product in which the bug was initially identified.		

Operator Notes

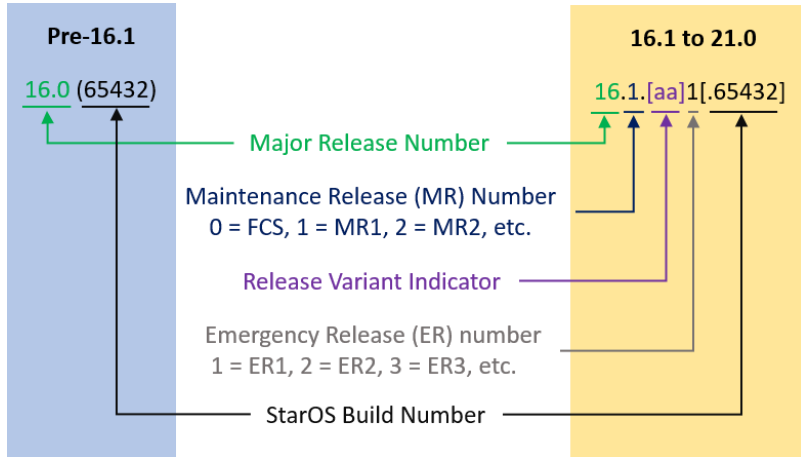
StarOS Version Numbering System

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.

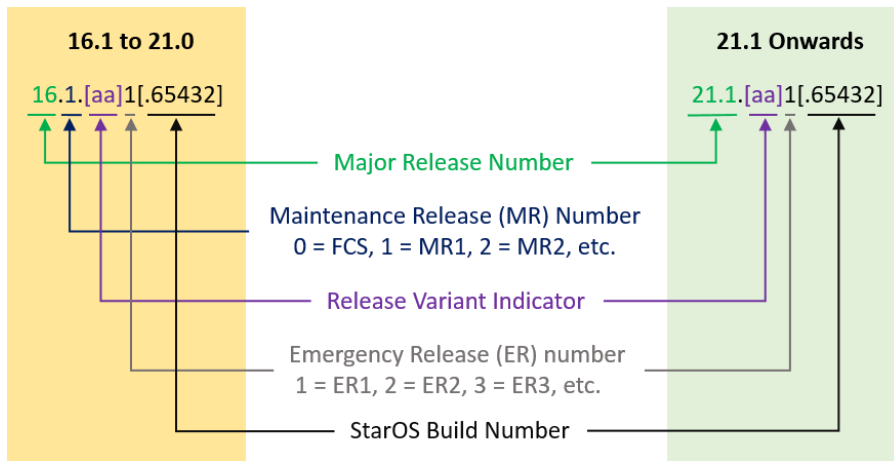
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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

Package	Description
qvmc-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.
qvmc-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.
qvmc-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.
qvmc-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.
qvmc-di-template-vmware-<release>.tgz	The VPC-DI binary software image that is used to on-board the software directly into Vmware.
qvmc-di-template-vmware_T-<release>.tgz	The trusted VPC-DI binary software image that is used to on-board the software directly into Vmware.
qvmc-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.
qvmc-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.
qvmc-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.
qvmc-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	
qvmc-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.
qvmc-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.
qvmc-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.
qvmc-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.
qvmc-si-template-vmware-<release>.ova	The VPC-SI binary software image that is used to on-board the software directly into Vmware.
qvmc-si-template-vmware_T-<release>.ova	The trusted VPC-SI binary software image that is used to on-board the software directly into Vmware.
qvmc-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.
qvmc-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.
qvmc-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
qvmc-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. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.