Release Notes for StarOS™ Software Version 21.6.2

First Published: February 15, 2018
Last Updated: February 15, 2018

Introduction

These Release Notes identify changes and issues related to this software release. This emergency release is based on release 21.6.1. These release notes are applicable to the ASR5500, VPC-SI and VPC-DI platforms.

Release Package Version Information

Software Packages	Version
StarOS packages	21.6.2 build 68797

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.

IPSec Software Data Path for IKEv1 Maps

Applicable Product(s) or Functional Area: IPSec

Feature Default: Disabled – Configuration Required

Feature Description

The IPSec Manager performs data path encryption/decryption, which is controlled by boot time CLI configuration. For each IKEv1 Crypto Map, a new IPSec Manager is spawned with a maximum of 11 per CPU and 22 per card for DPC1. Once the maximum number of IPSec Managers is spawned on each active DPC1 card, the new Crypto Map starts reusing existing IPSec Manager. The CLI command controlling this feature must be configured during the boot time.

NOTE: This feature is applicable only to DPC1 on ASR5500 platform. DPC2 is not supported.

Configuring Software Data Path for IKEv1 Maps

Use the following configuration to enable IPSec Software Data Path for IKEv1 Maps:

```
configure
  [ no ]  require crypto ikev1-acl software
  end
```

Notes:

- **crypto**: Crypto-related requirement.
- **ikev1-acl**: IKEv1-ACL IPSec sessions.
- **software:** IPSec Manager performs encryption/decryption/DH calculations.
- **no**: Disables IPSec Manager from performing encryption/decryption/DH calculations.

Monitoring and Troubleshooting

show configuration

The following new fields are added to the output of this command:

```
require ikev1-acl software
```

Hardware Crypto Assist for ePDG

Applicable Product(s) or Functional Area: ePDG

Feature Default: Enabled – Always-on (if Coleto Creek Card is present)

Feature Description

With this release, ePDG Hardware Crypto Assist feature is fully qualified and generally available. In release 21.5 ePDG Hardware Crypto Assist feature was not fully qualified and it was available only for testing purposes.

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

21.6.x releases include 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:

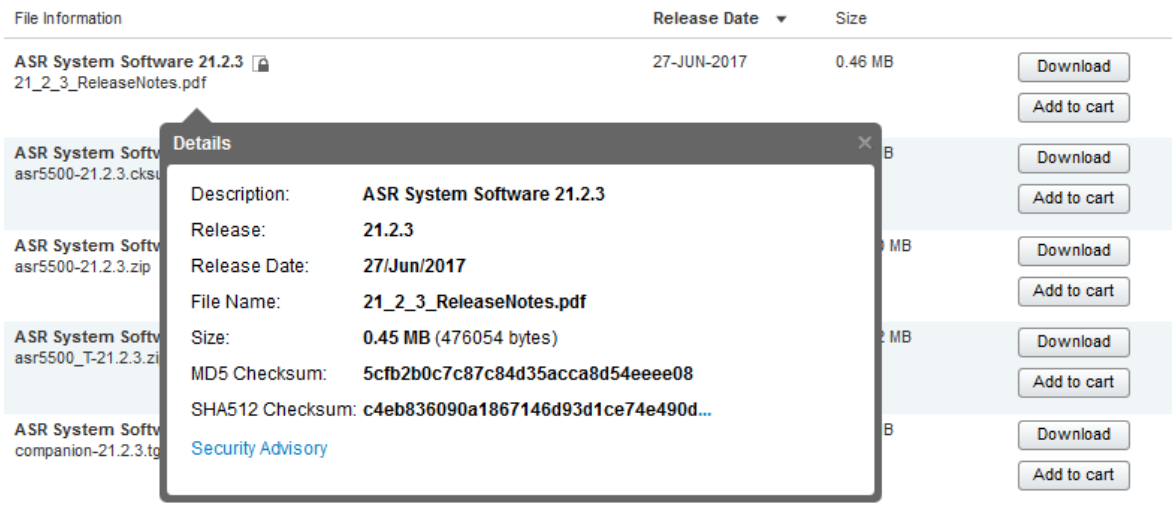
- A 60 second lockout upon lowering the ejector sub-handle (interlock). Failures were observed in the field where an MIO that was being removed attempted to become Active as it was being removed. The remaining MIO would then go Standby causing a chassis failure. Now after the front panel ejector subhandle (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 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*>

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*
CSCvg36262	Split the current MME-Decor related stats for TAU and Attach procedures	mme
CSCvh59780	Sessmgr restart in egtpc event handler path	mme
CSCvg89252	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
CSCvh64982	Planned SRP switchover followed by switchover due to BGP failure - aaamgr restarts	sae-gw
CSCvf32599	osd-compute reboot leaves CF in booting state: EMCTRL_CARDTYPE_MIS-MATCH	staros
CSCvh54162	[ePDG] performing iftask restart is causing SF to restart on ultraM with ser-vicemode as epdg	staros
CSCvh68111	The beakerd process has a memory leak	staros
CSCvh94362	QvPC-DI "show support details" command causes packet drops when run during heavy load conditions.	staros
CSCvh91499	PCAPs not working when 6 Interfaces are used for service ports when used with 40 VCPUs	staros
CSCvh83313	IFTASK Restart - VPC	staros
CSCvh84131	defaut mcdma latency is 0 leading to inefficiency	staros
CSCvh95333	logging filter level debug, SF card migration fails due to timeout	staros
CSCvh83392	NPU CPU util stuck at 100% after IFTASK Restart - VPC	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*
CSCvh79202	[ePDG] with Crypto hardware, data throughput at max cause the SF fail to respond	epdg
CSCvh60130	intermittent aaamgr restart on callmodel tear down seen	Pdn-gw
CSCvh19822	post-processing to next-hop IP hampered for partial HTTP packets	sae-gw
CSCvg78347	iftask syslog error:sn_anpusim_packet_frame_add:991 mbuf alloc failure	staros
CSCvh87011	iftask crashing resulting in SFs in continuous boot loop	staros
* Information in the "Product Found" column identifies the product in which the bug was initially identified.		

Operator Notes

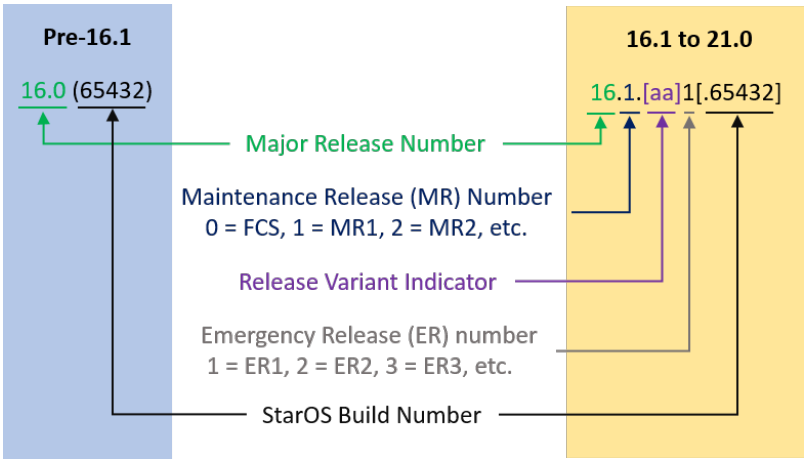
StarOS Version Numbering System

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.

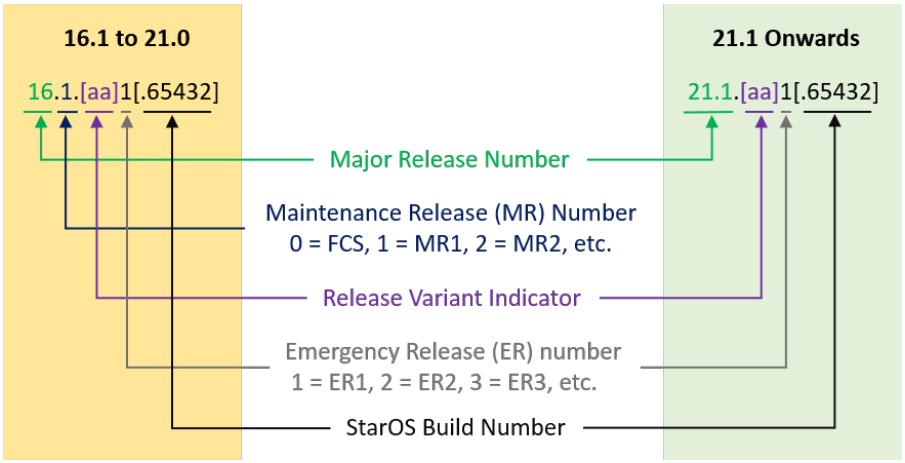
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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

Package	Description
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.
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.

Package	Description
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)

© 2018 Cisco Systems, Inc. All rights reserved.