Release Notes for StarOS™ Software Version 21.10.5 and Ultra Service Platform Version 6.4.1

First Published: November 26, 2018
Last Updated: November 26, 2018

Introduction

This Release Notes identify changes and issues related to this software release. This emergency release is based on release 6.4.0 and StarOS 21.10.5. This Release Notes is applicable to the Ultra Service platforms. For information on ASR5500, VPC-SI and VPC-DI please refer to Release Notes for 21.10.5

Release Package Version Information

Software Packages	Version
StarOS packages	21.10.5, build 73231
Ultra Service Platform ISO	6_4_1-10013
usp-em-bundle*	6.4.0, Epoch 7829
usp-ugp-bundle*	21.10.5, build 73231, Epoch 7812
usp-yang-bundle	1.0.0, Epoch 7794
usp-uas-bundle	6.4.0, Epoch 7875
usp-auto-it-bundle	5.8.0, Epoch 8018
usp-vnfm-bundle	4.3.0.121, Epoch 7795
ultram-manager RPM*	2.2.1, Epoch 1260
USP RPM Verification Utilities	6.4.1
* These bundles are also distributed separately from the ISO.	

Descriptions for the various packages provided with this release are located in Release Package Descriptions.

Feature and Behavior Changes

Refer to the *Release Change Reference* for a complete list of feature and behavior changes associated with this software release.

Related Documentation

For a complete list of documentation available for this release, go to:

- StarOS: https://www.cisco.com/c/en/us/support/wireless/asr-5000-series/products-installation-and-configuration-guides-list.html
- Ultra Gateway Platform (including the Ultra M Solution): https://www.cisco.com/c/en/us/support/wireless/ultra-gateway-platform/products-installation-and-configuration-guides-list.html
- Ultra Automation Services: https://www.cisco.com/c/en/us/support/wireless/ultra-automation-services/products-installation-and-configuration-guides-list.html
- Virtual Packet Core (including VPC-SI and VPC-DI): https://www.cisco.com/c/en/us/support/wireless/virtual-packet-core/products-installation-and-configuration-guides-list.html

Installation and Upgrade Notes

This Release Note does not contain general installation and upgrade instructions. Refer to the existing installation documentation for specific installation and upgrade considerations.

Ultra M Hyper-Converged Model Component Versions

HW	SW	5.8	6.0	6.1	6.2	6.3	6.4
	StarOS	68415	21.6.0, Build 68695	21.7.0, Build 68897	21.8.0, Build 69296	21.9.0, Build 69977	21.10.0, Build 70597
	ESC	3.1.0.116	3.1.0.145	3.1.0.145	4.0.0.104	4.2.0.74	4.3.0.121
	RH Kernel	7.3	7.3	7.3	7.4	7.5	7.5
	OSP	10	10	10	10	10	10
UCS C240 M4S SFF (NFVI)	BIOS	3.0(3c)	3.0(3c)	3.0(3c)	3.0(4a)	3.0(4a)	3.0(4a)
	CIMC (BMC)	3.0(3e)	3.0(3e)	3.0(3e)	3.0(4a)	3.0(4d)	3.0(4d)
	MLOM	4.1(3a)	4.1(3a)	4.1(3a)	4.1(3a)	4.1(3f)	4.1(3f)
C2960XR-48TD-I (Management)	Boot Loader	15.2(3r)E1	15.2(3r)E1	15.2(3r)E1	15.2(3r)E1	15.2(3r)E1	15.2(3r)E1
	IOS	15.2.(2) E5	15.2.(2) E5	15.2.(2) E5	15.2.(2) E5	15.2.(2) E5	15.2.(2) E5
C3850-48T-S (Management)	Boot Loader	3.58	3.58	3.58	3.58	3.58	3.58
	IOS	03.06.06E	03.06.06E	03.06.06E	03.06.06E	03.06.06E	03.06.06E
Nexus 93180-YC-EX (Leafs)	BIOS	7.59	7.59	7.59	7.59	7.59	7.59
	NX-OS	7.0(3)I5(2)	7.0(3)I5(2)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)

Nexus 9236C (Spines)	BIOS	7.59	7.59	7.59	7.59	7.59	7.59
	NX-OS	7.0(3)I5(2)	7.0(3)I5(2)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)

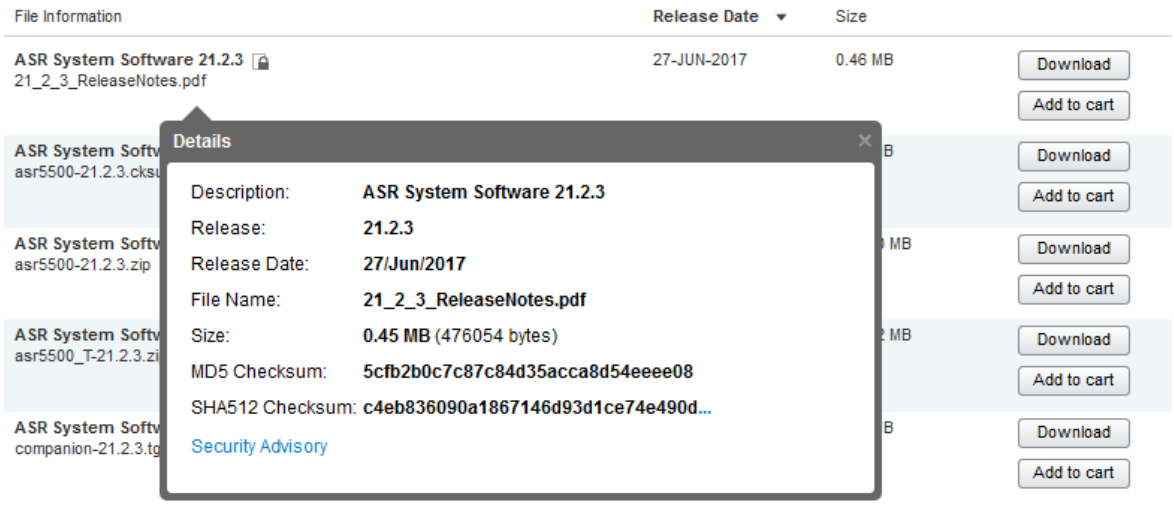
Firmware Updates

There are no firmware updates 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 **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.

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, see the following table.

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. USP ISO images are signed with a GPG key. 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 in this Release

The following table lists known bugs that were found in, and 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
CSCvk62265	[BP-CUPS]: UP never re-initiate SX association if it comes back before SX faillure detected in UP	cups-up
CSCvm59761	[PLT-CUPS-VPP]IPv6 fragmentation issue	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
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
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
CSCvo33689	inter-rat-nnsf mme-codes parameter missing after reload	mme
CSCvq03879	Single-registration-indication flag not set in case of 4G->3G->4G PS-HO	mme
CSCvp80850	sessmgr restart at tftcpsendpacket()	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
CSCvm82106	[BP-ICUPS] : Packets drop seen at vpp for TEP entries marled with DeferDel as “yes”.	pdn-gw
CSCvm91229	[BP-ICUPS-VPP] : sessmgr restart at fapi_tp_process_incoming_local_row_req() sp=0xffccd588()	pdn-gw
CSCvn27653	IP source violation should support L2TP allocated IP + Framed route combinations	pdn-gw
CSCvo25833	SM fail due to Segmentation fault on snx_pgw_driver_recreate_pdn	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
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

Bug ID	Headline	Product Found*
CSCvo08450	21.10.1: PGW is adding extra character “19” in MSISDN PCO on CSResp during SIM activation scenario.	pdn-gw
CSCvo09517	VPP related logs appear during DPC migration even if VPP function is disabled.	pdn-gw
CSCvr30611	ASR5500: “Transmit stalled” messages were seen in console	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
CSCvn31717	sessmgr restart on s4_smn_send_egtpc_pdn_local_purge	sgsn
CSCvp09454	session manager restart due to RABassign request	sgsn
CSCvm93185	[SGSN] DNS Naptr weight based load balancing not taking place	sgsn
CSCvn23275	[PLT-ICUPS] Both DPC2 rebooted upon planned migration	staros
CSCvm98426	[PLT-ICUPS-VPP] Not able to send fragmented packet through VPP.	staros
CSCvn67152	VPC-DI/XL710: Fix port statistic collection time intervals.	staros
CSCvm96218	"ASR5K device sends wrong objects for the traps with ifIndex 1343, 1344, 1345, 1346."	staros
CSCvn01449	Syslog messages missing hostname after evlogd kill	staros
CSCvo20944	[BP-ICUPS]: starOS CLI commands are NOT getting logged into configured syslog	staros
CSCvm91778	AutoVNF NETCONF trace has passwords in the clear	usp-uas

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

Resolved Bugs in this Release

The following table lists 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*
CSCvs06500	Unable to run snmpwalk v3 against AutoIT VM	ultram-manager

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

Operator Notes

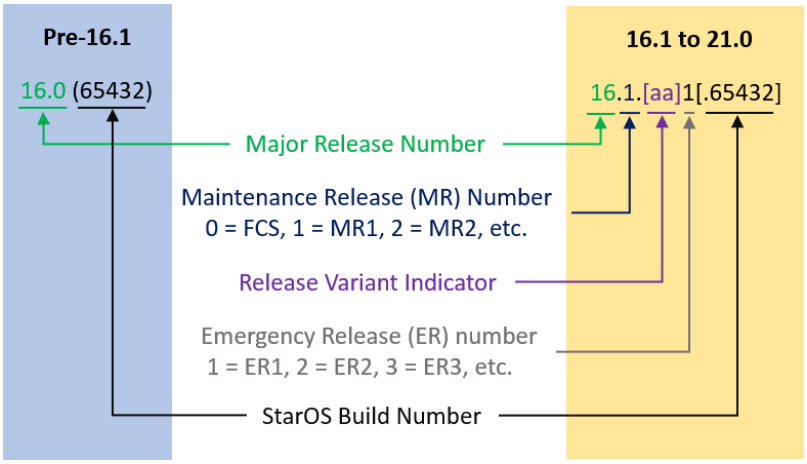
StarOS Version Numbering System

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.

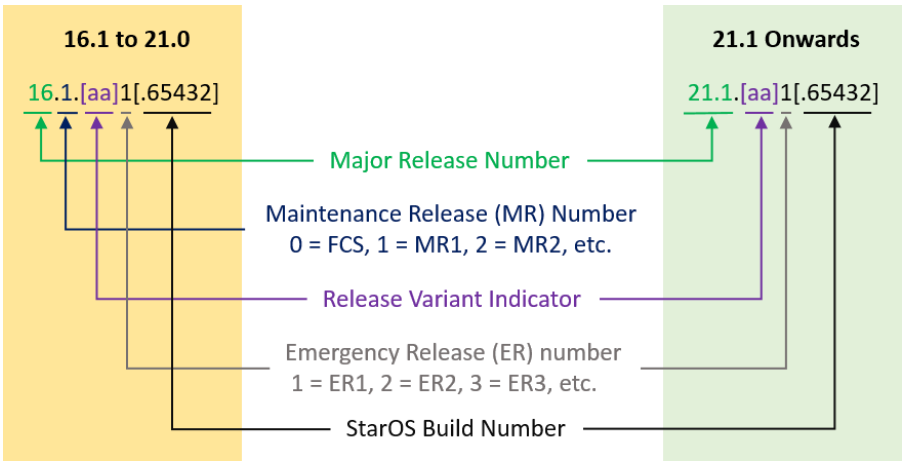
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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

Package	Description
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.
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.

Package	Description
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.
Ultra Service Platform	
usp-<version>.iso	The USP software package containing component RPMs (bundles). Refer to Table 3 for descriptions of the specific bundles.
usp_T-<version>.iso	The USP software package containing component RPMs (bundles). This bundle contains trusted images. Refer to Table 3 for descriptions of the specific bundles.
usp_rpm_verify_utils-<version>.tar	This package contains information and utilities for verifying USP RPM integrity.

Table 3 - USP ISO Bundles

USP Bundle Name	Description
usp-em-bundle-<version>-1.x86_64.rpm*	The Element Manager (EM) Bundle RPM containing images and metadata for the Ultra Element Manager (UEM) module.
usp-ugp-bundle-<version>-1.x86_64.rpm*	The Ultra Gateway Platform (UGP) Bundle RPM containing images for Ultra Packet core (VPC-DI). There are trusted and non-trusted image variants of this bundle.
usp-yang-bundle-<version>-1.x86_64.rpm	The Yang Bundle RPM containing YANG data models including the VNFD and VNFR.
usp-uas-bundle-<version>-1.x86_64.rpm	The Ultra Automation Services Bundle RPM containing AutoVNF, Ultra Web Services (UWS), and other automation packages.
usp-auto-it-bundle-<version>-1.x86_64.rpm	The bundle containing the AutoIT packages required to deploy the UAS.
usp-vnfm-bundle-<version>-1.x86_64.rpm	The VNFM Bundle RPM containing an image and a boot-up script for ESC (Elastic Service Controller).
ultram-manager-<version>-1.x86_64.rpm	This package contains the script and relevant files needed to deploy the Ultra M Manager Service.
* These bundles are also distributed separately from the ISO.	

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.