Release Notes for StarOS™ Software Version 21.26.h6

First Published: May 05, 2023
Last Updated: May 05, 2023

Introduction

This Release Note identifies changes and issues related to this software release. This emergency release is based on release 21.26.h5. This release note is specific to CUPS User Plane only.

Release Package Version Information

Table 1 - Release Package Version Information

Software Packages	Version
StarOS packages	21.26.h6, build 89828

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 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 general installation and upgrade instructions. Refer to the existing installation documentation for specific installation and upgrade considerations.
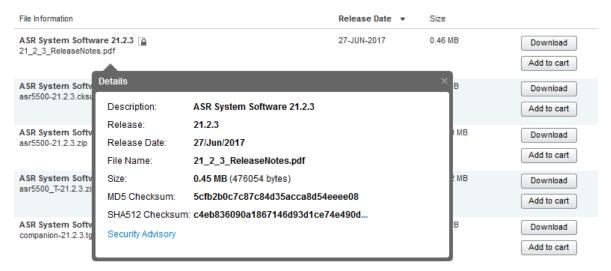
Firmware Updates

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 **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 2 and verify that it matches either the one provided on the software download page.

To calculate a SHA512 checksum on your local desktop see Table 2.

Table 2 - 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

In 21.12.0 and later releases, software images for StarOS, VPC-DI, and VPC-SI, and the companion software packages for StarOS and VPC are signed via x509 certificates. In pre-21.12.0 releases, image signing is not supported for VPC-DI and VPC-SI images, and for StarOS and VPC companion software packages.

USP ISO images are signed with a GPG key.

For more information and instructions on how to validate the certificates, refer to the README file available with the respective software packages.

Open Bugs in this Release

The following table lists the 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.

Table 3 - Open Bugs in this Release

Bug ID	Headline	Product Found*
CSCwa32380	Crash seen on CP while executing UE initiated dedicated bearer scenario	cups-cp
CSCwa83375	[BP-CUPS] Observed sessmgr restart : snx_sgw_driver_handle_modify_rsp on CP in Longevity setup	cups-cp
CSCwb57352	[CUPS] Sx-Modify containing Usage-Report failed. Cause=64 OffendingIE Type=131	cups-cp
CSCwa16910	[BP-CUPS] Assertion failure @ sess/sx/sxc/sx_interface.c:235 func sx_handle_user_sap_event	cups-cp
CSCwc07644	[BP-CUPS]AF at sess/smgr/sessmgr_gr_sess.c:1368 sessmgr_gr_handle_session_full_checkpoint on standby	cups-cp
CSCwd43179	please also apply the fix of CSCwc95182 to Cause New PDN type due to single address bearer only	cups-cp
CSCwa54600	[BP-CUPS] Assertion failure @ PC: [08dc3801/X] fill_dyn_chrg_rule_name_info()	cups-cp
CSCwc83349	[sgw 140014 error] Failure dispatching event <SNX_MSGTYPE_SGW_ADD_PDN_REQ> during longevity test	cups-cp
CSCwc59454	slow response for new calls to existing apn / ip pool at "push config" and "update ip-pool"	cups-cp
CSCwf12125	CUPS: Discrepancy between the time SGW CDR and the time CGF log	cups-cp
CSCwc63031	Sgsn change cdr prints wrong sgsn ip address when performing pureP to Collapsed Handover.	cups-cp
CSCwe74646	sessmgr restart on CUPS CP at function acsmgr_create_nsh_info	cups-cp
CSCvz44140	[BP-CPUS] mostly all aaamgr goes in warn state while running call model	cups-cp
CSCwc95182	SGW doesn't send DBR/DSR triggered by GTPU path failure	cups-cp

Bug ID	Headline	Product Found*
CSCvz99295	[CUPS-TACACS-IPSEC] Crypto map is in Incomplete after configuring	cups-up
CSCwa98318	[BP-CUPS] Assertion failure at Function: sn_memblock_memcache_alloc()	cups-up
CSCvw79600	"loopXX create failed" when recreate VRF on UP.	cups-up
CSCwa04551	[BP-CUPS]:Fatal Signal 6: Aborted Signal from: kernel	cups-up
CSCwa61385	Hermes: show ipv6 neighbors vpp has no output in HX	cups-up
CSCwf21929	sessmgr task restarted on UP, when LI and S8hr interception call is getting cleared	cups-up
CSCwd70361	Assertion failure at sess/sctrl/sessctrl_uplane_cfg_sync.c:23427	cups-up
CSCwd10265	[5GaaS] MME sending wrong destination realm resulting in 3002 from DRA	mme
CSCwa39049	UBR Buffering is partially working	mme
CSCwb09095	MME shall include Monitoring-Event-Report even when count of UEs is 0.	mme
CSCwb60734	Observing SDF Filter decoding failed error in Syslog during IMS call model run	pcf
CSCwc60913	PGW initiates Gy session eventhough PCRF didnt enable online charging	pdn-gw
CSCwa52583	ICUPS : Session Manager restarts on PGW	pdn-gw
CSCwe23018	CLI corruption in the output after running "update active-charging override-control rulebase-config	pdn-gw
CSCwc83287	[Smoke2-ICUPS] Undefined_Function_PC and hatsystem_process_card_fail_msg crash seen in regression	pdn-gw
CSCwe64879	Bulkstats are reporting high utilization for DATARATE_IPPOOL schema	pdn-gw
CSCwa44222	BP-ICUPS: VPP buffer were full while running callmodel when CUSP is enabled	pdn-gw
CSCwa49391	[BP-CUPS] Traffic Optimization UP stats not getting incremented/decremented properly	pdn-gw
CSCwf17642	The PGW sends a CCR-U with no USU when the Tariff-Time-Change value expires)	pdn-gw
CSCwa41640	BP-ICUPS: fragmentation doesn't work properly with CUSP enabled	pdn-gw
CSCwe27916	[PLT-RCM] rcm show-statistics checkpointmgr-endpointstats not working in 21.26.x	rcm
CSCwa40146	[LI-PGW] Observed un-expected content buffer stats output	sae-gw
CSCvz65453	[SGIR-Ph1] After MIO switchover sgi-reachability profiles status showing as DOWN	sae-gw
CSCwd27711	[UPF-SVI] : Uplane received invalid far id in PDU	smf
CSCwa37867	GRE Tunnel with KA not coming up after Card Migration	staros
CSCwd82707	NEMO - Traffic loop observed on the Egress side for GRE traffic	staros
CSCvy08166	sx peers not reconnecting after SMF shut/start	upf
CSCwe29094	[UPF-SVI] : Seen Uplane received invalid far id in PDU on task kill	upf
CSCwe34967	[UPF-SVI]:Invalid Checksum error in show srp info cli even though there is no mismatch in srp config	upf

Bug ID	Headline	Product Found*
CSCvz47574	[UPF SVI] :- PCF initiated Dedicated bearer creation is not working [EPSFB] on hSMF	upf
CSCwd74056	[UPF] IPv4v6 PDN Data Statistics not updated correctly for packet drops due to flow discard	upf
CSCwe59504	[UPF-SVI]: sessmgr crash at sx_validate_pfcp_message()	upf
CSCwd18400	configurable CLI for hold-queue-size change to be persistent.	upf
CSCwb99802	UPFs sending unexpected Session Event Records (SERs)	upf
CSCwe33291	[UPF-SVI]: Continuous error logs on standby UPF "SMGR ID mismatch during recovery"	upf
CSCwe59457	[UPF-SVI]: sessmgr crash at sx_tun_fsm_handle_sess_mod_rsp_evt()	upf
* 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 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.

Table 4 - Resolved Bugs in this Release

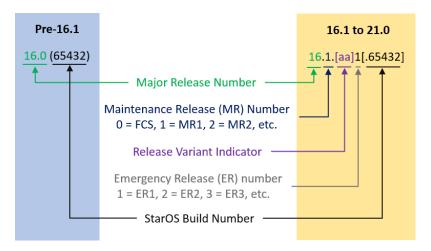| Bug ID	Headline	Product Found*
CSCwf09429	VPP NSH Fastpath Tables Not Initialized	cups-up
CSCwe21138	BP-ICUPS: sessmgr restart : sfw_nat_allocate_port_chunk_from_recovery_list()	pdn-gw
CSCwe70747	[BP-PGW] Gy_CCR-Termination message AVP’s validation is failed post the sessmgr/aaamgr recovery	pdn-gw
CSCwe95764	PGW-MPN: Session Manager restart happen during host-pool change	pdn-gw
CSCwd12198	[ICUPS-Smoke2] Assertion Failure @ acsmgr_config_acs_rule_options	pdn-gw
CSCwf01825	One way traffic reported after UE goes into assume positive state when CCR-U triggered by VT	pdn-gw
CSCwe35532	VPNMGR-INSTANCE 3 MEMORY ISSUE ON ICSR UPF pair	Upf
* 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.
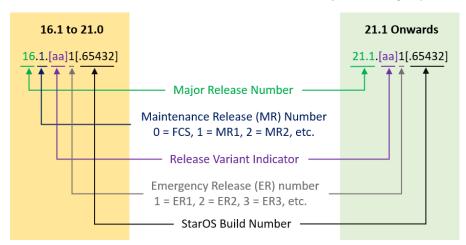
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build 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 4 provides descriptions for the packages that are available with this release.

Table 4 - Release Package Information

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
ASR 5500		
asr5500-<release>.zip	asr5500-<release>.bin	Contains 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>.zip	asr5500_T-<release>.bin	Contains 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.
StarOS Companion Package		
companion-<release>.zip	companion-<release>.tgz	Contains 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. In 21.12.0 and later releases, the StarOS companion package also includes 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.zip	qvpc-di-<release>.bin	Contains the VPC-DI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. In 21.12.0 and later releases, this package also includes 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.
qvpc-di_T-<release>.bin.zip	qvpc-di_T-<release>.bin	Contains the trusted VPC-DI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. In 21.12.0 and later releases, this package also includes 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.
qvpc-di-<release>.iso.zip	qvpc-di-<release>.iso	Contains the VPC-DI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image. In 21.12.0 and later releases, this package also includes 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.
qvpc-di_T-<release>.iso.zip	qvpc-di_T-<release>.iso	Contains the trusted VPC-DI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image. In 21.12.0 and later releases, this package also includes 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.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qvpc-di-template-vmware-<release>.zip	qvpc-di-template-vmware-<release>.tgz	Contains the VPC-DI binary software image that is used to on-board the software directly into VMware. In 21.12.0 and later releases, this package also includes 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.
qvpc-di-template-vmware_T-<release>.zip	qvpc-di-template-vmware_T-<release>.tgz	Contains the trusted VPC-DI binary software image that is used to on-board the software directly into VMware. In 21.12.0 and later releases, this package also includes 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.
qvpc-di-template-libvirt-kvm-<release>.zip	qvpc-di-template-libvirt-kvm-<release>.tgz	Contains the same VPC-DI ISO identified above and additional installation files for using it on KVM. In 21.12.0 and later releases, this package also includes 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.
qvpc-di-template-libvirt-kvm_T-<release>.zip	qvpc-di-template-libvirt-kvm_T-<release>.tgz	Contains the same trusted VPC-DI ISO identified above and additional installation files for using it on KVM. In 21.12.0 and later releases, this package also includes 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.
qvpc-di-<release>.qcow2.zip	qvpc-di-<release>.qcow2.tgz	Contains the VPC-DI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack. In 21.12.0 and later releases, this package also includes 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.
qvpc-di_T-<release>.qcow2.zip	qvpc-di_T-<release>.qcow2.tgz	Contains 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. In 21.12.0 and later releases, this package also includes 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-SI		
qvpc-si-<release>.bin.zip	qvpc-si-<release>.bin	Contains the VPC-SI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. In 21.12.0 and later releases, this package also includes 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.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qvpc-si_T-<release>.bin.zip	qvpc-si_T-<release>.bin	Contains the trusted VPC-SI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. In 21.12.0 and later releases, this package also includes 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.
qvpc-si-<release>.iso.zip	qvpc-si-<release>.iso	Contains the VPC-SI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image. In 21.12.0 and later releases, this package also includes 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.
qvpc-si_T-<release>.iso.zip	qvpc-si_T-<release>.iso	Contains the trusted VPC-SI ISO used for new deployments a new virtual machine is manually created and configured to boot from a CD image. In 21.12.0 and later releases, this package also includes 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.
qvpc-si-template-vmware-<release>.zip	qvpc-si-template-vmware-<release>.ova	Contains the VPC-SI binary software image that is used to on-board the software directly into VMware. In 21.12.0 and later releases, this package also includes 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.
qvpc-si-template-vmware_T-<release>.zip	qvpc-si-template-vmware_T-<release>.ova	Contains the trusted VPC-SI binary software image that is used to on-board the software directly into VMware. In 21.12.0 and later releases, this package also includes 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.
qvpc-si-template-libvirt-kvm-<release>.zip	qvpc-si-template-libvirt-kvm-<release>.tgz	Contains the same VPC-SI ISO identified above and additional installation files for using it on KVM. In 21.12.0 and later releases, this package also includes 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.
qvpc-si-template-libvirt-kvm_T-<release>.zip	qvpc-si-template-libvirt-kvm_T-<release>.tgz	Contains the same trusted VPC-SI ISO identified above and additional installation files for using it on KVM. In 21.12.0 and later releases, this package also includes 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.
qvpc-si-<release>.qcow2.zip	qvpc-si-<release>.qcow2.gz	Contains the VPC-SI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack. In 21.12.0 and later releases, this package also includes 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.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qvpc-si_T-<release>.qcow2.zip	qvpc-si_T-<release>.qcow2.gz	Contains 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. In 21.12.0 and later releases, this package also includes 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 Companion Package		
companion-vpc-<release>.zip	companion-vpc-<release>.tgz	Contains numerous files pertaining to this version of the VPC including SNMP MIBs, RADIUS dictionaries, ORBEM clients. These files pertain to both VPC-DI and VPC-SI, and for trusted and non-trusted build variants. In 21.12.0 and later releases, the VPC companion package also includes 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.
Ultra Service Platform		
usp-<version>.iso		The USP software package containing component RPMs (bundles). Refer to Table 5 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 5 for descriptions of the specific bundles.
usp_rpm_verify_utils-<version>.tar		Contains information and utilities for verifying USP RPM integrity.

Table 5 - 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.