Release Notes for the StarOS™ Software Version 2024.01.la0

First Published: February 29, 2024

Introduction

This Release Notes identifies changes and issues related to the Legacy Gateway (ASR 5500) software release.

Release Lifecycle Milestones

Release Lifecycle Milestone	Milestone	Date
First Customer Ship	FCS	29-Feb-2024
End of Life	EoL	29-Feb-2024
End of Software Maintenance	EoSM	29-Aug-2025
End of Vulnerability and Security Support	EoVSS	29-Aug-2025
Last Date of Support	LDoS	31-Aug-2026

Release Package Version Information

Software Packages	Version	Build Number
StarOS Package	2024.01.la0	21.28.9.92933

Descriptions for the various packages provided with this release are available in the

Release Package Descriptions section.

What's New in this Release

This version of Release Notes includes a new section titled **What's New in this Release** comprising all new features, enhancements, and behavior changes applicable for the release.

There are no new features or enhancements for this 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.

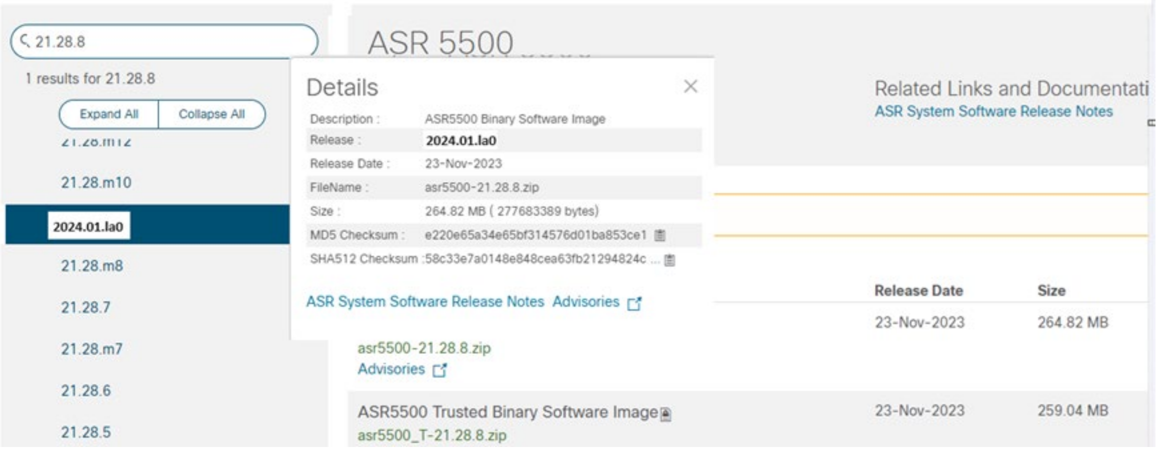
Firmware Updates

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.



Details

Description : ASR5500 Binary Software Image
Release : 2024.01.la0
Release Date : 23-Nov-2023
FileName : asr5500-21.28.8.zip
Size : 264.82 MB (277683389 bytes)
MD5 Checksum : e220e65a34e65bf314576d01ba853ce1
SHA512 Checksum :58c33e7a0148e848cea63fb21294824c ...

	Release Date	Size
asr5500-21.28.8.zip	23-Nov-2023	264.82 MB
ASR5500 Trusted Binary Software Image asr5500_T-21.28.8.zip	23-Nov-2023	259.04 MB

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 Table 1

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

In 2024.01 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.

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 for this Release

The following table lists the open bugs in this specific 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 2 - Open Bugs in this Release

Bug ID	Headline	Behavior Change
CSCwi94768	Documentation to update the max entries supported in Gx local-policy-service	cups-cp
CSCwj09524	Sx Failure seen when service port 1/10 goes down	cups-up
CSCwi69056	VPP buffer leak caused a VPP crash	cups-up
CSCwi35960	Huge amount of "ICMP packet parse failure" logs in 21.28.m15 with NAT	cups-up
CSCwi71670	X3 Lawful Intercept is marked as wrong EBI when using ipv6 session over dedicated bearer	cups-up
CSCwi52632	egtpu_process_update_req_evt()egtpu_handle_user_sap_event()sessmgr_up-lane_gtpu_tx_update()	cups-up
CSCwh58126	Fatal Signal 11: 11 PC: [0495e396/X] uplane_find_app_data_flow()	cups-up
CSCwh03670	Downlink total fp packets not shown correctly in case of http out of order packet	cups-up
CSCwi68424	Observing Sxdemux in warn/over state in Volte ICSR Standby UP nodes	cups-up
CSCwi55030	Observed multiple sessmgr went to warn/over state in 21.28.m18.92419 during re-gression	mme
CSCwd25108	DNS Failure - TCP READ, Kernel Closed - req_read_len = 0	mme
CSCwi88706	ADC detection accuracy is low for Telegram	pdn-gw
CSCwi69314	Planned swo gives incorrect message in ops-centre	rcm
CSCwi65948	Format of dateandtime used by RCM does not comply to snmpv2	rcm
CSCwi76266	SF/CF card reboots during VPC-DI system reboot on 21.28.mhx release	staros
CSCwj08070	intermittent rmmgr task failures on Hermes branch	staros
CSCwj07101	CF dual active caused by CF DI Internal duplex failure	staros
CSCwi26817	VPC DI keeps rebooting with ESC 6.0	staros
CSCwi59036	Port redundancy Failed in 4-port deployment VPC SI	staros
CSCwd99519	Error logs seen on UPF PDR not found with PDR ID 0x149 and Remove PDR PDR with ID 0x2ce	upf

Resolved Bugs for this Release

The following table lists the resolved bugs 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 3 - Resolved Bugs in this Release

Bug ID	Headline	Product Found
CSCwh90706	Invalid ARP value from PGW coming from the fix CSCwd32146	cups-cp
CSCwf58498	UL Data packet getting drop while CBresponse is pending and UL data came	cups-cp
CSCwi37202	Memory leak in function sessmgr_ggsn_sx_allocate_trans_info_node()	cups-cp
CSCwf12125	CUPS: Discrepancy between the time SGW CDR and the time CGF log	cups-cp

Bug ID	Headline	Product Found
CSCwi21602	Error log for SGW CDR Duration in future	cups-cp
CSCwi50450	HO failures due to invalid ARP value from PGW	cups-cp
CSCwi19980	Incorrect gtpc teid format in s8hr ims media packets	cups-cp
CSCwi68808	CCR-U request is not containing MSISDN information	cups-cp
CSCwh84055	CDRs are not sent after unplanned SF card migration after fix of CSCwe81062	cups-cp
CSCwd66214	Assertion failure at sess/snx/drivers/sgw/sgw_recovery.c:1277 on ICSR StandBY CP	cups-cp
CSCwh78561	GWC rejects directly CSR for some IMSIs with "no resources available"	cups-cp
CSCwh51263	CP does not create the Redirect-FAR for FUI-redirect on the second time	cups-cp
CSCwh43745	Assertion failure at sess/egtp/egtpc/egtpc_interface.c:280	cups-cp
CSCwh33064	CP is not sending Outer Header Removal IE for SxA uplink PDR for default bearer	cups-cp
CSCwe81062	CDRs are not sent after unplanned SF card migration	cups-cp
CSCwh12011	Multiple sessmgr restarts sgwdrv_epsb_fsm_st_connected_evt_s5_disconnected()	cups-cp
CSCwh79709	Error logs - ACS_SEF: CUPS SEF info allocation failed / PDR_ID crossed limit. 0, 0, 0	cups-cp
CSCwi61806	vpp restart fastpath_executive_node_fn on 21.28.m18	cups-up
CSCwi16517	VPP issues with 21.28.m14	cups-up
CSCwf34386	VPP restart	cups-up
CSCwi59651	VPP restart as /usr/sbin64/vpp(sn_assert_signal_handler	cups-up
CSCwi24925	vppctl errors seen on UP after Traffic Steering is enabled	cups-up
CSCwi51909	mmemgr restart at sbSqDeliver	mme
CSCwi37280	DNS - MME is not handling dns response in CNAME format properly as expected by customer	mme
CSCwi48857	Sessmgr Assertion failure at egtpc_send_req_msg()	mme
CSCwi23379	sessmgr failure at sess/egtp/egtpc/egtpc_interface.c:280	mme
CSCwi58326	mmemgr restarted at SNMME_PtLiHitUDatReq with PWS failure or Restart indication message from eNB	mme
CSCwi83811	QoS Validation Failure in Web authentication with LBO test case on 21.28.m19 Image	pdn-gw
CSCwh84412	User-Location-Information Avp is not changed for GGSN after Handoff	pdn-gw

Bug ID	Headline	Product Found
CSCwi26694	RTP stream is wrongly linked to Default bearer in LI reporting	pdn-gw
CSCwi54796	VPC-SI - bfd sometimes sending ipv6 packets with udp checksum 0x0 - which is invalid	pdn-gw
CSCwi47682	Gy Credit Control Request AVP for Subscription-ID (e.164) contains IMSI instead of MSISDN	pdn-gw
CSCwi71868	Usage Report Not Updating During Local Fallback	pdn-gw
CSCwi40532	sessmgr unexpected restart sess/ggsn/gtpc/gtp_enc_ie.c:4570	pdn-gw
CSCwh93900	RCM should reload old active UP after BGP monitor failure	rcm
CSCwi60684	Call loss during UP Manual Switchover by RCM for 21.28.x	rcm
CSCwh70845	"show apn statistics all" - huge increase of duration of command execution	sae-gw
CSCwf93799	session manager Assertion failure at sess/snx/drivers/sgw/sgw_epsb_fsm.c	sgw
CSCwh85618	hd raid CF2 disk is not used or available when CF1 is down	staros

Operator Notes

StarOS Version Numbering System

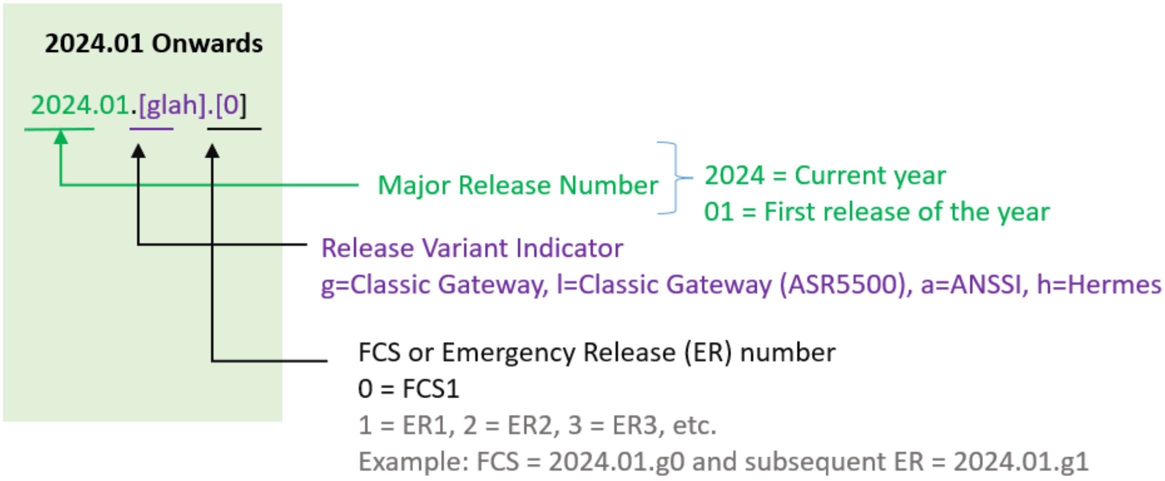
The output of the **show version** command displays detailed information about the version of StarOS currently running on the ASR 5500 or Cisco Virtualized Packet Core platform.

NOTE: Starting 2024.01.0 release (January 2024), Cisco is transitioning to a new release versioning scheme. The release version is based on the current year and product. Refer to **Figure** 1 for more details.

During the transition phase, some file names will reflect the new versioning whereas others will refer to the 21.28.x-based naming convention. With the next release, StarOS-related packages will be completely migrated to the new versioning scheme.

Version Numbering for FCS, Emergency, and Maintenance Releases

Figure 1 – Version Numbering


2024.01 Onwards
2024.01.[glah].[0]
Major Release Number
2024 = Current year
01 = First release of the year
Release Variant Indicator
g=Classic Gateway, l=Classic Gateway (ASR5500), a=ANSSI, h=Hermes
FCS or Emergency Release (ER) number
0 = FCS1
1 = ER1, 2 = ER2, 3 = ER3, etc.
Example: FCS = 2024.01.g0 and subsequent ER = 2024.01.g1

Release Package Descriptions

Table 4 provides descriptions for the packages that are available with this release. For more information about the release packages up to 21.28.x releases, refer to the corresponding releases of the release note.

Table 4 - Release Package Information

Software Package	Description
ASR 5500	
asr5500-<release>.zip	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	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	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.
VPC-DI	
qvpc-di-<release>.bin.zip	Contains the VPC-DI binary software image that is used to replace a previously deployed image on the flash disk in existing installations.
qvpc-di_T-<release>.bin.zip	Contains the trusted VPC-DI binary software image that is used to replace a previously deployed image on the flash disk in existing installations.s
qvpc-di-<release>.iso.zip	Contains 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.zip	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.
qvpc-di-template-vmware-<release>.zip	Contains the VPC-DI binary software image that is used to on-board the software directly into VMware.
qvpc-di-template-vmware_T-<release>.zip	Contains the trusted VPC-DI binary software image that is used to on-board the software directly into VMware.
qvpc-di-template-libvirt-kvm-<release>.zip	Contains the same VPC-DI ISO identified above and additional installation files for using it on KVM.
qvpc-di-template-libvirt-kvm_T-<release>.zip	Contains the same trusted VPC-DI ISO identified above and additional installation files for using it on KVM.
qvpc-di-<release>.qcow2.zip	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.
qvpc-di_T-<release>.qcow2.zip	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.
VPC-SI	
qvpc-si-<release>.bin.zip	Contains the VPC-SI binary software image that is used to replace a previously deployed image on the flash disk in existing installations.
qvpc-si_T-<release>.bin.zip	Contains the trusted VPC-SI binary software image that is used to replace a previously deployed image on the flash disk in existing installations.
qvpc-si-<release>.iso.zip	Contains 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.zip	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.
qvpc-si-template-vmware-<release>.zip	Contains the VPC-SI binary software image that is used to on-board the software directly into VMware.
qvpc-si-template-vmware_T-<release>.zip	Contains the trusted VPC-SI binary software image that is used to on-board the software directly into VMware.
qvpc-si-template-libvirt-kvm-<release>.zip	Contains the same VPC-SI ISO identified above and additional installation files for using it on KVM.
qvpc-si-template-libvirt-kvm_T-<release>.zip	Contains the same trusted VPC-SI ISO identified above and additional installation files for using it on KVM.
qvpc-si-<release>.qcow2.zip	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.
qvpc-si_T-<release>.qcow2.zip	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.
VPC Companion Package	

companion-vpc-<release>.zip	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.
Ultra Services Platform	
usp-<version>.iso	The USP software package containing component RPMs (bundles). Refer to the 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 the 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, refer to https://www.cisco.com/c/en/us/support/index.html.

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 ANYKIND, 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 WITHTHE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSEOR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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 of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.