Release Notes for the StarOS™ Software Version 2024.03.I0

First Published: July 31, 2024

Introduction

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

Release Lifecycle Milestones

Release Lifecycle Milestone	Milestone	Date
First Customer Ship	FCS	31-Jul-2024
End of Life	EoL	31-Jul-2024
End of Software Maintenance	EoSM	30-Jan-2026
End of Vulnerability and Security Support	EoVSS	30-Jan-2026
Last Date of Support	LDoS	29-Jan-2027

Release Package Version Information

Software Packages	Version	Build Number
StarOS Package	2024.03.I0	21.28.m25.94479

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

Verified Compatibility

Products	Version
ADC P2P Plugin	2.74.2.2209
RCM	20240715-043754Z
NED Package	ncs-6.1.6.1-nso-mob-fp-3.5.1-b3a2303-2024-07-24T0350 ncs-6.1.6.1-nso-mob-fp-3.5.1-b3a2303-2024-07-24T0350.tar.gz
NSO-MFP	6.1.6.1-3.5.1

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.

Features and Enhancements

This section covers a brief description of the features and enhancements introduced in this release.

Feature ID	Feature Name	Product
FEAT-28314	Standard IMSI Privacy support on ePDG	epdg
FEAT-26639	Address Hold Timer CLI	pdn-gw

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.

Synchronizing Boot File for Service Function Cards

To synchronize the boot file for all the Service Function (SF) VPC-DI non-management cards, use the following:

CLI executable command:

```
[local] host_name# system synchronize boot
```

This assures that the changes in boot file are identically maintained across the SF cards.

Ensure that you execute this command before reload for version upgrade from any version less than mh14 to

mh14 or later.

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.** Click **Linux,** and then choose the Software Image Release Version**.**

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 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	Product Found
CSCwk67137	[CUPS / LIVE / CP / 21.28.h7] Di-Net Heartbeat drop > 1% - Health status = Bad	cups-cp
CSCwk82412	CUPS UP - TCP flow classification breaks and flow readdressing is not working afterwards	cups-up
CSCwj59047	[BP-CUPS] Fatal Signal 6: Aborted PC: [f7f63062/X] ld-linux.so.2/_dl_sysinfo_int80()	cups-up
CSCwi68424	Observing Sxdemux in warn/over state in Volte ICSR Standby UP nodes	cups-up
CSCwk95168	[BP-CUPS] Performance improvement required in user-plane data path	cups-up
CSCwk65512	ipsecmgr cpu warn/over with device certificate and imsi privacy make-break	epdg
CSCwk81092	[CP-MME] Observed mmemgr restart and after mmemgr task kill its going to warn state	mme
CSCwk89076	[CP-MME] Observed vpnmgr restart after 24hrs longevity run(VPC-DI)	mme
CSCwk77504	21.28.mhx: SNMP traps not getting generated for NTP states	staros
CSCwj73773	Post unplanned MIO switchover all services failed to start and all contexts went into Initializing	staros

Bug ID	Headline	Product Found
CSCwj67156	RTNETLINK socket recv buffer under run error code 105 on hermes branch sw build on CUPS CP	staros

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
CSCwk52721	Home & roamer subscriber type changed to visitor after multiple sessmgr & aaamgr killed by sessctrl	cups-cp
CSCwk37340	S-CDRs showing future timestamp in changetime after TAI change	cups-cp
CSCwk57433	CUPS-CP - sxdemux 220446 error - SxCtrlmgr: No peer entry in Up Grp Name: GGN20990B-UP1	cups-cp
CSCwk45376	sxdemux restarts at sxmgr_handle_get_sx_peer_table	cups-cp
CSCwj84745	Sx IP Pool is in Disable state	cups-cp
CSCwk30287	TNL failures observed during Nokia CMM TAC migration to Cisco CUPS	cups-cp
CSCwk66031	CUPS CP: servingNodePLMNIdentifier field missing in CDR while in servers unreachable	cups-cp
CSCwk31021	On CUPS-CP node multiple session manager restarts observed after SRP switchover	cups-cp
CSCwj98143	show boot initial-config displays "encrypted li errors" on CP with trusted build only	cups-cp
CSCwh20742	Assertion failure at saegwdrv_ue_fsm_st_active_evt_snx_abortcall()	cups-cp
CSCwf13605	ipsecdemux crash on asr5500 during crypto call model longevity	epdg
CSCwd51494	IPsecMgr task restart while decrypting packets.	epdg
CSCwk03546	Multiple AAAMGR are in warn state	epdg
CSCwf18184	Multiple Ipsecmgr's are in warn state in 21.28.m3 build	epdg
CSCwe17332	IpsecDemux process restart due to invalid IpsecMgr id	epdg
CSCwf94414	ipsecmgr memory leak when certificate chain used for authentication	epdg
CSCwj44782	MME wrongly selecting s2b PGW record (x-3gpp-pgw:x-s2b-gtp+nc-smf) for 5G capable UE's	mme

Bug ID	Headline	Product Found
CSCwi07732	MMENewConnectionDisallowed and allowed Traps are continuously generating	mme
CSCwd40838	mme sessmgr restart at mme_app_do_sgw_dns_query	mme
CSCwj72131	Improper output for PDN GW Name in 'show mme-service db record ' is a display issue.	mme
CSCwe54989	MME is not checking encryption algorithms with default integrity-algorithm-lte config	mme
CSCwk24742	MME sending ipv6 in notify request even when receiving dual ip addresses in create session response.	mme
CSCwj36352	Assertion failure at sess/mme/mme-app/app/mme_tau_proc.c:1701	mme
CSCwk63359	vpnmgr task restarts due to DNS Timeouts/ServFail	mme
CSCwj54636	Abnormal reject PDN connectivity by "PTI already in Use"	mme
CSCwj57663	Remove mme_app_send_multipath_zero_action_recovery_req API from mme_app_ope()	mme
CSCwk57922	Abrupt increase observed for 4G-Inroamers in MMEs	mme
CSCwk12300	Healing Support || CUPS	nso-mfp
CSCwj52492	While triggerring the interim CDR, there is no aaa_sess_handle and sessmgr restart	pdn-gw
CSCwj78838	Assertion failure at "sit_api_rct_task_death_req" on 21.28.m23.93362	pdn-gw
CSCwj02791	sessmgr restart occurs when session moves to assume positive state	pdn-gw
CSCwj66981	Sessmgr crash-egtpc_send_ind_evt()	pdn-gw
CSCwj31708	[RCM] checkpointmgr restart @redmgrtcplocal.go:733	rcm
CSCwh00793	Assertion failure at sess/sgsn/sgsn-app/sm/smg_fsm_table Function: SmGenDownLinkDataInd()	sgsn
CSCwj68378	ASR5500 SPGW Assertion failure at sgwdrv_send_tx_setup_to_egtpu	sgw
CSCwj68218	Assertion failure at sgwdrv_collect_pdn_info	sgw
CSCwk63293	Nessus scan: High- CVE-2024-6387- OpenSSH < 9.8 RCE	staros
CSCwd75750	ipsecmgr_process_crashed at ipm_sad	staros
CSCwk27008	FSC cards with SSD HGST 400GB HUSMM3240ASS204 require SSD firmware update to version C17D	staros
CSCwk08792	[21.28.h6] BGP Routes Lost after Demux SF Restart	staros

Operator Notes

StarOS Version Numbering System

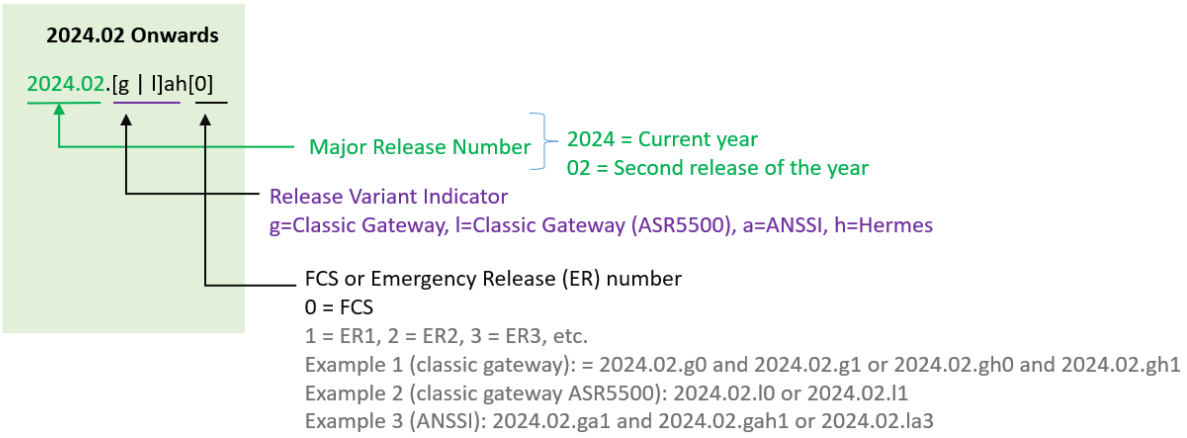
The output of the **show version** command displays detailed information about the version of StarOS currently running on the ASR 5500 or Cisco Virtualized Packet Core platform.

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



Note: For any clarification, contact your Cisco account representative.

Release Package Descriptions

Table 4 provides examples of packages according to the 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.
VPC Companion Package	

companion-vpc-<release>.zip For example, companion-vpc-2024.02.gh2.i4.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.
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.
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	
intelligent_onboarding-<release>.zip	Contains the VPC-SI onboarding signature package that is used to replace a previously deployed image on the flash disk in existing installations.
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.
RCM	
rcm-vm-airgap-<release>.ova.zip	Contains the RCM software image that is used to on-board the software directly into VMware.
rcm-vm-airgap-<release>.qcow2.zip	Contains the RCM software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack.
rcm-vm-airgap-<release>.vmdk.zip	Contains the RCM virtual machine disk image software for use with VMware deployments.
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.

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.

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 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.

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: http://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)