Release Notes for the StarOS™ Software Version 2025.01.gah0

First Published: January 31, 2024

Introduction

This Release Notes identifies changes and issues related to the Control and User Plane Separation (CUPS) software releases.

Products Qualified and Released in this Release

Products	Qualified Yes/No
cups-cp	Yes
cups-up	Yes
mme	No
ePDG	No
pdn-gw	No
saegw	No
sgsn	No
Platforms	
ASR 5500	No
VPC-DI	Yes
VPC-SI	Yes

Cisco Systems, Inc.   www.cisco.com

Release Lifecycle Milestones

Release Lifecycle Milestone	Milestone	Date
First Customer Ship	FCS	31-Jan-2025
End of Life	EoL	31-Jan-2025
End of Software Maintenance	EoSM	01-Aug-2026
End of Vulnerability and Security Support	EoVSS	01-Aug-2026
Last Date of Support	LDoS	31-Aug-2027

Release Package Version Information

Software Packages	Version	Build Number
StarOS Package	2024.04.gah0	21.28.h12.96494

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.h3.2586
RCM	20241016-104205Z
CVIM	5.0.1
ESC	6.0.0.50
Host OS	RHEL 9.2
RedHat OpenStack	RHOSP 17.1
XL710 NIC Version	Driver: 5.14.0-284.30.1.el9_2.x86_64 Firmware: 7.00 0x80005119 0.385.115
CIMC Version (UCS C220-M5)	4.1(2a)

Note: Use only these compatible software versions for the products qualified in this release.

What's New in this Release

Features and Enhancements

There are no specific features and enhancements introduced in 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.

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
CSCwn06583	While performing SGW Relocation getting error as EGTP_CAUSE_PEER_NOT_RESPONDING	cups-cp
CSCwm74110	[CUPS 21.28] Reboot SF Demux leads to BFD sessions DOWN on Standby Card	cups-cp
CSCwk67137	[CUPS / LIVE / CP / 21.28.h7] Di-Net Heartbeat drop > 1% - Health status = Bad	cups-cp
CSCwk79042	[CUPS-UP] SX path failure is not leading to SRP switchover with sx monitor enabled	cups-up
CSCwm51816	sessmgr task restarted on UP, when LI and S8hr interception call is getting cleared	cups-up

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
CSCwn12434	SAEGW is ignoring GTPC messages	cups-cp
CSCwj29750	Sessmgr restart after SW upgrade to 21.28.m19, mme_auth_awt_hss_hss_resp()	mme
CSCwn29026	sessmgr crash at mme_auth_awt_hss_hss_resp()	mme
CSCwm63294	Rewriting clear-route-multipath-zero CLI to be inline with other config CLIs	mme
CSCwm67862	Credit Control Failure Handling is showing UNKNOWN	pdn-gw
CSCwm47392	Sessmgr restarts after enabling VoLTE for specific inroamer IMSIs ranges	pdn-gw
CSCwm49666	SGW sends LTE-M on S8, though LTEMPI isn't set	sgw

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.
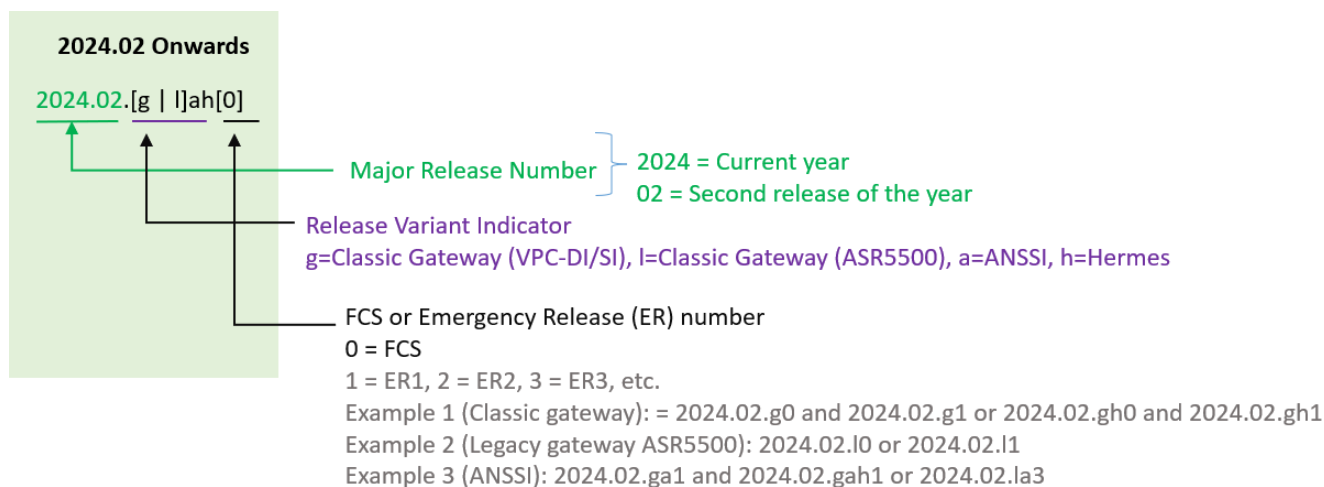
NOTE: Starting 2024.01.0 release (January 2024), Cisco is transitioning to a new release versioning scheme. The

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

2024.02 Onwards

2024.02.[g | l]ah[0]

Major Release Number — 2024 = Current year
02 = Second release of the year

Release Variant Indicator
g=Classic Gateway (VPC-DI/SI), l=Classic Gateway (ASR5500), a=ANSSI, h=Hermes

FCS or Emergency Release (ER) number
0 = FCS
1 = ER1, 2 = ER2, 3 = ER3, etc.
Example 1 (Classic gateway): = 2024.02.g0 and 2024.02.g1 or 2024.02.gh0 and 2024.02.gh1
Example 2 (Legacy gateway ASR5500): 2024.02.l0 or 2024.02.l1
Example 3 (ANSSI): 2024.02.ga1 and 2024.02.gah1 or 2024.02.la3

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

StarOS Configuration Recommendations for VPC-DI

Configure the following StarOS-level settings in the **staros_param.cfg** file to set up the day-0 cloud configuration for the VNF.

Enable the boot parameter to move KNI packets over MCDMA threads by setting KNI_ON_MCDMA_THREAD_ENABLE=1.

Troubleshooting Information

Issue: VIP accessibility for VPC-DI instances deployed via ESC on Openstack using the ML2/OVN mechanism driver may be problematic.

Workaround:

1. Identify the CF1 and CF2 ports on the management network within Openstack

2. Configure **allowed_address_pairs** for these ports to match the virtual port IP address (use /32 notation)

3. Avoid using CIDR format IP addresses for **allowed_address_pairs** on these ports

4. Execute the following command to set the allowed address **pairs:openstack port set** <CF-mgmt-port-ID> -- **allowed-address ip-address**=<VIP-address>,**mac-address**=<CF-mgmt-port-MAC-address>

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.