Release Notes for StarOS™ Software, Release 2025.04.gah0

Contents

StarOS™ Software, Release 2025.04.gah0

This Release Notes identifies changes and issues that are related to the Control, and User Plane Separation (CUPS) software release.

Qualified products and platforms

Table 1. Products and platforms qualified in this release

Component	Qualified?
Products	
CUPS	Yes
MME	No
ePDG	No
P-GW	No
SAEGW	No
SGSN	No
Platforms	
ASR 5500	No
VPC-DI	Yes
VPC-SI	Yes

Release lifecycle milestones

The following table provides EoL milestones for Cisco StarOS software:

Table 2. EoL milestone information for StarOS™ Software, Release 2025.04.gah0

Milestone	Date
First Customer Ship (FCS)	31-Oct-2025
End of Life (EoL)	31-Oct-2025
End of Software Maintenance (EoSM)	01-May-2027
End of Vulnerability and Security Support (EoVSS)	01-May-2027
Last Date of Support (LDoS)	30-Apr-2028

These milestones and the intervals between them are defined in the Cisco ASR 5500 and Ultra Packet Core software release lifecycle product bulletin available on cisco.com.

New software features

There is no new software features introduced in this release.

Changes in behavior

There is no behavior changes introduced in this release.

Resolved issues

This table lists the resolved issues in this specific software release.

Note: This software release may contain bug fixes first introduced in other releases. To see additional information, click the bug ID to access the Cisco Bug Search Tool. To search for a documented Cisco product issue, type in the browser: <bug number> site:cisco.com.

Table 3. Resolved issues for StarOS™ Software, Release 2025.04.gah0

Bug ID	Description	Product Found
CSCwq20529	vpnmgr restart at function vpnmgr_lookup_pool_by_id_slow()	cups-cp
CSCwq30875	Session manager recovery status instability	cups-cp
CSCwo94253	3GPP-Reporting-Reason VALIDITY_TIME in the CCR-U after GY RAR	cups-cp
CSCwp20248	CP is not sending Delete session request to UP incase of GTPU Path Failure	cups-cp
CSCwo33578	Unexpected session disconnection	cups-cp
CSCwm50323	Call reject with lpool-ip-validation-failed with No Chunks to allocate from this pool	cups-cp
CSCwk31021	On CUPS-CP node multiple session manager restarts observed after SRP switchover	cups-cp
CSCwq31050	sessmgr reload after ECS configuration modification	cups-cp
CSCwo01479	unplanned SF migration caused diamproxy instance # out of range	staros
CSCwq77638	Legacy-GW: kernel panic with sessmgr checkpointing issue observed in osp16 and osp17 setup	staros

Open issues

This table lists the open issues in this specific software release.

Note: This software release may contain open bugs first identified in other releases. To see additional information, click the bug ID to access the Cisco Bug Search Tool. To search for a documented Cisco product issue, type in the browser: <bug number> site:cisco.com.

Table 4. Open issues for StarOS™ Software, Release 2025.04.gah0

Bug ID	Description	Product Found
CSCwq38956	Interfaces are down Post upgrade : 21.28.h14.98513	cups-up
CSCwr83413	Unexpected DeleteSessionRequest after UEContextReleaseRequest	mme
CSCwr60848	CUTO Ctrl and VPP library version is not displaying	sae-gw

Known issues

This section describes the known issue that may occur during the upgrade of the StarOS image.

Install 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.

When upgrading the StarOS image from a previous version to the latest version, issues may arise if there is a problem with the Cisco SSH/SSL upgrade. To avoid such issues, ensure that the boot file for Service Function (SF) cards is properly synchronized.

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

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

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

Note: Ensure that you execute the system synchronize boot command before reloading for version upgrade from any version earlier than 21.28.h8 to version 21.28.h8, or versions higher than 21.28.h8.

Compatibility

This section provides compatibility information about the StarOS package version, and the software requirements for the CUPS software release.

Compatible StarOS package version

Table 5. Release package version information

StarOS packages	Version	Build number
StarOS package	2025.04.gah0	21.28.h15.99196

Compatible software components for CUPS

This table lists only the verified basic software and hardware versions. For more information on the verified software versions for the products qualified in this release contact the Cisco account representative.

Table 6. Compatibility information for Release 2025.04.gah0

Supported software	Version
ADC P2P plugin	2.74.h7.2683 **Note**: The 2025.04.gah0 StarOS software is compatible only with 2.74.h7.2683 or before P2P plugin version.

Supported software packages

This section provides information about the release packages associated with CUPS software.

Table 7. Software packages for Release 2025.04.gah0

Software package	Description
VPC companion package	
companion-vpc-2025.04.gah0.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-2025.04.gah0.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-2025.04.gah0.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-2025.04.gah0.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-2025.04.gah0.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-2025.04.gah0.zip	Contains the VPC-DI binary software image that is used to on-board the software directly into VMware.
qvpc-di-template-vmware_T-2025.04.gah0.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-2025.04.gah0.zip	Contains the same VPC-DI ISO identified above and additional installation files for using it on KVM.
qvpc-di-template-libvirt-kvm_T-2025.04.gah0.zip	Contains the same trusted VPC-DI ISO identified above and additional installation files for using it on KVM.
qvpc-di-2025.04.gah0.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.
VPC-SI	

Software package	Description
intelligent_onboarding-2025.04.gah0.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-2025.04.gah0.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-2025.04.gah0.iso.zip	Contains the VPC-SI ISO used for new deployment. A new virtual machine is manually created and configured to boot from a CD image.
qvpc-si-template-vmware-2025.04.gah0.zip	Contains the VPC-SI binary software image that is used to on-board the software directly into VMware.
qvpc-si-template-libvirt-kvm-2025.04.gah0.zip	Contains the same VPC-SI ISO identified above and additional installation files for using it on KVM.
qvpc-si-2025.04.gah0.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.

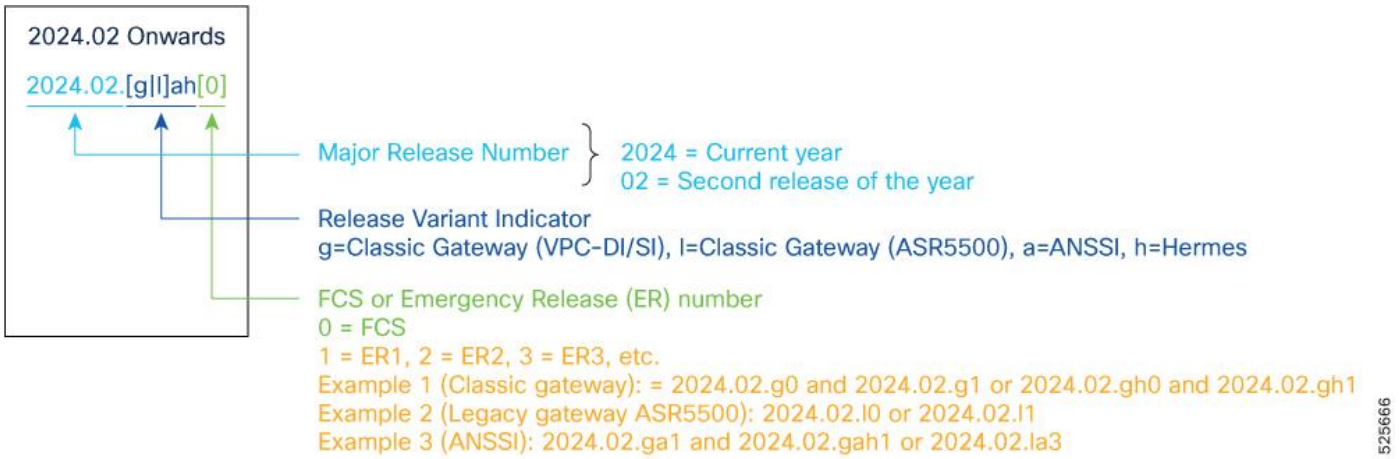
StarOS product version numbering system

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.

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 the figure for more details.

Note: 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.

Figure 1. Version numbering for FCS, emergency, and maintenance releases



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

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 the table and verify that it matches the one provided on the software download page. To calculate a SHA512 checksum on your local desktop see the table.

Table 8. 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`

Note: filename is the name of the file. extension is the file extension (for example, .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.

Related resources

This table provides key resources and links to the support information and essential documentation for StarOS products.

Table 9. Related resources and additional information

Resource	Link
Cisco ASR 5500 documentation	StarOS-based gateway and reference documentation
Cisco Ultra Packet Core documentation	CUPS documentation
Service request and additional information	Cisco Support

Legal information