Release Notes for StarOS™ Software, Release 2026.01.gh0

Contents

StarOS™ Software, Release 2026.01.gho

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

The key highlights of this release include:

- **MME disaster roaming enhancement**: MME now maintains ongoing emergency calls for disaster-roaming users when reverting to normal operation, while new roaming attach requests are rejected; existing sessions continue with support for TAU and handovers.
- **ePDG RTT enhancements**: ePDG supports additional RTT fields for procedures over the SWu and SWm interfaces.
- **Granular APN tracking and reporting**: Supports TLVs containing APN and Virtual APN in pilot packets, enabling more granular tracking, context-specific policy application, and APN-level reporting based on pilot packet data.
- **Enhanced ePDG observability**: Introduces new bulk statistics counters for IPSec and IKEv2 authentication to improve monitoring and observability.
- 16K UE Radio Capability IE feature support on VPC-DI platform.

For more information about the StarOS product documentation, see the Related resources section.

Qualified products and platforms

Table 1. Products and platforms qualified in this release

Component	Qualified?
Products	
CUPS	Yes
MME	Yes
ePDG	Yes
P-GW	Yes
SAEGW	Yes
SGSN	Yes
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 2026.01.gh0

Milestone	Date
First Customer Ship (FCS)	30-Jan-2026
End of Life (EoL)	30-Jan-2026
End of Software Maintenance (EoSM)	31-July-2027
End of Vulnerability and Security Support (EoVSS)	31-July-2027
Last Date of Support (LDoS)	31-July-2028

New software features

This section provides a brief description of the new software features introduced in this release.

Table 3. New software features for StarOS™ Software, Release 2026.01.gh0

Product impact	Feature	Description
Ease of Use	MME continues existing emergency calls from disaster-roaming UEs after reverting operator-policy config	When a network operator recovers from an outage or disaster and reverts its configuration from " disaster roaming mode" back to " normal operation, this feature prevents the MME from dropping existing emergency calls. While new roaming attach requests are rejected under the normal policy, existing emergency sessions are allowed to continue, including support for Tracking Area Updates (TAU) and Handovers. MME has been qualified for the above requirement in this release.
Ease of Use	ePDG RTT Enhancements	This feature enhances ePDG by supporting additional RTT fields for procedures over the SWu and SWm interfaces. These enhancements improve monitoring and troubleshooting by capturing specific details related to IKEv2 procedures and Diameter EAP procedures. IE Numbers 13, 80, 86, 87, 88, 148, 159, 160, 162, and 163 are supported with this release.
Software Reliability	Add TLVs containing APN and Virtual APN to Pilot Packets	This feature introduces support for including APN Name and Virtual APN Name as optional TLV attributes in pilot packets generated for subscriber session events. With this enhancement, external systems can perform more granular tracking, apply context-specific policies, and generate APN-level reports based on pilot packet data. The feature is configurable per context and applies to all pilot packet triggers.
Software Reliability	ePDG IPSec and IKEv2 KPI Enhancements	This feature supports ePDG observability with new bulk statistics counters for IPSec and IKEv2 authentication. The KPIs provide visibility into IKE_SA_INIT and IKE_AUTH exchanges, Including phase-level (P1, P2 and P3) authentication statistics for EAP-AKA method. Separate statistics provided for 5G sessions based on N1 mode capability. These counters

Product impact	Feature	Description
		are available through bulk statistics, as part of system schema.
Software Reliability	Password Complexity Enhancement	Enhances security by enforcing stronger password validation for locally configured user accounts. When `policy-strict-check keyword is` enabled, passwords must meet defined complexity and length requirements; noncompliant passwords are rejected. The feature is disabled by default, retains legacy behavior when disabled, and supports backward compatibility across upgrades and downgrades. Command introduced to enable : **configure** **context** context_nam [**password complexity ansi-t1.276-200 policy-strict-check**] Command introduced to disable: **configure** **context** context_name [**default password complexity**]
Upgrade	16K UE Radio Capability IE support qualification	The 16K UE Radio Capability feature is supported on the VPC-DI platform.

Changes in behavior

This section provides a brief description of the behavior changes introduced in this release.

Table 4. Behavior changes for StarOS™ Software, Release 2026.01.gh0

Description	Behavior changes
Cap on zero volume CDRs for secondary RAT records (CSCwr48395)	**Previous behavior**: When the CLI command gtpp suppress-cdrs zero-volume external-trigger-cdr was configured, all Zero Volume interim CDRs generated due to external triggers were suppressed, regardless of the number of secondary RAT records. **New behavior**: With the CLI command configured, Zero Volume interim CDRs generated due to external triggers are suppressed only up to 255 secondary RAT records. Once the limit of 255 secondary RAT records is reached, a Zero Volume external-trigger CDR will be generated.

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 5. Resolved issues for StarOS™ Software, Release 2026.01.gh0

Bug ID	Description	Product Found
CSCwr10359	Sessmgr restarted at function egtpc_handle_user_sap_event	cups-cp

Bug ID	Description	Product Found
CSCwr21255	Sessmgr restart seen on CP during call bring-up with VoGx enabled configuration	cups-cp
CSCwr87117	Wrong Time Quota observed in second SX_SESSION_MODIFICATION_REQUEST when new quota with RAR Trigger	cups-cp
CSCws16804	Sx Sess-Mod-Req failure with CC 69 Mandatory IE Incorrect	cups-cp
CSCws31425	sxdemux task memory usage high leading to a restart	cups-cp
CSCws71837	Subscriber is remaining in SU state after OCS is back online	cups-cp
CSCwq57920	Addition of a trap after the state of the peer user plane changes from configured to not configured or vice versa.	cups-cp
CSCwr15845	Gy session out of SU reports huge volume threshold in SxModify	cups-cp
CSCws41471	DHCP service sends IMSI instead of configured MSISDN in DHCP request	cups-up
CSCws26321	The ERAB Failed List IE is missing in the Path Switch Acknowledge message when the Path Switch Request contains invalid tunnel details.	mme
CSCws48490	DNS Records used for selecting AMF peer not released	mme
CSCwr32050	Emergency call-garbage value seen in bulkstat and show mme-ser statistics lte-emergency-profile profile-name lte1	mme
CSCwr48395	sessmgr restart at sn_aaa_client_action_item_lookup_by_key()	pdn-gw
CSCws18654	Legacy-GW: VzW ASR5500: sessmgr restart observed during configuration of new apn, new rulebase, new fw-nat-policy, and SRP switchover	pdn-gw
CSCwr95955	PGW (VPC) incorrectly charges for Router Solicitation (RS) packets in IPv6 sessions	pdn-gw
CSCwr56361	Assertion failure: EGTP-C service is being used by another MME/SGW/PGW service	pdn-gw
CSCws62168	P-CSCF Address Missing in CSRsp When DNS Returns Only CNAME Without Resource Records	pdn-gw
CSCws13802	Traffic is being re-directed in error by the PGW due to GOR ruledef update	pdn-gw
CSCwr44475	UDP quic traffic detection problem	pdn-gw
CSCwq60822	PGW is sending '0x40' for IpAddress instead of '0x04'	pdn-gw
CSCws98057	boot config change shows " Warning: Configuration was generated using a different chassis key"	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 6. Open issues for StarOS™ Software, Release 2026.01.gh0

Bug ID	Description	Product Found
CSCws71795	Resource Allocation Failure due to ACS_RULE_OPTION_LIST_MATCHING_FLOW_NOT_FOUND	cups-cp
CSCwq07274	Difference in the volume reported in Sx-Volume Measurement and monsub- CALL STATS	cups-up
CSCws98127	Wrong USERNAME is getting displayed in show sub all cli output	cups-up
CSCws50662	Assertion failure at diameter/diabase/diabase'	pdn-gw
CSCws66809	GW is sending CCR-U with charging rule report with cause " Rule-Failure-Code: UNSUCCESSFUL_QOS_VALIDATION"	pdn-gw
CSCws47044	PGW Session Setup Failure: Static IPv4 Address Mismatch for APN " nemo-cust101"	pdn-gw
CSCws47075	Unable to convert date-time string in the Diameter credit-control-request message processing	pdn-gw
CSCws05111	Legacy-GW: sessmgr checkpoint issue observed in osp17 vpcdi after card migrations	staros
CSCws98057	boot config change shows " Warning: Configuration was generated using a different chassis key"	staros

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.

Note: Cisco recommends offline upgrade-downgrade for CUPS CP VPC-DI ICSR deployments.

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: Execute the system synchronize boot command before reloading for version upgrade from any version earlier than 21.28.mh14 to version 21.28.mh14 or versions higher than 21.28.mh14.

Upgrade the confd version

This section explains upgrading third-party software. Upgrade the confd software to ensure system compatibility and performance.

Note: During July 2025.03.0 release, confd is upgraded to 8.1.16.2 version.

Prerequisites:

- Ensure you have appropriate permissions to perform this upgrade.
- Back up all necessary data and configurations to avoid permanent loss during file deletion.

Perform these steps to upgrade the confd version on the system.

1. Enter the debug shell using debug shell command.
2. Navigate to the confd directory.
3. Run the command:cd /mnt/hd-raid/meta/confd/ to access the directory.
4. Remove existing files with the command; rm -rf *

All files and subdirectories are deleted, preparing the system for a fresh installation. To preserve data across the Method of Procedure, users with ConfD configured must contact their Cisco representative.

Method of Procedure (MOP): Upgrade/Downgrade Between Non-Hermes and Hermes Builds

CSCwr80301: HD-RAID Not Ready During Upgrade from Non-Hermes to Hermes

Issue: When upgrading from a non-Hermes (202x.0x.gx) to a Hermes (202x.0x.ghx) build on both Virtualized Packet Core–Distributed Instance (VPC-DI) and Virtualized Packet Core–Single Instance (VPC-SI) platforms, the HD-RAID may not come up as expected.

Workaround: To avoid this hd-raid failure, follow the steps below during the upgrade and downgrade (for example, from 2025.03.g0 to 2026.01.gh0):

1. Pre-requisite: Back up all files stored in /hd-raid before upgrading from the .mx to .mhx build.

   Note: All data in /hd-raid will be lost during recovery.
2. Before the upgrade: On the .mx build, run the hd raid clear command.
3. Reboot and upgrade: Reboot the node to upgrade to the .mhx build.
4. Perform the CF card migration in case of VPC-DI or Reload the chassis on VPC-SI. Wait for the HD-RAID to recover.

   Note: It is recommended to use this Method of Procedure (MOP) for both upgrading and downgrading between Hermes and Non-Hermes StarOS builds.

Compatibility

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

Compatible StarOS package version

Table 7. Release package version information, Release 2026.01.gh0

StarOS packages	Version	Build number
StarOS package	2026.01.gh0	21.28.mh34.99750

Compatible software and hardware components

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 8. Compatibility software and hardware information, Release 2026.01.gh0

Product	Version
ADC P2P Plugin	2.74.gh1.2763
RCM	20260120-131924Z **Note**: Use this link to download the RCM package associated with the software
ESC	6.0.0.55
CVIM	5.0.4
Host OS	Ubuntu 22.04 / RHEL 8.4
RedHat OpenStack	RHOSP 17.1
E810C NIC Version	Driver version: ice 1.12.6 Firmware: 4.20 0x80018f67 0.387.18
CIMC	4.0 (4)
NED Package	ncs-6.1.11.2-nso-mob-fp-3.5.2-ad74d4f-2024-10-18T1052 ncs-6.1.11.2-nso-mob-fp-3.5.2-ad74d4f-2024-10-18T1052.tar.gz
NSO/MFP	nso-mob-fp-3.5.2.2024.04.g0 **Note**: MFP is qualified only with RHOSP 13.
SMI/CNDP	2026.01.1.08

Note: CVIM and ESC versions are qualified as part of 2025.04.0 release.

Supported software packages

This section provides information about the release packages associated with Control, and User Plane Separation (CUPS) software.

Table 9. Software packages for Release 2026.01.gh0

Software package	Description
NSO	
nso-mob-fp-3.5.2-2026.01.gh0.zip	Contains the signed NSO 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-2026.01.gh0.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-2026.01.gh0.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-2026.01.gh0.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-2026.01.gh0.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-2026.01.gh0.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-2026.01.gh0.zip	Contains the VPC-DI binary software image that is used to on-board the software directly into VMware.
qvpc-di-template-vmware_T-2026.01.gh0.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-2026.01.gh0.zip	Contains the same VPC-DI ISO identified above and additional installation files for using it on KVM.
qvpc-di-template-libvirt-kvm_T-2026.01.gh0.zip	Contains the same trusted VPC-DI ISO identified above and additional installation files for using it on KVM.
qvpc-di-2026.01.gh0.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	
intelligent_onboarding-2025.02.gh2.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-2026.01.gh0.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.

Software package	Description
qvpc-si-2026.01.gh0.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-2026.01.gh0.zip	Contains the VPC-SI binary software image that is used to on-board the software directly into VMware.
qvpc-si-template-libvirt-kvm-2026.01.gh0.zip	Contains the same VPC-SI ISO identified above and additional installation files for using it on KVM.
qvpc-si-2026.01.gh0.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.

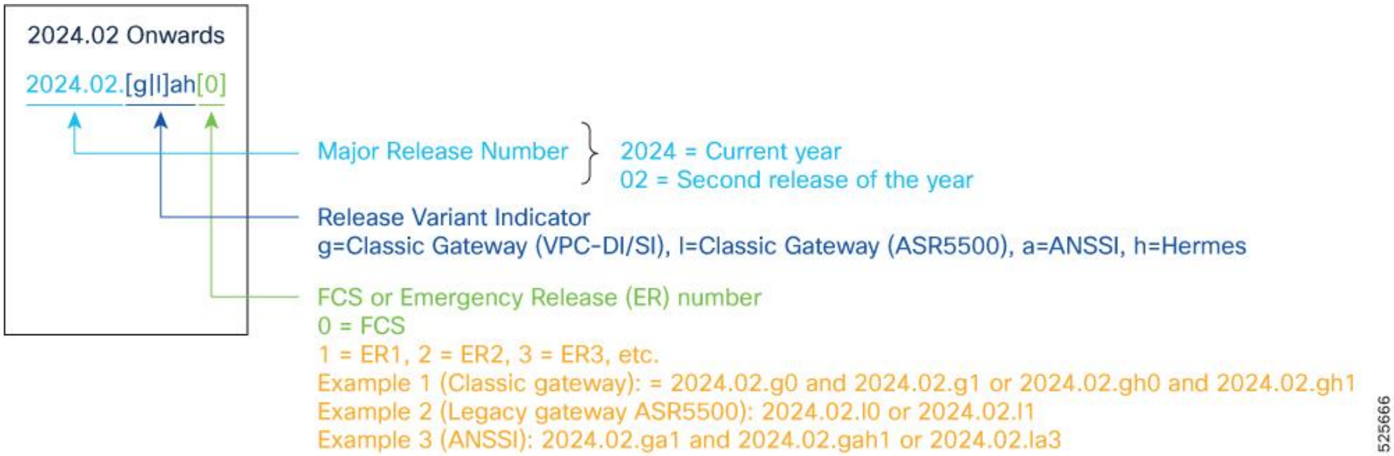
StarOS product version numbering system

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


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
525666

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 10. 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 and CUPS products.

Table 11. Related resources and additional information

Resource	Link
Cisco ASR 5500 documentation	StarOS documentation

Resource	Link
Cisco Ultra Packet Core documentation	CUPS documentation
Service request and additional information	Cisco Support

Legal information

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.