Release Notes for StarOS™ Software, Release 2025.04.l0

Contents

StarOS™ Software, Release 2025.04.l0

This Release Notes identifies changes and issues that are related to the Legacy Platform (for ASR 5500 DPC2) software releases.

Qualified products and platforms

Table 1. Products and platforms qualified in this release

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

Release lifecycle milestones

The following table provides EoL milestones for Cisco StarOS software:

Table 2. EoL milestone information for StarOS™ Software, Release 2025.04.l0

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 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

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

Table 3. Behavior changes for StarOS™ Software, Release 2025.04.l0

Description	Behavior changes
Consistent SGW Downlink FAR Buffering in CSFB Suspend/Resume [CSCwq94647]	**Previous behavior**: In the Circuit-Switched Fallback (CSFB) scenario, when a Radio Access Bearer (RAB) Release Request was received along with suspend and resume notifications, the system did not set the SGW downlink Forwarding Action Rule (FAR) to BUFFER due to a specific check. When only suspend and resume notifications were received (without the RAB Release Request), the SGW downlink FAR was moved to BUFFER, resulting in buffering of downlink data. **New Behavio**r: The check preventing the FAR action from moving to BUFFER when the RAB Release Request is present has been removed. This change ensures that the SGW consistently moves the downlink FAR to BUFFER during both scenarios—whether the RAB Release Request is received or not—providing uniform buffering behavior. **Customer Impact**: Customers will experience consistent buffering of downlink data during CSFB suspend and resume procedures regardless of the presence of a RAB Release Request. This leads to improved handling of downlink data buffering, avoiding discrepancies and potential data loss or forwarding inconsistencies during CSFB suspend and resume operations.
Improved collision handling for Bearer requests [CSCwq79531]	**Previous behavior**: When a Pure S/Collapsed call was in progress and the system received an Update Bearer Request while the user equipment (UE) was transitioning from Idle to Active, and the SGW was already processing a Modify Bearer Request for the same transition, the Update Bearer Request was rejected with a " No Resource Available" message. **New behavior**: Now, if an Update Bearer Request arrives while the SGW is already processing a Modify Bearer Request for the same transition (Idle to Active), the SGW will silently drop the Update Bearer Request. The PGW will automatically retry, and the request will be processed successfully. **Customer Impact**: With this change, Update Bearer Requests in these scenarios are now retried and processed.
Allow N26 traffic over the S10 interface [CSCwr18465]	**Previous behavior**: Interworking procedures that use the N26 interface enable the exchange of Mobility Management (MM) and Session Management (SM) states between the source and target network. The default eGTP service is supported on the N26 interface. However, N26 traffic is not allowed over the S10 interface in MME. **New behavior**: To allow N26 traffic over the S10 interface, enable the combine-n26-s10-interface command in the MME service configuration mode. **Command changes**: configure **context** context_name mme-**service** service_name **[no] combine-n26-s10-interface** **exit** **combine-n26-s10-interface**: This option lets N26 traffic over the S10 interface. If S10/S3-S11

Description	Behavior changes
	Interface Separation is not enabled, N26 and S10 use the default EGTP-C instance or service. If S10/S3-S11 Interface Separation is enabled, N26 uses a separate EGTP-C instance or service linked to S10. S10 uses its own EGTP-C instance or service. **no**: The no option disables N26 traffic over the S10 interface.

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 4. Resolved issues for StarOS™ Software, Release 2025.04.l0

Bug ID	Description	Product Found
CSCwr10359	Sessmgr crash at function egtpc_handle_user_sap_event	cups-cp
CSCwq30875	Session manager recovery status instability	cups-cp
CSCwq56872	GY SU-URR are not associated with existing URR when the Online Charging System (OCS) is in a Server Unreachable (SU) state.	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
CSCwq31050	sessmgr reload after ECS configuration modification	cups-cp
CSCwo94253	3GPP-Reporting-Reason VALIDITY_TIME in the CCR-U after GY RAR	cups-cp
CSCwr30828	UP passes the traffic despite 4012 from OCS	cups-cp
CSCwq79531	Emergency call failed due to missing location information in CCR-U	cups-cp
CSCwm50323	[CUPS CP] Call reject with Ipool-ip-validation-failed with No Chunks to allocate from this pool	cups-cp
CSCwq56869	Periodic updates not being sent when 'diameter send-ccri session-start' is configured and when FUI with terminate is received in CCA-I	cups-cp
CSCwq94647	CUPS - UE not reachable from network after CSFB	cups-cp
CSCwp20248	CP is not sending Delete session request to UP incase of GTPU Path Failure	cups-cp
CSCwr12949	Sessmgr crash at function egtpc_handle_modify_bearer_rsp_evt in CUPS-CP	cups-cp
CSCwo33578	Unexpected session disconnection	cups-cp
CSCwq96280	Assertion failure at sess/egtp/egtpc/egtpc_evt_handler_func.c:800	cups-cp
CSCwr15845	Gy session out of SU reports huge volume threshold in SxModify	cups-cp

Bug ID	Description	Product Found
CSCwr44639	lpool_ip_validation_failed after SRP switchover on CP	cups-cp
CSCwq68820	[SMU-FAPI: init_hash_req_record() error logs are triggered after UP Upgrade	cups-up
CSCwq24253	Observed Additional IE: RAT Type in SX Modification Request Message	cups-up
CSCwp26591	sessmgr crash on UP - shm_uplane_remove_rule_line_dns_snooping_list	cups-up
CSCwq31100	Packet drop detected in FUI Scenarios	cups-up
CSCwp91767	Abnormal CC-Total-Octets values after UP reload	cups-up
CSCwr40180	sessmgr restarts after SRP switchover	cups-up
CSCwq36099	ePDG VPC-SI : dhmgr mem warn	epdg
CSCwr06145	Emergency Call Incorrect Implicit Detach	mme
CSCwn59725	MME Collision Handling between E-RAB Release Indication and E-RAB Modification Indication	mme
CSCwr08706	[CP-MME] MME is sending Forward Relocation Response with incorrect local IPv6 address	mme
CSCwr06035	sessmgr failure in Function: mme_emm_registered_idle_handle_im_exit_trigger()	mme
CSCwr34679	UE detaches after 60 secs post MME handover to other MME	mme
CSCwr18465	N26/S10 interface separation - allow N26 traffic over S10 interface	mme
CSCwq12952	During X2 handover MME modifies NR UE Security Capabilities received in Path Switch Request prior returning it to eNB	mme
CSCwq68664	Sessmgr restarts after SGW relocation with dedicated Bearers Deletion for MB Response delay with " context not found" scenarios.	pdn-gw
CSCwq55405	Updates to a Group of Ruledefs triggers an mtree data structure rebuild, the configuration under the GOR retains old hash causing packet mismatches	pdn-gw
CSCwq83591	sessmgr crash when using certain RG acsmgr_dcca_get_cca_n_premptive_request_rating_groups()	pdn-gw
CSCwq97734	Add support for generating the pcap file from the hexdump for a monsub session of a PGW service	pdn-gw
CSCwq36837	Sessmgr task restart at function sessmgr_get_ipv6_end_user_address()	pdn-gw
CSCwq22148	Legacy-GW ATT : ASR5500 chassis hwctrl process shows warn state in show task resources	pdn-gw
CSCwq56968	Discrepancy observed while modification of 'cdr transfer-mode push' CLI	pdn-gw
CSCwq00151	Sessmgr restarts after enabling VoLTE for specific inroamer IMSIs ranges	pdn-gw
CSCwr18037	SGW calls are not getting created due to sessmgr assertion	pdn-gw

Bug ID	Description	Product Found
CSCwp60108	session manager crash with an unknown signature time encoding data at smgr_gr_encode_uplane_call_info_uchckpt_cmd	sae-gw
CSCwq56385	Assertion failure at midplane/libsn_midplane.c in SPGW	sae-gw
CSCwr57827	sessmgr reload at Function: is_dhcp_server_down()	staros
CSCwo01479	Unplanned SF migration caused diamproxy instance # out of range	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 5. Open issues for StarOS™ Software, Release 2025.04.l0

Bug ID	Description	Product Found
CSCwq38956	[BP-CUPS] Interfaces are down Post upgrade : 21.28.h14.98513	cups-up
CSCwr83413	Unexpected DeleteSessionRequest after UEContextReleaseRequest	mme

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 a version upgrade from any version less than 21.28.m23 to 21.28.m23, or versions higher than 21.28.m23.

Upgrade the confd version

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

Note: During the 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.

Compatibility

This section provides compatibility information about the StarOS package version, and the software requirements for the Legacy Platform (for ASR 5500 DPC2) software.

Compatible StarOS package version

Table 6. Release package version information

StarOS packages	Version	Build number
StarOS package	2025.04.l0	21.28.m38.99199

Compatible software components for ASR 5500

This section lists compatibility information of the StarOS™ Software products that are verified to work with this version of the ASR 5500.

Table 7. Compatibility information for ASR 5500 DPC2, Release 2025.04.l0

Supported software	Version
ADC P2P plugin	2.74.12.2726

Supported software packages

This section provides information about the release packages associated with Legacy Platform (for ASR 5500 DPC2) software.

Table 8. Software packages for Release 2025.04.l0

Software package	Description
ASR 5500 companion package	
companion-asr5500-2025.04.l0.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.

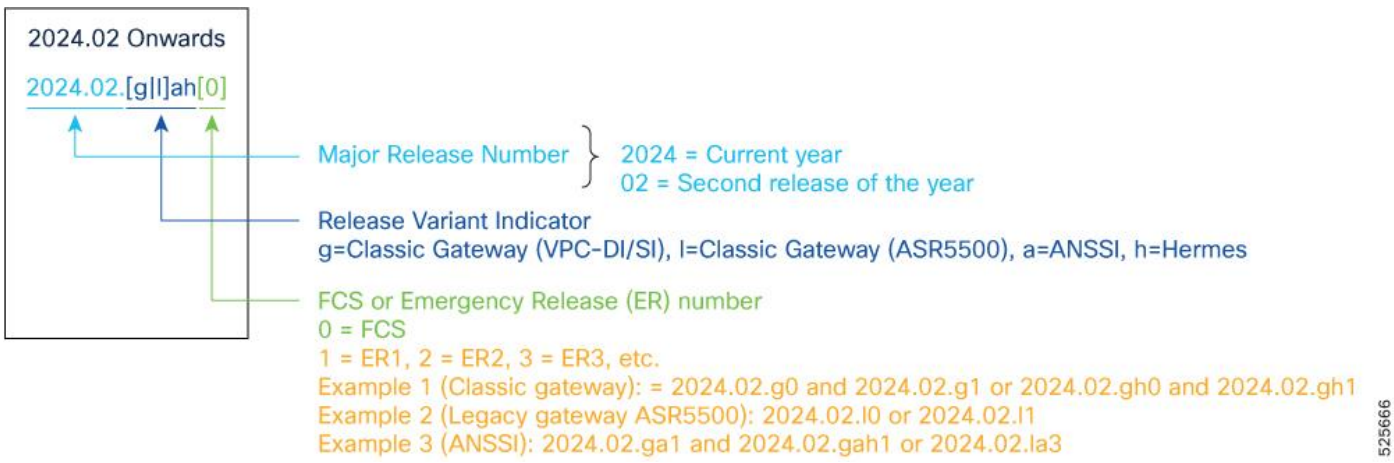
StarOS product version numbering system

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 9. 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 10. Related resources and additional information

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

Legal information