Release Notes for StarOS™ Software, Release 2026.03.l0

Contents

StarOS™ Software, Release 2026.03.l0

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

The key highlights of this release include:

- **Lawful Intercept (LI) Decryption**: Provided a new parameter (J option) for LI Admin users to decrypt and view LI AVP values in PGW messages, along with enhanced session monitoring.
- **Secure CDR Storage**: Enabled AES-256-CBC-SHA256 encryption for locally stored Charging Data Records (CDRs) to ensure data security during Charging Gateway Function outages.
- **Support higher bit encryption in SNMPv3**: Enhanced SNMPv3 security with support for advanced SHA-2 authentication and AES-192 privacy, in addition to the existing algorithms to ensure security compliance.

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	No
MME	Yes
ePDG	Yes
P-GW	Yes
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

Milestone	Date
First Customer Ship (FCS)	23-July-2026
End of Life (EoL)	23-July-2026
End of Software Maintenance (EoSM)	21-Jan-2028
End of Vulnerability and Security Support (EoVSS)	21-Jan-2028
Last Date of Support (LDoS)	31-Jan-2029

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

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

Table 3. New software features for StarOS™ Software, Release 2026.03.l0

Product impact	Feature	Description
Software Reliability	LI AVP Decryption	This feature provides LI Admin users to decrypt and view the Lawful Intercept AVP values in PGW messages using a new parameter, **J** option in monitor protocol and monitor subscriber catalog. This feature also enhances the show command **show ims-authorization sessions full callid** *<id>* to include a dedicated LI-Indicator-Gx section. For more information, contact the Cisco account representative.
Software Reliability	CDR encryption and decryption at rest for GTPP storage-server	This feature enables protection of locally stored Charging Data Records with AES-256-CBC-SHA256 encryption, while the Charging Gateway Function is unavailable. It encrypts and decrypts the CDRs and transmits once the connectivity is restored. It helps ensure that the sensitive billing data is secure during outages. Commands enhanced: **[no] gtpp storage-server cdr-encryption-at-rest aes-256-cbc-sha256 key** <passphrase> For more information contact the Cisco account representative.
Software Reliability	SNMPv3 security enhancements	SNMPv3 security is enhanced through support for advanced authentication (SHA-256, SHA-384, and SHA-512) and AES-192 privacy. These updates are in addition to the existing algorithms (MD5, SHA-1, and DES) to provide enhanced security and ensure compliance with RFC 7860 standards. For more information contact the Cisco account representative.

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 2026.03.l0

Description	Behavior changes
APN name accepts wildcard characters when Enabling monitor subscribers [CSCwt53545]	**Previous behavior**: When enabling monitor subscriber, the APN name did not accept wildcard characters such as * and $. **New behavior**: When enabling monitor subscriber, the APN name now accepts wildcard characters: $ represents a single character, and * represents multiple characters. This enhancement provides users with more flexible and efficient monitoring options.
Sessmgr traffic rejection for Unresolved predefined tule or Application IDs [CSCwt78261]	**Previous behavior**: The UPF accepted the activation of predefined rules containing undefined ruledefs. This resulted in rule match failures and triggered an ADC rule crash. **New behavior**: During the Create-PDR procedure, sessmgr now rejects requests if the referenced predefined rule is unresolved due to a missing valid ruledef or group binding.

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 2026.03.l0

Bug ID	Description	Product Found
CSCwu32273	Session manager reloads at egtpc_resume_suspended_proc()	mme
CSCws52471	MME fails to select the peer, While default egtp service is configured with ipv4 and S10/N26 EGTP Separation service with ipv6	mme
CSCwu34081	Memory leak in acs_free_l3_session() cleanup path	pdn-gw
CSCwv03259	CLI proclet restart observed during StarOS configuration loading following the upgrade of starOS 21.28.mh36	pdn-gw
CSCwt76990	WhatsApp calls blocking accuracy problem	pdn-gw
CSCwu66014	Missing NOA/NPI Octet in PGW-CDRs when MSISDN length is greater than 10 digits	pdn-gw
CSCwv33834	PDNGW unexpectedly includes User-CSG-Information in Rf ACR when CSReq and Gx CCA contain no CSG information	pdn-gw

Bug ID	Description	Product Found
CSCwt19501	PGW sends the IMSI in the CCR-I message to the PCRF for unauthenticated emergency calls	pdn-gw
CSCwu24438	Session manager assertion failure at diabase module	sae-gw

Open issues

This table lists the open 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 6. Open issues for StarOS™ Software, Release 2026.03.l0

Bug ID	Description	Product Found
CSCwu95813	IPSECMGR restart observed in function ikev2_encode_header_ipv4	epdg
CSCwv51804	E-RAB Modification Collision During VoWiFi-to-VoLTE Handover Results in Bearer Setup Failure	mme
CSCwv39305	Active Charging uplink CSS accounting missing for specific L2TP IPv4 sessions	pdn-gw
CSCwv63071	ASR5500 sessmgr crash with SIGSEGV in ipms_msg_getstats() during IPMS config/unconfig handling	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 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 StarOS 2026.02 release, confD is upgraded to 8.6 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.
- ConfD must be unconfigured (stopped) before running the **clear confdmgr confd all** CLI command.

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 *

   -or-

   Run the StarOS CLI command **clear confdmgr confd all** to clear the same confD contents.

   Note: The /mnt/hd-raid/meta/confd directory will be empty. After clearing, confD can be started again as required. This clear cli should be used only during ConfD upgrade scenarios and not on each reload or reboot.

   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 account representative.

HD-RAID may fail to initialize during upgrades or downgrades between non-Hermes builds

Issue: When upgrading or downgrading between non-Hermes builds (202x.0x.lx) on ASR5k platforms, the HD-RAID may fail to initialize as expected.

Workaround: This Method of Procedure (MOP) should be used during upgrades or downgrades between non-Hermes builds.

To avoid HD-RAID failure, perform these steps during upgrade or downgrade (for example, from 2026.02.lx to 2026.03.lx:

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

   Note: All data in /hd-raid will be lost during recovery.
2. Before the upgrade: On the current (source) build, run the `**hd raid clear**` command.
3. Upgrade and reboot: Reboot the node to upgrade to the newer (target) build.
4. Wait for the hd-raid to recover and restore the files from backup.

   Note: It is recommended to use this Method of Procedure (MOP) for upgrading and downgrading between .mx builds.

Compatibility

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

Compatible StarOS package version

Table 7. Release package version information

StarOS packages	Version	Build number
StarOS package	2026.03.l0	21.28.m45.101106

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 2026.03.l0

Product	Version
ADC P2P Plugin	2.74.17.2815

Supported software packages

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

Table 9. Software packages for Release 2026.03.l0

Software package	Description
ASR 5500 companion package	
companion-asr5500-2026.03.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.

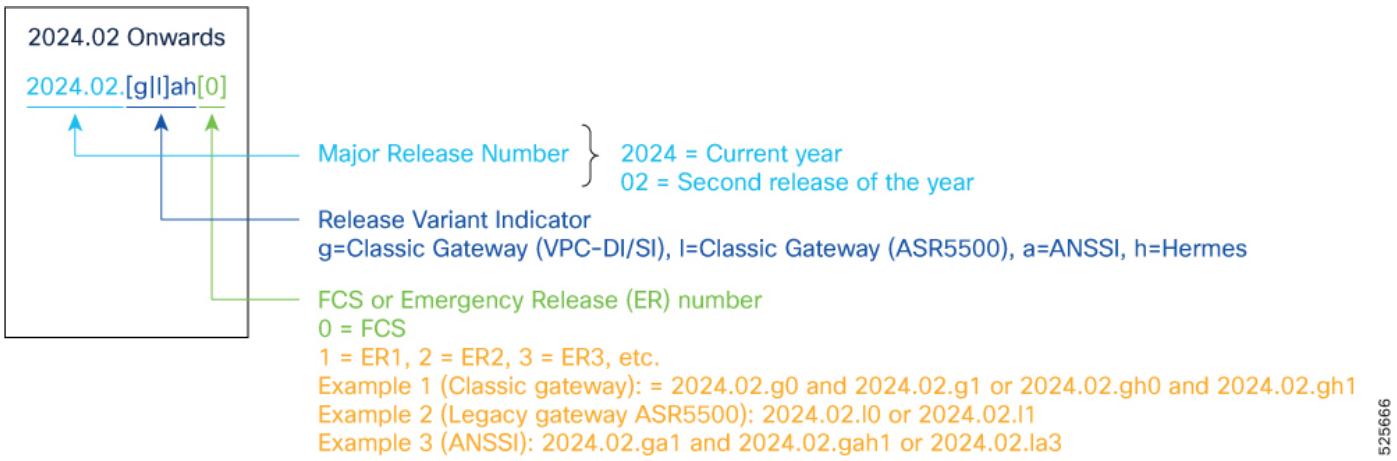
StarOS product version numbering system

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

Legal information