



# Release Notes for StarOS™ Software, Release 2026.01.10

# Contents

StarOS™ Software, Release 2026.01.I0 .....	3
New software features .....	4
Changes in behavior .....	4
Resolved issues .....	4
Open issues .....	5
Known issues .....	5
Compatibility .....	6
Supported software packages .....	7
Related resources .....	8
Legal information .....	9

## StarOS™ Software, Release 2026.01.lo

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

The key highlights of this release include:

- **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.

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?
<b>Products</b>	
CUPS	No
MME	Yes
ePDG	Yes
P-GW	Yes
SAEGW	Yes
SGSN	Yes
<b>Platforms</b>	
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 2026.01.lo

Milestone	Date
First Customer Ship (FCS)	30-Jan-2026
End of Life (EoL)	30-Jan-2026

Milestone	Date
End of Software Maintenance (EoSM)	31-July-2027
End of Vulnerability and Security Support (EoVSS)	31-July-2027
Last Date of Support (LDoS)	30-July-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

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

**Table 3.** New software features for StarOS™ Software, Release 2026.01.10

Product impact	Feature	Description
Software Reliability	<a href="#">Add TLVs containing APN and Virtual APN to Pilot Packets</a>	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.

## 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 4.** Resolved issues for StarOS™ Software, Release 2026.01.10

Bug ID	Description	Product Found
<a href="#">CSCws26321</a>	The ERAB Failed List IE is missing in the Path Switch Acknowledge message when the Path Switch Request contains invalid tunnel details.	mme
<a href="#">CSCws48490</a>	DNS Records used for selecting AMF peer not released	mme
<a href="#">CSCwr48395</a>	sessmgr restart at sn_aaa_client_action_item_lookup_by_key()	pdn-gw
<a href="#">CSCws18654</a>	Legacy-GW: VzW ASR5500: sessmgr restart observed during configuration of new apn, new rulebase, new fw-nat-policy, and SRP switchover	pdn-gw

Bug ID	Description	Product Found
<a href="#">CSCwr56361</a>	Assertion failure: EGTP-C service is being used by another MME/SGW/PGW service	pdn-gw
<a href="#">CSCws62168</a>	P-CSCF Address Missing in CSRsp When DNS Returns Only CNAME Without Resource Records	pdn-gw
<a href="#">CSCws13802</a>	Traffic is being re-directed in error by the PGW due to GOR ruledef update	pdn-gw
<a href="#">CSCwr44475</a>	UDP quic traffic detection problem	pdn-gw
<a href="#">CSCwr95955</a>	PGW (VPC) incorrectly charges for Router Solicitation (RS) packets in IPv6 sessions.	pdn-gw
<a href="#">CSCwa60822</a>	PGW is sending '0x40' for IP Address instead of '0x04'	pdn-gw

## 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 2026.01.10

Bug ID	Description	Product Found
<a href="#">CSCws47044</a>	PGW Session Setup Failure: Static IPv4 Address Mismatch for APN " nemo-cust101"	pdn-gw
<a href="#">CSCws47075</a>	Unable to convert date-time string in the Diameter credit-control-request message processing	pdn-gw
<a href="#">CSCws50662</a>	Assertion failure at diameter/diabase/diabase'	pdn-gw
<a href="#">CSCws66809</a>	GW is sending CCR-U with charging rule report with cause " Rule-Failure-Code: UNSUCCESSFUL_QOS_VALIDATION"	pdn-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 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	2026.01.10	21.28.m41.99724

#### 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 2026.01.I0

Supported software	Version
ADC P2P plugin	2.74.14.2762

## 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 2026.01.I0

Software package	Description
ASR 5500 companion package	companion-asr5500-2026.01.I0.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.

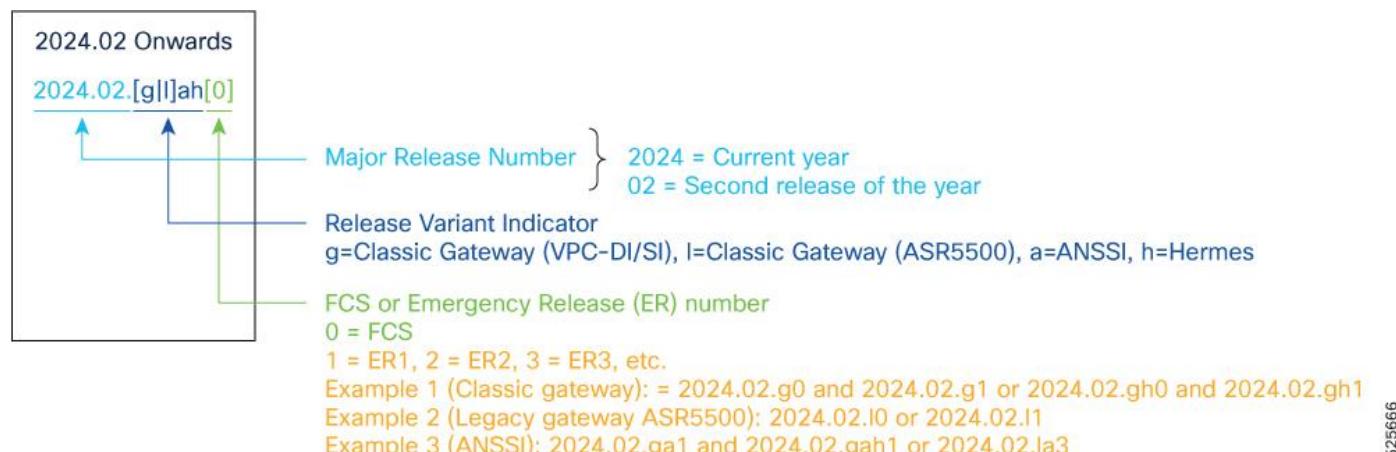
## StarOS product version numbering system

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	<a href="#">StarOS documentation</a>
Cisco Ultra Packet Core documentation	<a href="#">CUPS documentation</a>
Service request and additional information	<a href="#">Cisco Support</a>

## Legal information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.

© 2026 Cisco Systems, Inc. All rights reserved.