# Release Notes for StarOS™ Software, Release 2026.02.gh0

# Contents

## StarOS™ Software, Release 2026.02.gho

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

The key highlights of this release include:

- Adjusted S1 handover guard timers to prevent timeout issues and optimize network resources.
- Supported validation of IRGW on CNDP in Supermicro servers with IPv4 and IPv6 interfaces.
- Improved reliability and flexibility in charging data handling for P-GW.
- Ensured dual-stack connection success by anchoring IPv6 sessions to the same User Plane as the HOLD IPv4 session.
- Implemented additional Real Time Tool (RTT) fields for ePDG S2b interface procedures.
- Configured RTT monitoring support for specific procedures to optimize CPU, memory, and storage usage.
- Added support for filtering monitor subscriber commands by specific sessmgr instances for pgw, sgw, saegw, and ggsn.
- Enabled Gz tariff time replication from Gy buckets to prevent signaling storms in CUPS deployments.

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

| Milestone | Date |
|---|---|
| First Customer Ship (FCS) | 23-Apr-2026 |
| End of Life (EoL) | 23-Apr-2026 |
| End of Software Maintenance (EoSM) | 22-Oct-2027 |
| End of Vulnerability and Security Support (EoVSS) | 22-Oct-2027 |
| Last Date of Support (LDoS) | 31-Oct-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

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

**Table 3.** New software features for StarOS™ Software, Release 2026.02.gh0

| Product impact | Feature | Description |
|---|---|---|
| Software Reliability | Configurable MME S1 HO guard timer duration | This feature allows the network operator to modify the default hardcoded S1 HO guard timer value of 50 seconds into configurable range between 10 to 50 seconds specifically for the inbound S1 handover procedure over the S10 interface.<br>This prevents external MME timeout issues and optimizes network resource usage during mobility events.<br>Command introduced: under MME service configuration mode.<br>• **default policy handover s10 guard-timer**<br>• **policy handover s10 guard-timer <***guard-timer seconds***>** - Enter the Guard timer intervals between 10-50 seconds. |
| Software Reliability | IRGW validation on CNDP | This feature tests and validates the IRGW on CNDP in Supermicro servers with IPv4 and IPv6 interface. |
| Software Reliability | Delay charging over TLS/QUIC | This feature enables secure delayed charging over TLS/QUIC with improved reliability and flexibility in charging data handling. |
| Software Reliability | IPv6 Session Affinity | Anchors IPv6 session to the same User Plane (UP) as the HOLD IPv4 session during reassociation, overriding standard UP selection algorithms to ensure dual-stack connections are successful. |

| Product impact | Feature | Description |
|---|---|---|
| Software Reliability | RTT field enhancement | Implementation of additional Real Time Tool (RTT) fields for S2b interface procedures for ePDG. |
| Software Reliability | Enabling selective RTT measurement for ePDG | This feature allows you to configure/unconfigure RTT measurement for specific procedures.<br>Commands updated:<br>**[no] reporting-action event-record procedure** command under the **epdg-service** configuration mode.<br>By limiting RTT monitoring to only necessary procedures, you optimize CPU, memory, and storage usage. |
| Software Reliability | Tariff time replication on CUPS | The feature enables replication of Gz tariff time from the Gy bucket. It ensures suppression of Sx Query-URR to prevent signalling storms in CUPS deployments.<br>**Command introduced**:<br>**egcdr tariff replicate-ocs-tariff-time-change**- This CLI command is configured in Active Charging Service command mode.<br>**Default settings**: Disabled-Configuration required to enable |

## 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 2026.02.gh0

| Description | Behavior changes |
|---|---|
| PGW IMSI Suppression during unauthenticated emergency attach messages<br>[CSCwt19501] | **Previous Behavior:**<br>During unauthenticated emergency attach, the PGW forwards both E164 and IMSI to the PCRF with the r8-standard dictionary enabled under the ims-auth service. The Subscription-Id AVPs include:<br>• Subscription-Id-Type: END_USER_E164 (0)<br>• Subscription-Id-Data: 9890098900<br>• Subscription-Id-Type: END_USER_IMSI (1)<br>• Subscription-Id-Data: 404005123456788<br>**New Behavior:**<br>PGW behavior aligns with 3GPP specification 23.401. During unauthenticated IMSI reported by the MME through the “CREATE SESSION REQUEST” message, which is marked with uimsi flag in Indicator IE. IMSI is suppressed towards the PCRF during unauthenticated emergency attach. The Subscription-Id AVP includes only:<br>• Subscription-Id-Type: END_USER_E164 (0)<br>• Subscription-Id-Data: 9890098900<br>Command introduced under the PGW service configuration mode:<br>subscription-id service-type { closed_rp \| ggsn \| ha \| ipsg \| l2tplns \| mipv6ha \| pdsn \| pgw \| samog-epdg } { e164 \| imsi \| nai \| **lsm-emergency-imei-instead-of-uimsi** }<br>**Note**: This keyword is configured under the 'ims-auth service' for emergency APNs. It applies only to emergency APNs over TLS/QUIC, providing improved reliability and flexibility for charging data handling. |

| Description | Behavior changes |
|---|---|
| NOA/NPI is added to the servedMSISDN field in the PGWCDRs<br><br>[CSCwt19446] | **Previous behavior:**<br><br>servedMSISDN of the PGWCDR does not contain NOA/NPI<br><br>**New behavior**:<br><br>PGWCDRs supports the Nature of Address (NOA) and Numbering Plan Indicator (NOI) parameters aligning with 3GPP TS 29.002. These parameters are used in routing calls and messages to determine how a phone number should be interpreted.<br><br>**Command introduced**:<br><br>**include-msisdn-noa-npi**- Indicates NOA/NPI(0x91) in the PGWCDR MSISDN.<br><br>**Customer impact:** When this **include-msisdn-noa-npi** CLI is enabled you can have the new behavior visibility. |
| Colocated gateway selection during EPSFallback for roaming PLMN<br><br>[CSCwq14755 ] | **Previous behavior:**<br><br>During a Tracking Area Update (TAU) for EPS fallback, roaming subscribers did not utilize the configured co-location or topology criteria for SGW selection.<br><br>**New behavior:**<br><br>The gw-selection command within the Call Control Profile configuration mode has been enhanced with the **apply-for-roame**r option. When this configuration is enabled, roaming subscribers will now undergo SGW selection based on the configured co-location or topology criteria during EPS fallback TAU scenarios.<br><br>**Customer Impact**: The customer will have better control over resource management for roaming subscribers. |
| ConfD schema compatibility handling [CSCwo47013] | **Previous behavior**:<br><br>During ConfD upgrades, version incompatibilities with persisted schema files could lead to initialization failures and repeated confdmgr crashes; as there was no CLI utility available to clear this data, it was necessary to manually remove the contents of the /mnt/hd-raid/meta/confd directory during the upgrade process to ensure system stability.<br><br>**New behavior:**<br><br>A new CLI command, **clear confdmgr confd all**, has been introduced to clear all persistent ConfD data, which facilitates a clean reinitialization and prevents initialization failures during upgrades.<br><br>For more information on the method of procedure, refer to the Upgrade the confd version |

## 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 2026.02.gh0

| Bug ID | Description | Product Found |
|---|---|---|
| CSCwt53217 | Unauthorized Session Establishment Triggered by Gy CCR-U and RAR Timing Collision | cups-cp |

| Bug ID | Description | Product Found |
|---|---|---|
| CSCwt65229 | Destination Realm AVP missing in CCR-I message after fallback to Local Policy | cups-cp |
| CSCwf27561 | High number of CC category misses | cups-cp |
| CSCws39624 | Sessmgr restart due to Segmentation fault: acsmgr_allocate_cups_sef_info() | cups-cp |
| CSCwt93437 | Combination of PFD Push Enabled and Disabled with two UP groups is not supported | cups-cp |
| CSCwq07274 | Difference in the volume reported in Sx-Volume Measurement and monsub- CALL STATS | cups-up |
| CSCwq38956 | Interfaces are down Post upgrade : 21.28.h14.98513 | cups-up |
| CSCwt36200 | Sessmgr restarts due to assertion failure in snx_epdgstubdrv_fsm() | epdg |
| CSCws50507 | Memory leak observed in func mme_db_cache_alloc_non_current_security_context w/ n26 | mme |
| CSCwt66319 | Observed sessmgr assert during Outbound Handover to peer MME | mme |
| CSCwt47887 | In a failover scenario, MME does not retry properly to all the recieved RR's from DNS based on priority | mme |
| CSCwt64846 | TAU is rejected post inbound HO when MICR check and decor is enabled | mme |
| CSCwr32050 | Emergency call-garbage value seen in bulkstat and show mme-ser statistics lte-emergency-profile profile-name lte1 | mme |
| CSCwq14755 | Colocated gateway selection during EPSFallback for roaming PLMN | mme |
| CSCwt34638 | MME rounding down APN-AMBR value received from ULA before comparing with ctx-resp | mme |
| CSCwt68720 | Observing sessmgr crash for function :: mme_egptc_set_pdn_state in version | mme |
| CSCwt95240 | MFP4.0 April 2026 the build need to support cilium instead of calico. Hitting issues with calico during RCM deployment. Also, rcm ned needs correction to proper 4G CUPS based RCM NED currently its 5G SMI based. | nso-mob-fp |
| CSCwm96403 | Mobility MFP 3.4.3 / CommandSanitizer incorrectly removing configuration from string | nso-mob-fp |
| CSCws66809 | GW is sending CCR-U with charging rule report with cause " Rule-Failure-Code: UNSUCCESSFUL_QOS_VALIDATION" | pdn-gw |
| CSCws47075 | Unable to convert date-time string in the Diameter credit-control-request message processing. | pdn-gw |
| CSCwt54017 | Unexpected S6b Event File Generation on PGW Gateways | pdn-gw |
| CSCws50662 | Assertion failure at diameter/diabase/diabase' | pdn-gw |
| CSCwt19446 | Incorrect MSISDN Encoding: Missing NOA/NPI Octet in PGW-CDRs 3GPP TS 32.298 Compliance | pdn-gw |
| CSCwt19501 | PGW sends the IMSI in the CCR-I message to the PCRF for unauthenticated emergency calls | pdn-gw |

| Bug ID | Description | Product Found |
|---|---|---|
| CSCwr95955 | PGW (VPC) incorrectly charges for Router Solicitation (RS) packets in IPv6 sessions. | pdn-gw |
| CSCwt51790 | Active-charging MBR change after Gx CCR-U | pdn-gw |
| CSCwt03412 | High speed traffic is not reported in CDR and Gy | pdn-gw |
| CSCws47044 | PGW Session Setup Failure: Static IPv4 Address Mismatch for APN " nemo-cust101" | pdn-gw |
| CSCwt37898 | Some of the http flows are not getting accelerated | pdn-gw |
| CSCws62168 | P-CSCF Address Missing in CSRsp When DNS Returns Only CNAME Without Resource Records | pdn-gw |
| CSCws05111 | sessmgr checkpoint issue observed in osp17 vpcdi after card migration | staros |
| CSCwt97154 | VMware DI platform binary upgrade fails non-hermes to hermes | staros |

## Open issues

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

**Note**: This software release may contain open bugs 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 2026.02.gh0

| Bug ID | Description | Product Found |
|---|---|---|
| CSCwt06603 | Context removal & addition leads to incorrect flow creation leading to TCP flows recognized incorrect | cups-cp |
| CSCwt86456 | Zero volume Usage seen in UNIT_BEFORE_TARIFF_CHANGE in Gy CCR Update while validity Time | cups-cp |
| CSCwt94942 | While Rulebase change CP creates the Static rule URRs causing Gy Replicate functionality | cups-cp |
| CSCwt30038 | sessctrl_handle_mgr_notify_server_list_ipaddr_status_update() | cups-up |
| CSCwt55278 | Multiple TCP connection over X3 interface | cups-up |
| CSCwt99888 | Silent sessctrl restart during booting up of n:m UP after reload/switchover. Crash list not updated | cups-up |
| CSCwu05660 | Valgrind Observations seen for April26 FCS release | cups-up |
| CSCwt76897 | With Firewall enabled in scenario of fragmentation failure all fragmented packets are not reaching to sessmgr | cups-up |
| CSCwt80226 | Vpp is not reassembling the fragmented packets when traffic is sent by pacer | cups-up |

| Bug ID | Description | Product Found |
|---|---|---|
| CSCwt98942 | Multiple sessmgr restart with Assertion failure at diameter/diabase/diabase with acsmgr_mscc_tx_timeout() | pdn-gw |
| CSCwt76990 | WhatsApp calls blocking accuracy problem | 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.

**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 the 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.

**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 2025.04.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 .mx and .mhx StarOS builds.

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

## Compatibility

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

### Compatible StarOS package version

**Table 7.** Release package version information

| StarOS packages | Version | Build number |
|---|---|---|
| StarOS package | 2026.02.gh0 | 21.28.mh38.100465 |

### 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 2026.02.gh0

| Product | Version |
|---|---|
| ADC P2P Plugin | 2.74.gh2.2788 |
| RCM | 20260417-160533Z<br>**Note**: Use this link to download the RCM package associated with the software. |
| ESC | 6.0.0.55 |
| CVIM | 5.0.4 |
| Host OS | RHEL 9.2 |
| RedHat OpenStack | RHOSP 17.1 |
| Intel XL710C NIC Version | Driver version: i40e-2.17.4<br>Firmware: 7.00 0x80005119 0.385.115 |
| CIMC | 4.2 (3) |
| NSO MFP | 4.0<br>**Note:** MFP 4.0 includes two OpenStack NED versions: 4.2.33 and 4.2.34. For deployments using Red Hat OpenStack Platform 13, it is recommended to use NED version 4.2.33 due to an API version incompatibility between NED 4.2.34 and OSP 13. |

**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 2026.02.gh0

| Software package | Description |
|---|---|
| **NSO** | |
| nso-mob-fp-4.0-2026.02.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-2026.02.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-2026.02.gh0.bin.zip | Contains the VPC-DI binary software image that is used to replace a |

| Software package | Description |
| --- | --- |
| | previously deployed image on the flash disk in existing installations. |
| qvpc-di_T-2026.02.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-2026.02.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-2026.02.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-2026.02.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-2026.02.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-2026.02.gh0.zip | Contains the same VPC-DI ISO identified above and additional installation files for using it on KVM. |
| qvpc-di-template-vmware-2026.02.gh0.zip | Contains the VPC-DI binary software image that is used to on-board the software directly into VMware. |
| qvpc-di-template-libvirt-kvm_T-2026.02.gh0.zip | Contains the same trusted VPC-DI ISO identified above and additional installation files for using it on KVM. |
| qvpc-di-2026.02.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. |
| qvpc-di_T-2026.02.gh0.qcow2.zip | Contains the trusted 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** | |
| intellig3nt_onboarding-2026.02.gh0.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-2026.02.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. |
| qvpc-si_T-2026.02.gh0.bin.zip | Contains the trusted VPC-SI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. |
| qvpc-si-2026.02.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_T-2026.02.gh0.iso.zip | Contains the trusted VPC-SI ISO used for new deployments a new virtual machine is manually created and configured to boot from a CD image. |
| qvpc-si-template-vmware-2026.02.gh0.zip | Contains the VPC-SI binary software image that is used to on-board |

| Software package | Description |
|---|---|
| | the software directly into VMware. |
| qvpc-si-template-vmware_T-2026.02.gh0.zip | Contains the trusted VPC-SI binary software image that is used to on-board the software directly into VMware. |
| qvpc-si-template-libvirt-kvm-2026.02.gh0.zip | Contains the same VPC-SI ISO identified above and additional installation files for using it on KVM. |
| qvpc-si-template-libvirt-kvm_T-2026.02.gh0.zip | Contains the same trusted VPC-SI ISO identified above and additional installation files for using it on KVM. |
| qvpc-si-2026.02.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. |
| qvpc-s3_T-2026.02.gh0.qcow2.zip | Contains the trusted VPC-SI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack. |

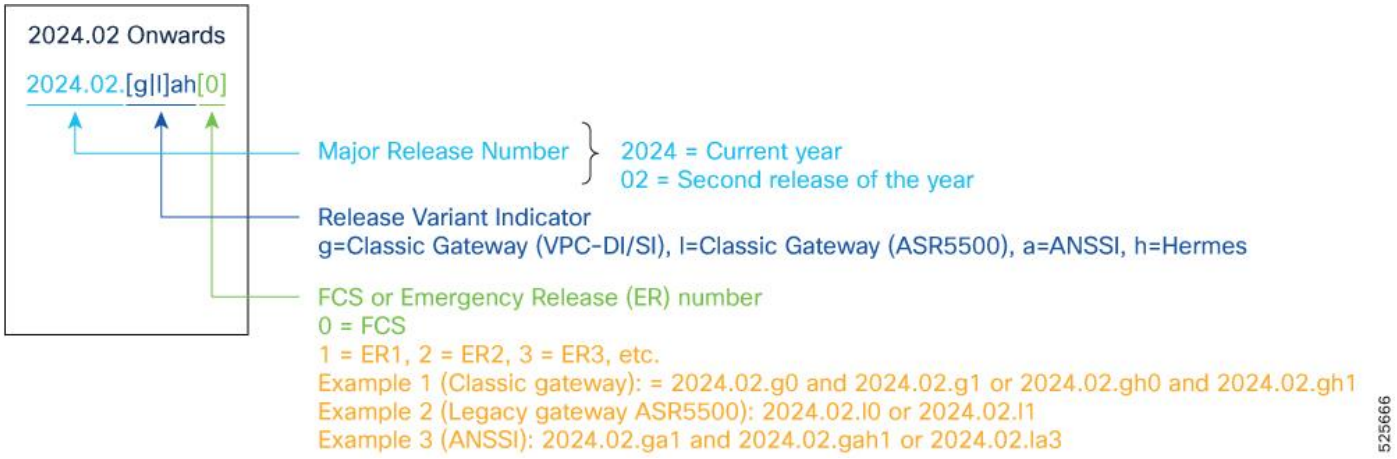
## StarOS product version numbering system

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 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:<br>`> certutil.exe -hashfile <filename>.<extension> SHA512` |
| Apple MAC | Open a terminal window and type the following command:<br>`$ shasum -a 512 filename.extension` |
| Linux | Open a terminal window and type the following command:<br>`$ sha512sum filename.extension`<br>OR<br>`$ shasum -a 512 filename.extension` |
| Note: filename is the name of the file.<br>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