Release Notes for StarOS™ Software, Release 2026.04.gh1

© 2026 Cisco and/or its affiliates. All rights reserved.

Contents

StarOS™ Software, Release 2026.04.gh1 3
New software features 4
Changes in behavior 4
Resolved issues 5
Open issues 7
Known issues 7
Compatibility 9
Supported software packages 10
Related resources 13
Legal information 13

© 2026 Cisco and/or its affiliates. All rights reserved.

StarOS™ Software, Release 2026.04.gh1

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:

- AES-256 encryption for SNMPv3.
- Qualification of ePDG for CNDP/KVM deployments on Cisco UCS M5.
- Increase in the Lawful Intercept throughput limit on the vPC-DI platform from 400 Mbps to 600 Mbps.

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)	5-Nov-2026
End of Life (EoL)	5-Nov-2026

© 2026 Cisco and/or its affiliates. All rights reserved.

Milestone	Date
End of Software Maintenance (EoSM)	5-May-2028
End of Vulnerability and Security Support (EoVSS)	5-May-2028
Last Date of Support (LDoS)	31-May-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 2026.04.gh1

Product impact	Feature	Description
Software reliability	AES-256 encryption in SNMPv3	This feature supports AES-256 as an additional SNMPv3 privacy protocol in the existing snmp target and snmp user configuration paths. This enhancement provides higher-bit privacy encryption for SNMPv3 traffic while preserving backward compatibility with existing des and aes-192 privacy options. For more information, contact the Cisco account representative.
Software reliability	ePDG qualification added on CNDP/KVM platform	ePDG is qualified for CNDP and KVM deployments on Cisco UCS M5 server.
Software reliability	Enhanced vPC-DI platform to increase Lawful Intercept throughput limit from 400 Mbps to 600 Mbps	Enhanced the vPC-DI platform to increase the cumulative Lawful Intercept (LI) throughput limit from 400 Mbps to 600 Mbps by optimizing the LI packet forwarding path. This reduces per-packet syscall overhead in the connproxy proclet, alleviating CPU bottlenecks, and enabling higher-bandwidth enterprise 4G services. 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 2026.04.gh1

Description	Behavior changes
E-RAB modification collision during VoWiFi-to-VoLTE	**Previous behavior**: During a collision caused by an E-RAB Modification Indication (DCNR/NSA) where a NotToBeModified (NTM) bearer is not fully active—for example, if the default bearer is waiting for " Activate-Default-EPS-Bearer-Accept" from UE during a

© 2026 Cisco and/or its affiliates. All rights reserved.

Description	Behavior changes
handover results in Bearer setup failure [CSCwv51804]	VoWiFi to VoLTE handover—the MME rejects the ERMI and releases the S1 connection. As a result, the UE enters an idle state, which leads to a failed bearer setup. **New behavior**: A new CLI-controlled configuration knob allows flexible handling of these collisions. The default behavior remains unchanged to maintain backward compatibility. Users can opt in for the new functionality. Command introduced under the mme-service configuration mode: **policy erab-mod-ind collision ntm-activation-pending** {**allow** | **reject** | **reject-and-s1-release**} • **allow**: Allows the E-RAB Modification indication procedure and maintains the UE in a connected state. • **reject**: Rejects the E-RAB Modification procedure but maintains the UE in a connected state. • **reject-and-s1-release**: Rejects the E-RAB Modification Indication procedure and initiates an S1 release to move the UE to an idle state. This is the default behavior. **Note**: This change does not alter the behavior for To Be Modified (TM) non-active bearers in ERMI and activation pending collisions.

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 2026.04.gh1

Bug ID	Description	Product Found
CSCwt65229	Destination Realm AVP missing in CCR-I message after fallback to Local Policy	cups-cp
CSCwu70867	sxdemux restart at sn_memblock_cache_block_flush	cups-cp
CSCwv38311	sessmgr and sxdemux crashes on an ASR5500 system running 21.28.m36	cups-cp
CSCwv92539	Pre-emptive Quota RG0 not requested in Gy CCR-I	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
CSCww15471	CUPS-CP Continuous sessmgr process restarts after adding active-charging configuration	cups-cp
CSCww42917	sessmgr memory keep increase on standby chassis with L2TP call	cups-cp
CSCww03173	sessmgr crash on Standby CP nodes during NTSR micro-checkpoint installation	cups-cp

© 2026 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description	Product Found
CSCww26794	Proactive UBReq not triggered post 2G->4G handover when PCRF CCA-U contain	cups-cp
CSCwx20089	Sessmgr Crash (Resource temporarily unavailable) observing in INVIGJ02GNR2SPCP01CO	cups-cp
CSCwx53520	Sessmgr failure at snx_pgw_driver_get_pdn_rcvry_info()	cups-cp
CSCwx53536	Sessmgr Crash on sessmgr_collect_pgw_call_rcvry_info()	cups-cp
CSCwx58383	S1 Error Ind Event in Connected Sx Pending State	cups-cp
CSCwt99888	Silent sessctrl restart during booting up of n:m UP after reload/switchover.	cups-up
CSCww51452	NAT port allocation failure for ICMP flow	cups-up
CSCww02980	DNS-Snoop Hashtable Leak	cups-up
CSCwo47013	Continuous confdmgr restart seen at function " confdmgr_fsm_state_wait_p0_handler"	cups-up
CSCwv883211	CUPS-UP slmgr restart - Task dead slmgr/0 cpu 1/0. Missed heartbeat	cups-up
CSCwu95813	IPSECMGR restart observed in function ikev2_encode_header_ipv4	epdg
CSCww47405	sgmentation fault observed on mme_send_delete_ded_brr_resp_with_cause	mme
CSCww89418	Flooding of mme-app error level log on Attach reject based on attach restrict policy	mme
CSCwv45580	sessmgr crashes due to assertion failure at sess/egtp/egtpc/egtpc_evt_handler_func.c:1073	mme
CSCwv51804	E-RAB Modification Collision During VoWiFi-to-VoLTE Handover Results in Bearer Setup Failure	mme
CSCwu77308	Incorrect Service request response or no response	mme
CSCwt84844	MON sub doesn't display context setup response	mme
CSCwv92851	mmemgr sending Aborts with cause " Out of resource" towards enodebs	mme
CSCwx15244	StarOS LI AVP Decode Enhancement decoded fields remain blank or display zero values	pdn-gw
CSCwv96074	Session Manager Crashes on the SAEGW running 21.28.m36 release	pdn-gw
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
CSCwt63057	Wrong time zone in CDRs	sgsn
CSCws02289	Legacy-GW: rct process in warn state due to high memory usage after mio card switch	staros
CSCww86561	Intel E810-XXV NIC compatibility with StarOS (VMWare ESXi 6.7)	staros

© 2026 Cisco and/or its affiliates. All rights reserved.

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 2026.04.gh1

Bug ID	Description	Product Found
CSCwx65666	SGW Is not send UB response with " EGTP_CAUSE_NO_RESOURCES_AVAILABLE" when Modify response is pending from UP for earlier ULI change MB request	cups-cp
CSCwv63320	Sessmgr restart at function sessmgr_epdg_dequeue_transcb_msg()	epdg
CSCwx08512	Planned Active SF Migration with Live Sessions Fails and Causes Significant Subscriber Drop in 21.28	mme
CSCwx65399	Sessmgr Process Assertion failure at sess/egtp/egtpc/egtpc_interface.c:298 | Function egtpc_handle_user_sap_event()	pdn-gw
CSCwv73793	Destination-Host AVP incorrectly set to DRA hostname when OCS Origin-Host exceeds 63 characters	pdn-gw
CSCwx25216	Show version <build> not displaying for secure boot enabled build	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

© 2026 Cisco and/or its affiliates. All rights reserved.

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.

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

Issue: When upgrading or downgrading between non-Hermes builds (202x.0x.[g/l/ga/la]x) and Hermes builds 202x.0x.[gah]x), on VPC-DI and VPC-SI 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 and Hermes builds.

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

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

© 2026 Cisco and/or its affiliates. All rights reserved.

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

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	2026.04.gh1	21.28.mh43.101856

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 2026.04.gh1

Product	Version
ADC P2P Plugin	2.74.gh4.2832
RCM	20261102-063542Z Note: Use this link to download the RCM package associated with the software.
ESC	6.0.0.64
HVIM	6.0.1 (RHOSP 18.0, RHEL 9.4, CIMC 4.3) **Note**: The SI deployment with 24 VPP threads was qualified with patch version 2.6.7 of the Intel ICE out-of-tree driver.
Host OS	RHEL 9.2
RedHat OpenStack	RHOSP 17.1
Intel XL710C NIC Version	Driver version: i40e-2.17.4 Firmware: 7.00 0x80005119 0.385.115
CIMC	4.2 (3)
NSO MFP	ncs-6.4.8.2-nso-mob-fp-4.0-bf213e2-2026-04-17T0418 ncs-6.4.8.2-nso-mob-fp-4.0-bf213e2-2026-04-17T0418.tar.gz **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.

© 2026 Cisco and/or its affiliates. All rights reserved.

Product	Version
SMI/CNDP	2026.04.1.10

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 2026.04.gh1

Software package	Description
NSO	
nso-mob-fp-4.0-2026.04.gh1.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-2026.04.gh1.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-2026.04.gh1.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-2026.04.gh1.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-2026.04.gh1.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-2026.04.gh1.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-2026.04.gh1.zip	Contains the VPC-DI binary software image that is used to on-board the software directly into VMware.
qvpc-di-template-vmware_T-2026.04.gh1.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-2026.04.gh1.zip	Contains the same VPC-DI ISO identified above and additional installation files for using it on KVM.
qvpc-di-template-libvirt-kvm_T-2026.04.gh1.zip	Contains the same trusted VPC-DI ISO identified above and additional installation files for using it on KVM.

© 2026 Cisco and/or its affiliates. All rights reserved.

Software package	Description
qvpc-di-2026.04.gh1.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-2026.04.gh1.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-2026.04.gh1.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-2026.04.gh1.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-2026.04.gh1.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-2026.04.gh1.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-2026.04.gh1.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-2026.04.gh1.zip	Contains the VPC-SI binary software image that is used to on-board the software directly into VMware.
qvpc-si-template-vmware_T-2026.04.gh1.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-2026.04.gh1.zip	Contains the same VPC-SI ISO identified above and additional installation files for using it on KVM.
qvpc-si-template-libvirt-kvm_T-2026.04.gh1.zip	Contains the same trusted VPC-SI ISO identified above and additional installation files for using it on KVM.
qvpc-si-2026.04.gh1.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-si_T-2026.04.gh1.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

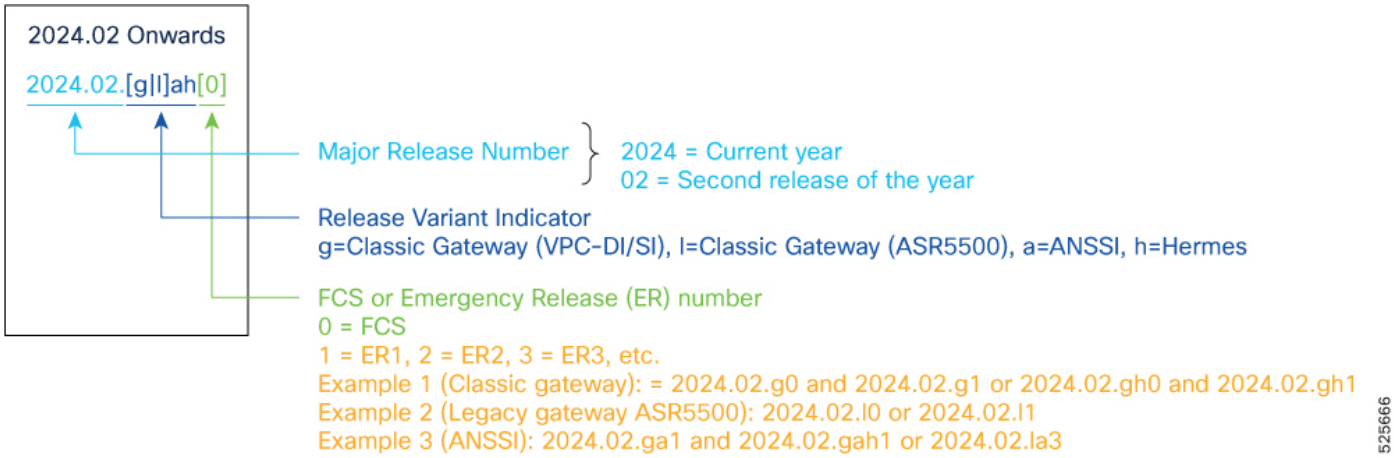
The output of the show version command displays detailed information about the version of StarOS currently running on the ASR 5500 or Cisco Virtualized Packet Core platform.

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.

© 2026 Cisco and/or its affiliates. All rights reserved.

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

© 2026 Cisco and/or its affiliates. All rights reserved.

Operating system	SHA512 checksum calculation command examples
	`$ 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

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. 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.