Release Notes for StarOS™ Software, Release 2025.03.g0

Contents

StarOS™ Software, Release 2025.03.g0

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

The key highlights of this release include:

- UEFI-based secure boot for VM-based RCM: Ensures only authenticated software runs at boot by verifying cryptographic signatures, enhancing system security.
- Option to disable SRP monitor-based switchovers for ICSR nodes: Allows operators to maintain session integrity and system stability by preventing SRP monitor-triggered switchovers.
- Timezone enhancements: Streamlines operations by removing the need for manual timezone workarounds and ensuring local time alignment.
- Multiple P-CSCF payload attributes support: Enables configuration of up to 10 IPv4/IPv6 P-CSCF address values, providing greater flexibility and simplifying complex setups.

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, Release 2025.03.g0

Milestone	Date
First Customer Ship (FCS)	14-Aug-2025
End of Life (EoL)	14-Aug-2025
End of Software Maintenance (EoSM)	12-Feb-2027
End of Vulnerability and Security Support (EoVSS)	12-Feb-2027
Last Date of Support (LDoS)	29-Jan-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 2025.03.g0

Product impact	Feature	Description
Software Reliability	Disabling SRP monitor-based switchovers for ICSR nodes	This feature lets operators disable Service Redundancy Protocol (SRP) monitor-based switchovers in the ICSR pair nodes preventing interruptions and ensuring session integrity during such events. Command introduced: **srp-monitor-based-switchover** {**enable** | **disable**}
Software Reliability	UEFI-based secure boot support for VM-based RCM	This feature introduces UEFI-based Secure Boot support for VM-based RCM, enhancing system security by ensuring only authenticated and trusted software is executed during the boot process. Secure Boot leverages cryptographic signatures to validate each stage of the bootloader and kernel, preventing unauthorized or tampered software from running. The implementation supports both Cisco and customer code signing, integrates with Cisco's certificate infrastructure, and provides clear guidelines for VM configuration, partitioning, and binary signing to maintain a secure and verifiable boot chain.
Ease of use	Timezone enhancements	To reflect the recent removal of Central Daylight Time (CDT) by the Government of Mexico, the Classic Gateway (GW) has been updated to support the revised Mexico timezone. This enhancement eliminates the need for workarounds, ensures seamless network operations, aligns with local time standards, and improves operational efficiency.
Upgrade	Support for multiple P-CSCF payload	This feature allows the network operator to configure multiple types for P-CSCF attributes in CFG_REQUEST and CFG_REPLY messages as part of the CP payload in the IKE_AUTH Request and Response messages

Product impact	Feature	Description
	attributes	that ePDG sends and receives from the UEs. Using this feature the network operator can configure a range of 10 values or up to 10 different values for IPv4 and IPv6 P-CSCF address attributes type. Command enhanced: **[no] configuration-payload private-attribute-type { imei imei_value | p-cscf-v4 { v4_value | range start_value end_value } | p-cscf-v6 { v6_value | range start_value end_value } }:** This CLI is configured under Crypto Template Configuration mode Default setting: Disabled–Always Enabled

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 2025.03.g0

Description	Behavior changes
Automatic SRP switchover for MAV issues during CF failover	**Previous Behavior**: On ASR 5500 systems, when a Control Function (CF) failure occurred and a redundant CF instance was available, the system would attempt to switch over to the standby CF to minimize service disruption. For example, if CF1 failed (such as a reboot), the system would automatically switch to the standby CF2—even if CF2 had a Multi Attach Volume (MAV) issue. In such cases, the chassis (active VNF) could enter an unrecoverable state. **New Behavior**: If a CF failure occurs and the newly active CF card (for example, CF2) has a MAV issue, the system now automatically initiates a Service Redundancy Protocol (SRP) switchover. This SRP switchover process helps ensure system recovery and typically completes in approximately 3 minutes.
MME Handling of NR UE Security Capability in Path Switch Procedures	**Previous Behavior**: MME includes the NR UE Security Capability Information Element (IE) over the S1AP interface in the following messages: • INITIAL-CONTEXT-SETUP-REQUEST • PATH-SWITCH-REQUEST-ACK If the MME receives the NR UE Security Capability in a PATH SWITCH REQUEST from the eNodeB, it uses this value in the PATH SWITCH ACK. Otherwise, it parses and uses the NR UE Security Capability from the UE Additional Security Capability received in one of these messages: • ATTACH REQUEST • TAU REQUEST • UE-CONTEXT-MODIFICATION-REQUEST • HANDOVER REQUEST • DOWNLINK-NAS-TRANSPORT **New Behavior**: If the MME receives the NR UE Security Capability in a PATH SWITCH REQUEST from eNodeB, it now ignores this value. Instead, the MME always uses its backed-up value parsed from the UE Additional Security Capability received in the ATTACH or TAU request when sending

Description	Behavior changes
	the PATH SWITCH ACK.
Updated cause to handle SGW errors during 4G to 5G handover	**Previous behavior**: For Pure S call, if the Update Bearer Request is received while the SGW is already processing Modify Bearer Request for the PRA change, then the Update Bearer Request message was rejected with the cause No Resource Available. **New behavior**: For Pure S call, if the Update Bearer Request is received while the SGW is already processing Modify Bearer Request for the PRA change, then the Update Bearer Request is silently dropped. The P-GW retries the Update Bearer Request message and S-GW processes it.

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 2025.03.g0

Bug ID	Description	Product Found
CSCwq20529	vpnmgr restart at function vpnmgr_lookup_pool_by_id_slow()	cups-cp
CSCwq30875	Session manager recovery status instability	cups-cp
CSCwq09903	Corrupted Diameter Realm value in STR	cups-cp
CSCwq31050	sessmgr reload after ECS configuration modification	cups-cp
CSCwq00805	CUPS-CP not triggering CCRU to PCRF after wifi to wifi handover	cups-cp
CSCwp03503	CDR corruption after CP switchover	cups-cp
CSCwp16586	Generated URRs are not associated with PDR's when the Online Charging System (OCS) is in a Server Unreachable (SU) state.	cups-cp
CSCwo94253	3GPP-Reporting-Reason VALIDITY_TIME in the CCR-U after GY RAR	cups-cp
CSCwq22329	Lack of P-CSCF address in EGTP_CREATE_SESSION_RESPONSE in case of VoWiFi	cups-cp
CSCwp84482	Mapping of Default IMS bearer QCI set 1 by PGW so no dedicated created for the reason UE faced Issue while connecting to call once to comes back to volte from vowifi.	cups-cp
CSCwq18010	MBR-UBR collision in CUPS-SGW during handover	cups-cp
CSCwp10751	Periodic updates not being sent when 'diameter send-ccri session-start' is configured	cups-cp
CSCwk31021	On CUPS-CP node multiple session manager restarts observed after SRP switchover	cups-cp
CSCwo87056	Wrong UP behavior after getting CREDIT_LIMIT_REACHED	cups-up
CSCwq18455	Huge amount of logs skipping adf creation for NAT subscriber in UPF	cups-up

Bug ID	Description	Product Found
CSCwj84817	sessmgr crash observed [21.28.m3.88506] :Function: sessmgr_handle_get_global_smgr_stats()	cups-up
CSCwp83463	Multiple sessmgr 12093 error logs generated in the system	cups-up
CSCwo35415	gtpumgr OVER state for volte UPF's	cups-up
CSCwn78141	Packet drops when GSU in CCA-I only provides CC-TIME with FUI terminate without volume quota	cups-up
CSCwo47679	Buffered bytes dropped due to flow action discard in charging action incorrect under input byte drop	cups-up
CSCwo64859	Frequent authentication failures in the second PDN on ePDG	epdg
CSCwn30866	mme sessmgr crash-mme_pdn_fsm_connect_pending_brr_evt	mme
CSCwp84512	To send unauthenticated IMSI in Location Report Request for unauthenticated emergency attach with IMSI	mme
CSCwo87872	Code change to drop a PDN Connection Request for an existing PDN with same APN when Service Request Procedure is ongoing and 'policy pdn-reconnection restart' is configured	mme
CSCwq12952	During X2 handover MME modifies NR UE Security Capabilities received in Path Switch Request prior returning it to eNB	mme
CSCwo68956	Handling of enodeb transmission to avoid mmemgr crash	mme
CSCwp32238	SLR being triggered for default bearer aswell during handover	mme
CSCwo70089	EDR getting generated without TAC	pdn-gw
CSCvd29285	FE chip internal table bit flip causing chassis reboot	pdn-gw
CSCvd01015	Fabric serdes lanes flapping leading to AFIO: " Event stuck in list" message filling up syslog	pdn-gw
CSCwo37912	Legacy-GW ATT: vpnmgr crash observed in sn_tacacs_authen_login_cleanup function	pdn-gw
CSCwo74921	Error log for SGW - wrong 'recordOpeningTime' in CDR	sgw
CSCwq14804	" starBusyoutReason" and " starSxPeerIP" are used/referenced and not defined.	staros
CSCvq18187	Auto collect register dumps for analysis of Ingress fabric (IFMA/IFMB) overflows	staros
CSCux53126	AF Controller takes abnormally long time for card update notification	staros
CSCvq76231	Fabric issues causing IFMA/IFMB buffer overflows	staros
CSCwo89406	Incorrect value in Rx port utilization counter	staros
CSCvx22943	Monitor DCH FIFO Discards in the FE600 health check	staros
CSCvm53290	Traffic needs to be stopped after a fabric event in order to recover	staros

Bug ID	Description	Product Found
CSCvd23310	MIO reload due to un-correctable error; MIO went into permanent boot cycle	staros
CSCvt06102	DPC2 memory correctable errors over threshold causing fabric IFMA/Bs	staros
CSCvb40910	DPC2/MIO1: Both cards reboot due to unplanned migration	staros
CSCwo65162	Incorrect output in command " show bulkstats internal intervals"	staros
CSCwo01479	Unplanned SF migration caused diamproxy instance # out of range	staros
CSCuy34023	Nonfatal warning AFIO Process during system upgrade	staros
CSCuz46018	ASR5500 manual clock change failure (fabric ping stops)	staros
CSCux61392	ASR5500 restarted - petrab FDR IFMA overflow -> hatcpu dead!	staros
CSCvh07441	Fabric issues causing IFMA/IFMB buffer overflows	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 2025.03.g0

Bug ID	Description	Product Found
CSCwp28316	Sx peer failure with demux SF unplanned migration	cups-cp
CSCwp20248	CP is not sending Delete session request to UP in case of GTPU Path Failure	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
CSCwq56872	Generated URR's are not associated with PDR's when the Online Charging System (OCS) is in a Server Unreachable (SU) state.	cups-cp
CSCwo82799	CUPS UP UL/DL packets dropping	cups-up
CSCwq29508	After SGW relocation (S1-HO), traffic not sent.	cups-up
CSCwq36099	ePDG VPC-SI: dhmgr mem warn	epdg
CSCwq48299	Incorrect VLR Status Displayed on MME Post sgs vlr-failure/vlr-recover with Pooled VLRs.	mme
CSCwq50254	Fatal Signal 11: failures observed due to sessmgr_dhcpv6app_api_release_address	pdn-gw

Bug ID	Description	Product Found
CSCwq22148	Legacy-GW ATT: ASR5500 chassis hwctrl process shows warn state in show task resources	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
CSCwq60067	Disable rapid-commit-dhcpv6' command causing SRP Peer Checksum failure error during the image upgrade in Legacy	pdn-gw
CSCwq56385	Assertion failure at midplane/libsn_midplane.c in SPGW	sae-gw
CSCwp60108	session manager crash with an unknown signature time encoding data at smgr_gr_encode_uplane_call_info_uchckpt_cmd	sae-gw
CSCwq58304	Peer Checksum Validation Failure during upgrade test from Apr25 FCS build to July25 EFT2 build	upf

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 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	2025.03.g0	21.28.m36.98639

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 2025.03.g0

Product	Version
ADC P2P Plugin	2.74.10.2682
RCM	20250723-132226Z
ESC	5.6.108
CVIM	4.4.3
Host OS	RHEL 8.4
RedHat OpenStack	RHOSP 16.2
Intel XL710C NIC Version	Driver version: i40e-2.17.4 Firmware: 7.00 0x80005119 0.385.115
CIMC	4.0 (4)
NED Package	ncs-6.1.11.2-nso-mob-fp-3.5.2 -ad74d4f-2024-10-18T1052/ncs-6.1.11.2 -nso-mob-fp-3.5.2-ad74d4f-2024-10- 18T1052.tar.gz

Product	Version
NSO	nso-mob-fp-3.5.2

Supported software packages

This section provides information about the release packages associated with StarOS Classic Gateway, Control, and User Plane Separation (CUPS) software.

Table 9. Software packages for Release 2025.03.g0

Software package	Description
NSO	
nso-mob-fp-3.5.2-2025.03.g0.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-2025.03.g0.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-2025.03.g0.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-2025.03.g0.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-2025.03.g0.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-2025.03.g0.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-2025.03.g0.zip	Contains the VPC-DI binary software image that is used to on-board the software directly into VMware.
qvpc-di-template-vmware_T-2025.03.g0.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-2025.03.g0.zip	Contains the same VPC-DI ISO identified above and additional installation files for using it on KVM.
qvpc-di-template-vmware-2025.03.g0.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-2025.03.g0.zip	Contains the same trusted VPC-DI ISO identified above and additional

Software package	Description
	installation files for using it on KVM.
qvpc-di-2025.03.g0.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-2025.03.g0.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-2025.03.g0.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-2025.03.g0.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-2025.03.g0.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-2025.03.g0.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-2025.03.g0.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-2025.03.g0.zip	Contains the VPC-SI binary software image that is used to on-board the software directly into VMware.
qvpc-si-template-vmware_T-2025.03.g0.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-2025.03.g0.zip	Contains the same VPC-SI ISO identified above and additional installation files for using it on KVM.
qvpc-si-template-libvirt-kvm_T-2025.03.g0.zip	Contains the same trusted VPC-SI ISO identified above and additional installation files for using it on KVM.
qvpc-si-2025.03.g0.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-2025.03.g0.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.
RCM	
rcm-vm-airgap-2025.03.g0.ova.zip	Contains the RCM software image that is used to on-board the software directly into VMware.
rcm-vm-airgap-2025.03.g0.qcow2.zip	Contains the RCM software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack.

Software package	Description
rcm-vm-airgap-2025.03.g0.vmdk.zip	Contains the RCM virtual machine disk image software for use with VMware deployments.

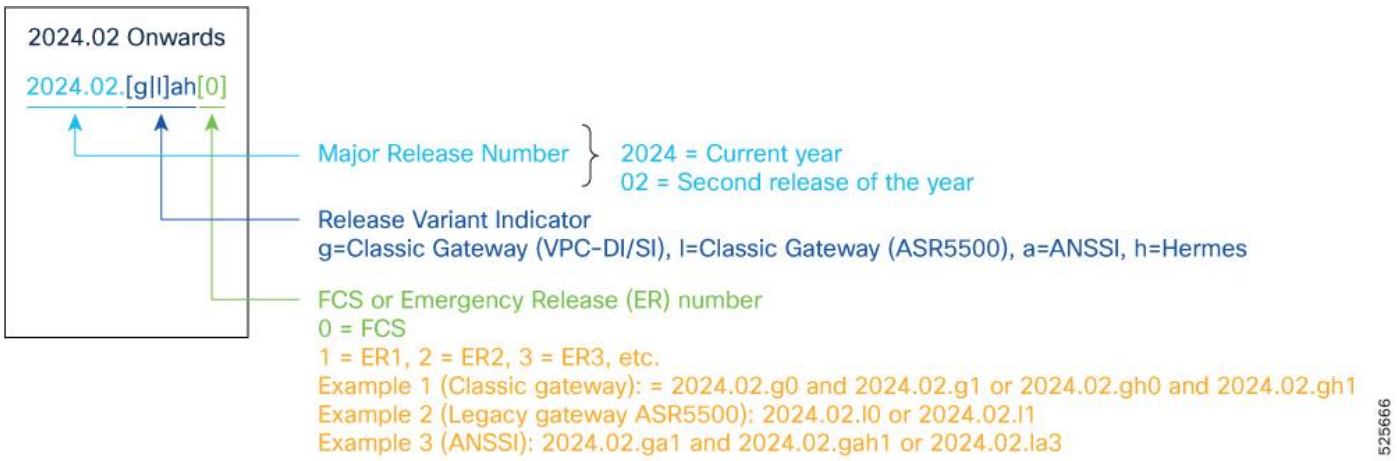
StarOS product version numbering system

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