Release Notes for the StarOS™ Software Version 2025.02.gh0

First Published: April 30, 2025

Introduction

This Release Notes identifies changes and issues related to the Legacy GW, Control and User Plane Separation (CUPS) software releases.

Products Qualified and Released in this Release

Products	Qualified?
CUPS	Yes
MMEs	Yes
ePDG	Yes
P-GW	Yes
SAEW	Yes
SGSN	Yes
Platforms	
ASR5500	No
VPC-DI	Yes
VPC-SI	Yes

Release Lifecycle Milestones

Release Lifecycle Milestone	Milestone	Date
First Customer Ship	FCS	30-Apr-2025
End of Life	EoL	30-Apr-2025
End of Software Maintenance	EoSM	29-Oct-2026
End of Vulnerability and Security Support	EoVSS	29-Oct-2026
Last Date of Support	LDoS	31-Oct-2027

Release Package Version Information

StarOS Packages	Version	Build Number
StarOS Package	2025.02.gh0	21.28.mh27.97848

Descriptions for the various packages provided with this release are available in the Release Package Descriptions section.

Verified Compatibility

Products	Version
ADC P2P Plugin	2.74.h5.2659
RCM	20250423-134337Z **Note**: Use this link to download the RCM package associated with the software.
ESC	6.0.0.52
Host OS	RHEL 9.2
RedHat OpenStack	RHOSP 17.1
E810C NIC Version	Driver: 1.12.6 Firmware: 4.20 0x80018f67 0.387.18
CIMC Version (UCS C220-M6S)	4.3 (2.230207)
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
NSO-MFP	nso-mob-fp-3.5.2

Note: Use only these compatible software versions for the products qualified in this release.

What's New in this Release

Features and Enhancements

This section covers a brief description of the features and enhancements introduced in this release.

Feature Title	Description	Product

Fallback to default rulebase during movement from 5G area to 4G area	This feature allows a session to revert to the default rulebase when transitioning from a 5G area to a 4G area. It ensures continuity of the call using the default rule configured under the APN, even if the PCRF removes the installed rulebase during the transition. Commands Introduced: **active-charging fallback-to-apn-rulebase**: This CLI is configured under APN to make the session fallback to its default rulebase. **Default Settings**: Disabled—Configuration Required to Enable.	CUPS
Load and overload control in multi-Sx scenario	This feature extends the load and overload control functionality to multi-Sx scenario. This allows other UPs to share the load of incoming new calls if an existing UP fails due to any error. **Default Settings**: Always-enabled.	CUPS
Deployment of CUPS on CNDP with UCS M7 Server	This release supports the deployment and configuration of CUPS on CNDP and KVM-based Redundancy and Configuration Management (RCM). **NOTE**: You can also automate the deployment of CUPS on CNDP using the NSO Automation Function Pack (AFP). This feature is beneficial for new operators aiming to deploy CUPS on CNDP. Additionally, it supports existing operators seeking to expand their network using the UCS M7 server and transition their CUPS deployment from OpenStack to CNDP on M7. For detailed information, see the *Ultra Packet Core CUPS Control Plane Administration Guide for Release 21.28*, the *NSO Subscriber Microservices Infrastructure Automation Function Pack (AFP) Configuration Guide for Release 2025.02.0*, and the *UCC SMI Operations Guide*.	CUPS
Qualification of CUPS on OSP 17	The Red Hat OpenStack Platform version 17.1 with RHEL 9.2 has been validated with ESC 6.0 and recommended for use with CUPS deployments. For more information on deploying RHEL 9.2/OSP 17.1, see the RedHat documentation.	CUPS
RADIUS retry counters for context replacement	The RADIUS Accounting feature is enhanced with RADIUS retry counters for context replacement. The following bulk statistics are added to the RADIUS schema: • **acc-rsp-drop-sgw-context-replacement** - Total accounting response messages dropped due to SGW context replacement • **acc-req-timeout-sgw-context-replacement** - Total accounting request messages timed out due to SGW context replacement	PGW
Support for MFA based authentication for console login	This feature enhances TACACS+ MFA support for console port login through Telnet and SSH services. Commands Introduced: **[no] console challenge-response-authentication**: This CLI command is configured under Context configuration mode to enable TACACS+ MFA for console port login through SSH or Telnet. **Default Settings**: Disabled-Configuration required to enable.	StarOS

Behavior Changes

This section covers a brief description of the behavior changes introduced in this release.

Behavior Change	Description
Bypass downlink-initiated TCP/UDP flow in CUPS node	**Previous Behavior**: In CUPS, TCP/UDP flows initiated from the downlink public NAT IP were created, but packets were dropped during NAT processing, resulting in flows with zero volume. When subscribers moved from idle to active state, downlink-initiated flows were sometimes misinterpreted as originating from the subscriber's private IP, allowing them to bypass NAT treatment. **New Behavior**: For subscribers with many-to-one NAT enabled, flow creation is bypassed for downlink-initiated TCP/UDP flows and ICMP (non-error messages) flows. This change aims to prevent the creation of empty or zero volume EDRs and creation of non-Nat flows.
Removal of the overload data statistics after clearing the User plane service statistics	**Previous Behavior**: When the Userplane Service Statistics were cleared, the Overload Data Statistics were not cleared. The system continued to fetch VPP overload or self-protection state statistics for dropped packets. **New Behavior**: Clearing the Userplane Service Statistics now also clears the Overload and self-protection data statistics, ensuring a comprehensive reset of all related metrics.
Counting the ICMPv6 drop packets at session manager	**Previous Behavior**: ICMPv6 packets going through the VPP were not counted at the Session Manager, resulting in a zero count for ICMPv6 packet drops. **New Behavior**: Packet drops at the Session Manager are now counted, including ICMPv6 drop packets, providing a more accurate reflection of packet handling. This change ensures that ICMPv6 packet drops are accurately recorded, improving network diagnostics and monitoring.

Related Documentation

For a complete list of documentation available for this release, go to: https://www.cisco.com/c/en/us/support/wireless/virtual-packet-core/products-installation-and-configuration-guides-list.html

Installation 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.

Synchronizing Boot File for Service Function Cards

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.

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.

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 1. 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 -a512 <filename>.<extension>`

Linux	Open a terminal window and type the following command:
	`$sha512sum <filename>.<extension>`
	Or
	`$shasum -a512 <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.

Firmware Updates

There is no firmware upgrade required for this release.

Open Bugs

The following table lists the open bugs in this specific software release.

Note: This software release may contain open bugs first identified in other releases. Additional information for all open bugs for this release are available in the Cisco Bug Search Tool.

Table 2. Open bugs in this release

Bug ID	Headline	Product Found
CSCwo93460	sxmgr_pfcp_read_callback()	cups-cp
CSCwo47679	Buffered bytes dropped due to flow action discard in charging action incorrect under input byte drop	cups-up
CSCwk65512	ipsecmgr cpu warn/over during make-break sessions with 4096 keysize device certificate	epdg
CSCwo37912	Vpnmgr crash observed in sn_tacacs_authen_login_cleanup function	pdn-gw
CSCwo75863	Sessmgr restarts after enabling VoLTE for specific inroamer IMSIs ranges	pdn-gw
CSCwo74921	Error log for SGW - wrong 'recordOpeningTime' in CDR	sgw

Resolved Bugs

This document uses the following conventions. The following table lists the resolved bugs in this specific software release.

Note: This software release may contain open bugs first identified in other releases. Additional information for all resolved bugs for this release are available in the Cisco Bug Search Tool.

Table 4. Resolved bugs in this release

Bug ID	Headline	Product Found
CSCwn98063	Multiple sessmgr crash happened w.r.t. diameter route table and sessmgr were in standby state	cups-cp
CSCwn12297	Cannot change monitoring key at session level on CUPS when changing rulebase and ruledef	cups-cp
CSCwn94146	CUPS-CP doesn't retry to send CCR-U to the secondary OCS again after 3004 from the first OCS	cups-cp
CSCwo41694	Flooded Warning msg in CUPS CP	cups-cp
CSCwo33578	Unexpected session disconnection	cups-cp
CSCwo57407	CSResp should be sent with PCI=1 and PVI=0 when those are not included in ARP on CCA-I	cups-cp
CSCwm40394	Sx-IPSec - clear crypto security-association results in Sx failure	cups-cp
CSCwo44644	Assertion failure at snutil/sn_memblock.c:258	cups-cp
CSCwo57071	audit_chassis_state is empty in bulkstats	cups-cp
CSCwn75996	Sessmgr restart-sgwdrv_send_create_session_rsp_failure()	cups-cp
CSCwo28191	PGW is not terminating the sessions after receiving 3002 diameter result code from OCS	cups-cp
CSCwo67004	Incorrect number of the Active Subscribers for collapsed call in show saegw-service all	cups-cp
CSCwo10621	[CUPS / LIVE / CP / 21.28.h7] CLI crash : PC: [f6fe1b6f/X] libc.so.6/__strlen_ia32()	cups-cp
CSCwk79042	SX path failure is not leading to SRP switchover with sx monitor enabled	cups-up
CSCwm47782	UP not sending 'sx session report' to CP when UE goes into Idle state in RA case.	cups-up
CSCwo21877	ipsecmgr crash for function :: ipmcrypt_dh_pubkey_alloc in EPDG	epdg
CSCwk39766	Memory usage kept increasing for ipsecmgr instances on ePDG when server certificate config used	epdg
CSCwo21333	Sessmgr ASSERTs at egtpc_handle_user_sap_event()	epdg
CSCwm81858	" VPLMN access in not Allowed" CCP is applicable for Emergency SIP call, which must be ignored	mme

Bug ID	Headline	Product Found
CSCwn39406	MME TAI specific statistics are populated with erroneous values	mme
CSCwn43642	Sessmgr crash-mme_app_egtpc_abort_low_priority_trans()	mme
CSCwh97716	Sessmgr restarts while changing traffic between SPGWs,	mme
CSCwn87726	Assertion failure at snmp/send_trap.c:6540	mme
CSCwn18588	Multiple sessmgr in warn state due to mme_app_allocate_ue_addl_security_cap and SN_cmAlloc	mme
CSCwo41780	TAUs are getting rejected with “UE identity cannot be delivered”	mme
CSCwj29750	Sessmgr restart after SW upgrade to 21.28.m19, mme_auth_awt_hss_hss_resp()	mme
CSCwn42611	Sessmgr unexpected restart on multiple MME due to memory corruption	mme
CSCwn29026	Sessmgr crash at mme_auth_awt_hss_hss_resp()	mme
CSCwo45335	Sessmgr restart observed during the wifi to lte handover scenario	pdn-gw
CSCwn55113	After vPGW software upgrade (21.28.mh20-95098) customer observing all cards lock state "UNKNOWN"	pdn-gw
CSCwo22197	Assertion failure at vpn/vpnmgr/vpnmgr_kernel and observing 2 crashes	pdn-gw
CSCwn65225	Support required for Radius accounting retry for context replacement	pdn-gw
CSCwo70089	EDR getting generated without TAC	pdn-gw
CSCwo34877	Legacy-GW:sessmgr limit changed to 20k on sessctrl and multiple sessmgr restarts	pdn-gw
CSCwo35989	Sessmgr restart: sessmgr_ipv4_process_inet_pkt_part3_pgw_ggsn()	pdn-gw
CSCwn58706	CDRs are stucked when transport problems were observed	sae-gw
CSCwn19439	CVIM5.0.1 - VPCDI deployment fails to bring up SF	staros
CSCwn41761	Flash, hard drive and service interfaces not getting loaded in 21.28.hx	staros

Operator Notes

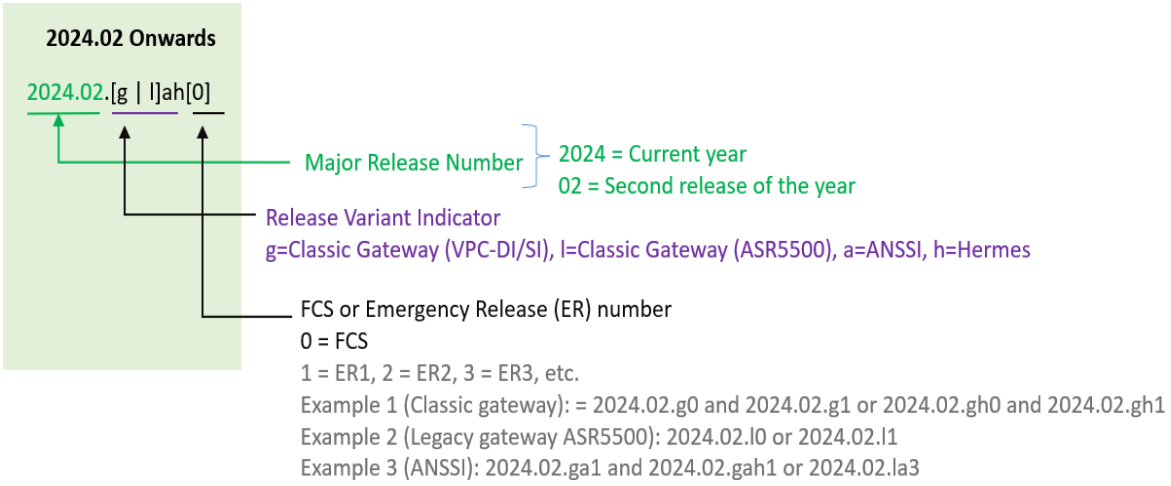
Software Version Numbering System

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.

Release Package Descriptions

The table provides examples of packages according to the release. For more information about the release packages up to 21.28.x releases, refer to the corresponding releases of the release note.

Table 5. Release package information

Software Package	Description
ASR 5500	
asr5500-<release>.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.
asr5500_T-<release>.zip	Contains the signed, trusted 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.
VPC Companion Package	
companion-vpc-<release>.zip For example, companion-vpc- 2024.02.gh2.i4.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-<release>.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-<release>.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-<release>.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-<release>.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- <release>.zip	Contains the VPC-DI binary software image that is used to on-board the software directly into VMware.
qvpc-di-template-vmware_T- <release>.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- <release>.zip	Contains the same VPC-DI ISO identified above and additional installation files for using it on KVM.
qvpc-di-template-libvirt-kvm_T- <release>.zip	Contains the same trusted VPC-DI ISO identified above and additional installation files for using it on KVM.

qvpc-di-<release>.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-<release>.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	
intelligent_onboarding-<release>.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-<release>.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-<release>.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-<release>.iso.zip	Contains the VPC-SI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image.
qvpc-si_T-<release>.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-<release>.zip	Contains the VPC-SI binary software image that is used to on-board the software directly into VMware.
qvpc-si-template-vmware_T-<release>.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-<release>.zip	Contains the same VPC-SI ISO identified above and additional installation files for using it on KVM.
qvpc-si-template-libvirt-kvm_T-<release>.zip	Contains the same trusted VPC-SI ISO identified above and additional installation files for using it on KVM.
qvpc-si-<release>.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-<release>.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-<release>.ova.zip	Contains the RCM software image that is used to on-board the software directly into VMware.
rcm-vm-airgap-<release>.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.
rcm-vm-airgap-<release>.vmdk.zip	Contains the RCM virtual machine disk image software for use with VMware deployments.
Ultra Services Platform	
usp-<version>.iso	The USP software package containing component RPMs (bundles).

usp_T-<version>.iso	The USP software package containing component RPMs (bundles). This bundle contains trusted images.
usp_rpm_verify_utils-<version>.tar	Contains information and utilities for verifying USP RPM integrity.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.