



# Release Notes for the StarOS™ Software Version 2024.03.gah0

**First Published:** July 31, 2024

## Introduction

This Release Notes identifies changes and issues related to the CUPS software release.

## Release Lifecycle Milestones

| Release Lifecycle Milestone               | Milestone | Date        |
|---|-----------|-------------|
| First Customer Ship                       | FCS       | 31-Jul-2024 |
| End of Life                               | EoL       | 31-Jul-2024 |
| End of Software Maintenance               | EoSM      | 30-Jan-2026 |
| End of Vulnerability and Security Support | EoVSS     | 30-Jan-2026 |
| Last Date of Support                      | LDoS      | 29-Jan-2027 |

## Release Package Version Information

| Software Packages | Version      | Build Number   |
|-------------------|--------------|----------------|
| StarOS Package    | 2024.03.gah0 | 21.28.h8.94492 |

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.h1.2328  |
| RCM            | 20240724-143322Z  |
| NED Package    | ncs-6.1.6.1-nso-mob-fp-3.5.1-b3a2303-2024-07-24T0350<br>ncs-6.1.6.1-nso-mob-fp-3.5.1-b3a2303-2024-07-24T0350.tar.gz |
| NSO-MFP        | 6.1.6.1-3.5.1   |

## What's New in this Release

This version of Release Notes includes a new section titled **What's New in this Release** comprising all new features, enhancements, and behavior changes applicable for the release.

## Features and Enhancements

There are no specific features and enhancements in this release.

## Related Documentation

For a complete list of documentation available for this release, go to:

<http://www.cisco.com/c/en/us/support/wireless/asr-5000-series/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 executable command:

```
[local] host_name# system synchronize boot
```

This assures that the changes in boot file are identically maintained across the SF cards.

Ensure that you execute this command before reload for version upgrade from any version less than mh14 to mh14 or later.

## Firmware Updates

There are no firmware upgrades required for this release.

## 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 Table 1 and verify that it matches either the one provided on the software download page.

To calculate a SHA512 checksum on your local desktop see Table 1

**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<br><br><pre>&gt; certutil.exe -hashfile &lt;filename&gt;.&lt;extension&gt; SHA512</pre>  |
| Apple MAC   | Open a terminal window and type the following command<br><br><pre>\$ shasum -a 512 &lt;filename&gt;.&lt;extension&gt;</pre>  |
| Linux   | Open a terminal window and type the following command<br><br><pre>\$ sha512sum &lt;filename&gt;.&lt;extension&gt;</pre> <p>Or</p> <pre>\$ shasum -a 512 &lt;filename&gt;.&lt;extension&gt;</pre> |
| <p><b>NOTES:</b></p> <p>&lt;filename&gt; is the name of the file.</p> <p>&lt;extension&gt; is the file extension (e.g. .zip or .tgz).</p> |  |

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.

## Open Bugs for this Release

## 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.

## Open Bugs for this Release

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 |
|-----------------------------|--|---------------|
| <a href="#">CSCCwk67137</a> | [CUPS / LIVE / CP / 21.28.h7] Di-Net Heartbeat drop > 1% - Health status = Bad                     | cups-cp       |
| <a href="#">CSCCwk67344</a> | [CUPS / LIVE / UPF / 21.28.h7] sess/egtp/egtpu/egtpu_session.c:2712                                | cups-up       |
| <a href="#">CSCCwk49621</a> | Server Unreachable 5030, No Gz URRs are created on UP and the URR quota is not replenished         | cups-cp       |
| <a href="#">CSCCwk82412</a> | TCP flow classification breaks and flow readdressing is not working afterwards                     | cups-up       |
| <a href="#">CSCCwi59047</a> | Fatal Signal 6: Aborted PC: [f7f63062/X] ld-linux.so.2/_dl_sysinfo_int80()                         | cups-up       |
| <a href="#">CSCCwi68424</a> | Observing Sxdemux in warn/over state in Volte ICSR Standby UP nodes                                | cups-up       |
| <a href="#">CSCCwk65512</a> | ipsecmgr cpu warn/over with device certificate and imsi privacy make-break                         | epdg          |
| <a href="#">CSCCwk81092</a> | Observed mmemgr restart and after mmemgr task kill its going to warn state                         | mme           |
| <a href="#">CSCCwi57303</a> | Enhancement to DCNR bulkstats - New CLP based connected, idle and total DCNR capable sessions      | mme           |
| <a href="#">CSCCwk77504</a> | 21.28.mhx: SNMP traps not getting generated for NTP states   | staros        |
| <a href="#">CSCCwi73773</a> | Post unplanned MIO switchover all services failed to start and all contexts went into Initializing | staros        |
| <a href="#">CSCCwi67156</a> | RTNETLINK socket recv buffer under run error code 105 on hermes branch sw build on CUPS CP         | staros        |
| <a href="#">CSCCwk90352</a> | Observed the vpnmgr crash "vpnmgr_ip_pool_icmp_init" in 21.28.hx                                   | staros        |

## Resolved Bugs for this Release

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

**NOTE:** This software release may contain bug fixes first introduced in other releases. Additional information for all resolved bugs for this release are available in the [Cisco Bug Search Tool](#).

**Table 3 - Resolved Bugs in this Release**

| Bug ID                     | Headline  | Product Found |
|----------------------------|---|---------------|
| <a href="#">CSCwk52721</a> | Home & roamer subscriber type changed to visitor after multiple sessmgr & aaamgr killed by sessctrl | cups-cp       |
| <a href="#">CSCwi84745</a> | Sx IP Pool is in Disable state  | cups-cp       |
| <a href="#">CSCwh04674</a> | INSUFFICIENT_BEARER_RESOURCES high  | cups-cp       |
| <a href="#">CSCwh37204</a> | sessmgr crash with libc.so.6/___memcpy_sse2_unaligned()   | cups-up       |
| <a href="#">CSCwe17332</a> | IpsecDemux process restart due to invalid IpsecMgr id   | epdg          |
| <a href="#">CSCwf13605</a> | ipsecdemux crash on asr5500 during crypto call model longevity                                      | epdg          |
| <a href="#">CSCwd51494</a> | IPsecMgr task restart while decrypting packets.   | epdg          |
| <a href="#">CSCwk03546</a> | Multiple AAAMGR are in warn state   | epdg          |
| <a href="#">CSCwf18184</a> | Multiple Ipsecmgr's are in warn state in 21.28.m3 build   | epdg          |
| <a href="#">CSCwf94414</a> | ipsecmgr memory leak when certificate chain used for authentication                                 | epdg          |
| <a href="#">CSCwk63359</a> | vpnmgr task restarts due to DNS Timeouts/ServFail   | mme           |
| <a href="#">CSCwj57663</a> | Remove mme_app_send_multipath_zero_action_recovery_req API from mme_app_ope()                       | mme           |
| <a href="#">CSCwi02791</a> | sessmgr restart occurs when session moves to assume positive state                                  | pdn-gw        |
| <a href="#">CSCwh00793</a> | Assertion failure at sess/sgsn/sgsn-app/sm/msg_fsm_table Function: SmGenDownLinkDataInd()           | sgsn          |
| <a href="#">CSCwk63293</a> | Nessus scan: High- CVE-2024-6387- OpenSSH < 9.8 RCE   | staros        |

Operator Notes

| Bug ID                     | Headline                               | Product Found |
|----------------------------|--|---------------|
| <a href="#">CSCwd75750</a> | ipsecmgr_process_crashed at ipm_sad    | staros        |
| <a href="#">CSCwk08792</a> | BGP Routes Lost after Demux SF Restart | staros        |

## Operator Notes

### StarOS Version Numbering System

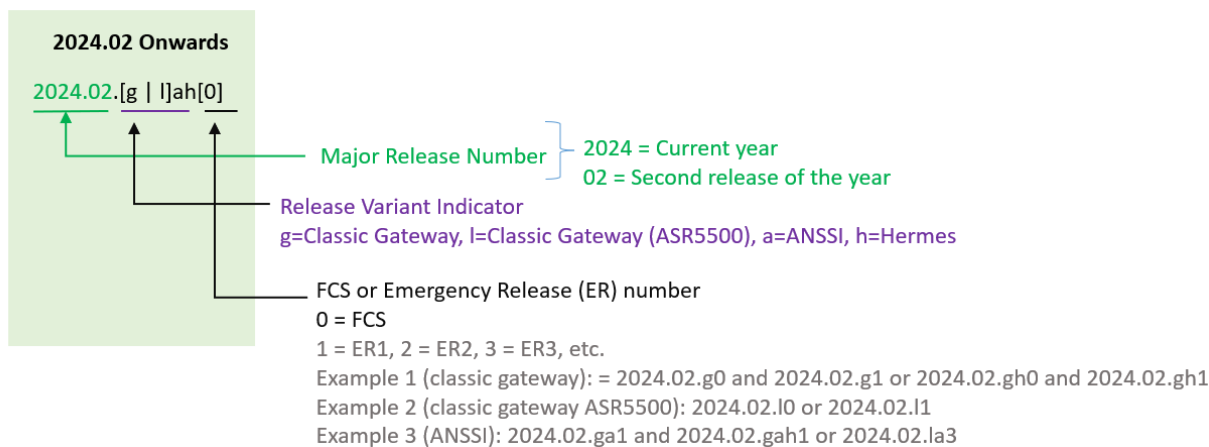
The output of the **show version** command displays detailed information about the version of StarOS currently running on the ASR 5500 or Cisco Virtualized Packet Core platform.

**NOTE:** 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 [Figure 1](#) for more details.

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.

### Version Numbering for FCS, Emergency, and Maintenance Releases

**Figure 1 - Version Numbering**



**Note:** For any clarification, contact your Cisco account representative.

### Release Package Descriptions

**Table 4** 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 4 - Release Package Information**

| Software Package   | Description   |
|--|---|
| <b>ASR 5500</b>  |   |
| 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. |
| <b>VPC Companion Package</b>   |   |
| companion-vpc-<release>.zip<br><br>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. |
| <b>VPC-DI</b>  |   |
| qvpn-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.  |
| qvpn-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.  |
| qvpn-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.   |
| qvpn-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.   |
| qvpn-di-template-vmware-<release>.zip  | Contains the VPC-DI binary software image that is used to on-board the software directly into VMware.   |
| qvpn-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.   |
| qvpn-di-template-libvirt-kvm-<release>.zip                                       | Contains the same VPC-DI ISO identified above and additional installation files for using it on KVM.  |
| qvpn-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.  |
| qvpn-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.   |
| qvpn-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.   |
| <b>VPC-SI</b>  |   |
| 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.                                  |
| <b>RCM</b>                                   |  |
| 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.  |
| <b>Ultra Services Platform</b>               |  |
| usp-<version>.iso                            | The USP software package containing component RPMs (bundles).<br>Refer to the <a href="#">Table 5</a> for descriptions of the specific bundles.                                      |
| usp_T-<version>.iso                          | The USP software package containing component RPMs (bundles). This bundle contains trusted images.<br>Refer to the <a href="#">Table 5</a> for descriptions of the specific bundles. |
| 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, refer to <https://www.cisco.com/c/en/us/support/index.html>.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright ©1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

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: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2024 Cisco Systems, Inc. All rights reserved.