Release Notes for UCC 5G UPF, Release 2026.04.h0

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

Ultra Cloud Core – User Plane Function, Release 2026.04.h0 3
New software features 3
Changes in behavior 3
Resolved issues 3
Open issues 4
Compatibility 4
Supported software packages 4
Related resources 7
Legal information 8

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

Ultra Cloud Core - User Plane Function, Release 2026.04.h0

This Release Notes identifies changes and issues related to the release of 5G User Plane Function (UPF).

For more information on UPF, see the Related resources section.

Release lifecycle milestones

The following table provides EoL milestones for Cisco UCC UPF software:

Table 1. EoL milestone information for UCC UPF, Release 2026.04.h0

Milestone	Date
First Customer Ship (FCS)	5-Nov-2026
End of Life (EoL)	5-Nov-2026
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 Ultra Cloud Core (UCC) Software Release Lifecycle Product Bulletin available on cisco.com.

New software features

There are no new software features introduced in this release.

Changes in behavior

There are no new behavior changes introduced in this release.

Resolved issues

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

Note: This software release may contain resolved bugs first identified 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 2. Resolved issues for UCC UPF, Release 2026.04.h0

Bug ID	Description
CSCwo47013	Continuous confdmgr restart seen at function " confdmgr_fsm_state_wait_p0_handler" .
CSCwv51879	Monitor subscriber trace can NOT be captured for 2nd UE session on Voice UPF.

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

Bug ID	Description
CSCww02980	DNS-Snoop Hashtable Leak.
CSCww51452	NAT port allocation failure for ICMP flow.

Open issues

There are no open issues in this specific software release.

Known issues

There are no known issues that may occur during the upgrade of the UPF image.

Compatibility

This section lists compatibility information of the Cisco UCC software products that are verified to work with this version of the UCC UPF software.

Table 3. Compatibility information for UCC UPF, Release 2026.04.h0

Product	Supported Release
ADC Plugin	2.74.gh4.2832
RCM	2026.04.0
Ultra Cloud Core SMI	2026.04.1.10
Ultra Cloud SMF and cnSGWc	2026.04.0

Supported software packages

This section provides information about the release packages associated with UCC UPF software.

Table 4. Software packages for UCC UPF, Release 2026.04.h0

Software Package	Description	Release
companion-vpc-2026.04.h0.zip.SPA.tar.gz	Contains files pertaining to VPC, including SNMP MIBs, RADIUS dictionaries, ORBEM clients, etc. These files pertain to both trusted and non-trusted build variants. The VPC companion package also includes the release signature file, a verification script, the x.509 certificate, and a README file containing information on how to use the script to validate the certificate.	2026.04.h0 (21.28.mh43.101856)
qvpc-si-2026.04.h0.bin.SPA.tar.gz	The UPF release signature package. This package contains the VPC-SI deployment software for the UPF as well as the release signature, certificate, and verification information. Files within this package are nested under a top-level folder pertaining to the corresponding StarOS build.	2026.04.h0 (21.28.mh43.101856)

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

Software Package	Description	Release
qvpc-si-2026.04.h0.qcow2.zip.SPA.tar.gz	The UPF release signature package. This package contains the VPC-SI deployment software for the UPF as well as the release signature, certificate, and verification information. Files within this package are nested under a top-level folder pertaining to the corresponding StarOS build.	2026.04.h0 (21.28.mh43.101856)
NED Package	The NETCONF NED package. This package includes all the yang files that are used for NF configuration.	ncs-6.4.15-cisco-staros-5.59.9
NSO	Note that NSO is used for the NED file creation.	6.4.15

Use this link to download the NED package associated with the software.

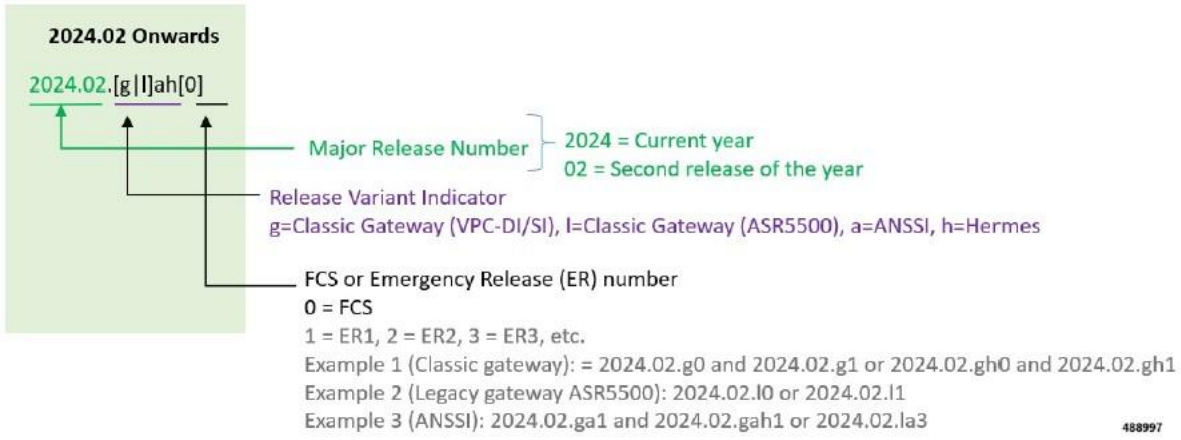
StarOS version numbering system

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 the figure 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.

Figure 1. StarOS version numbering system format



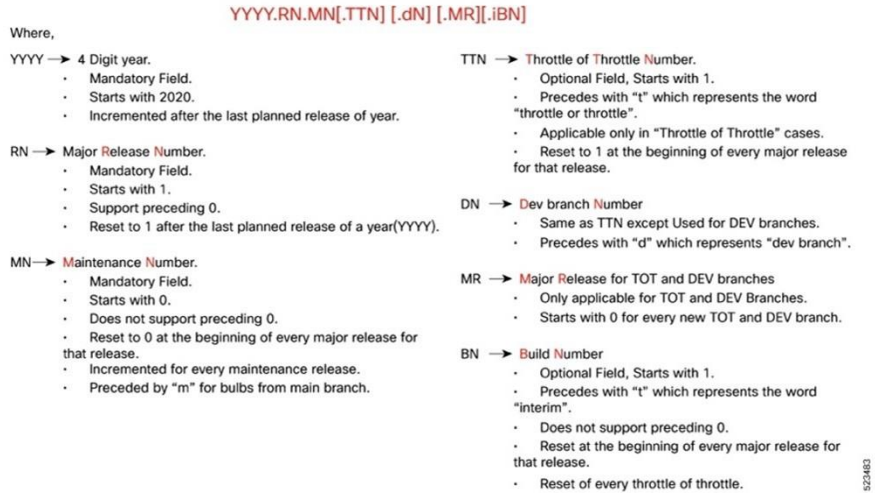
For any clarification, contact your Cisco account representative.

Cloud native product version numbering system

The show helm list command displays detailed information about the version of the cloud native product currently deployed.

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

Figure 2. Cloud native product versioning format and description



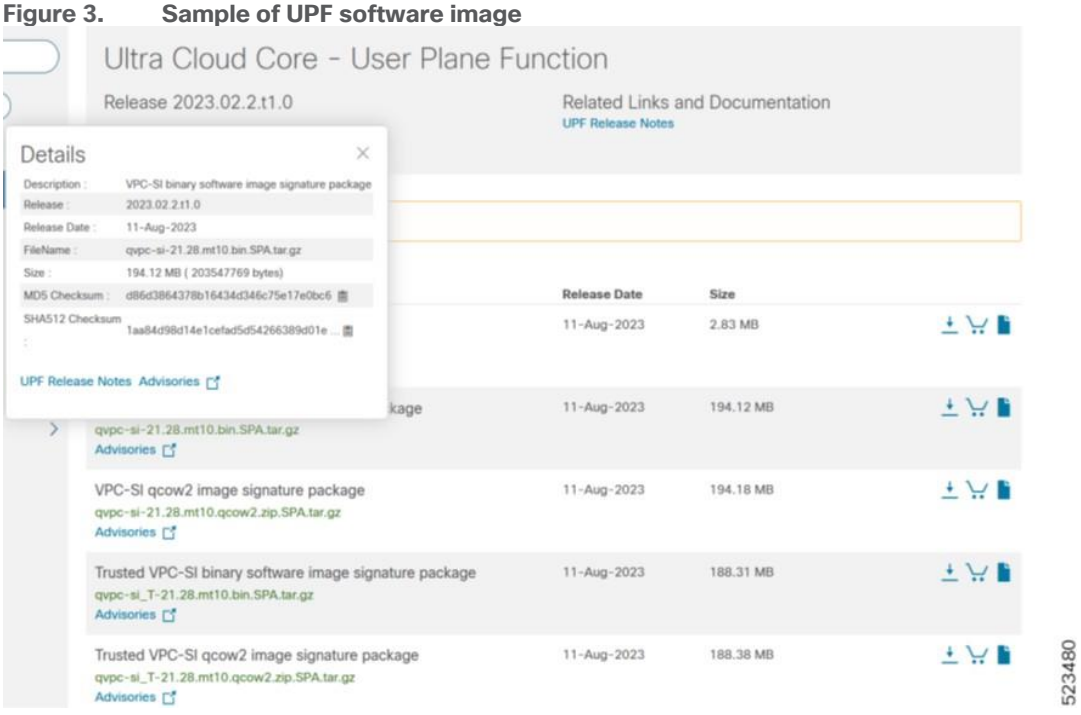
The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research software releases.

Software integrity version

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**. To find the checksum, hover the mouse pointer over the software image you have downloaded.

Figure 3. Sample of UPF software image



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.

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

To validate the information, calculate a SHA512 checksum using the information in the following table and verify that it matches the one provided on the software download page.

To calculate a SHA512 checksum on your local desktop, see this table.

Table 5. SHA512 checksum calculation commands by 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 type 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 not to 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

UPF software images are signed via x509 certificates. Please view the .README file packaged with the software for information and instructions on how to validate the certificates.

Related resources

Table 6. Related resources and additional information

Resources	Link
UPF documentation	User Plane Function
Ultra Cloud Core Subscriber Microservices Infrastructure	Subscriber Microservices Infrastructure
Ultra Cloud Core Session Management Function	Session Management Function
Ultra Cloud Core Serving Gateway Function	Ultra Cloud Core Serving Gateway Function

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

Resources	Link
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.