



# StarOS™ Software Version 21.6.b15 and Ultra Service Platform Software Version 6.2.b5 Release Notes

First Published: Nov 16, 2018

Last Updated: Nov 16, 2018

## Introduction

This Release Note identifies the resolved/fixes and unresolved/open bugs that are related to StarOS 21.6.b15 and Ultra Service Platform (USP) 6.2.b5 release.

Table 1 - Release Package Information

Package	Description	Version
StarOS packages	The StarOS package.	21.6.b15, build 70673
usp-6_2_b5-6953.iso	The USP software package containing component RPMs (bundles).  Refer to <a href="#">Table 2</a> for information on the specific bundles.	6.2.b5.6953
ultram-manager-2.0.2-1.x86_64.rpm	The Ultra M Health bundle RPM containing images for the event management functionality. This RPM is also packaged in the USP ISO.	2.0.2-1
usp_rpm_verify_utils-6.2.b5.tar	USP RPM Verification Utilities.	6.2.b5

Table 2 - Bundles Comprising the USP ISO

USP Bundle Name	Description	Version
usp-em-bundle	The Element Manager (EM) Bundle RPM containing images and metadata for the Ultra Element Manager (UEM) module.	6.2.0, Epoch 4441
usp-ugp-bundle	The Ultra Gateway Platform (UGP) Bundle RPM containing images for Ultra Packet core (VPC-DI). This bundle contains non-trusted images.	StarOS 21.6.b15, build 70673, Epoch 4963
usp-yang-bundle	The Yang Bundle RPM containing YANG data models including the VNFD and VNFR.	1.0.0, Epoch 4034
usp-uas-bundle	The Ultra Automation Services Bundle RPM containing AutoVNF, Ultra Web Services (UWS), and other automation packages.	6.2.0, Epoch 5028

## Feature and Behavior Changes

USP Bundle Name	Description	Version
usp-auto-it-bundle	The bundle containing the AutoIT packages required to deploy the UAS.	5.8.0, Epoch 4241
usp-vnfm-bundle	The VNFM Bundle RPM containing an image and a boot-up script for ESC (Elastic Service Controller).	ESC 4.0.0.104, Epoch 4035
ultram-manager-2.0.2-1-src.rpm	The Ultra M Manager bundle RPM containing images for the event management functionality. This RPM is also provided separately from the USP ISO.	2.0.2, Epoch 298

## Feature and Behavior Changes

For a complete list of feature and behavior changes associated with the corresponding 21.6.x StarOS software release, refer to the [Release Change Reference](#).

For a complete list of feature and behavior changes associated with the corresponding 6.2.x USP software release, refer to the [Release Change Reference](#).

## Related Documentation

For a complete list of available documentation related to this release, go to <https://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 installation and upgrade instructions. Refer to the existing installation documentation for specific installation and upgrade considerations.

## Ultra M Hyper-Converged Model Component Versions

HW	SW	Version
NA	StarOS	21.6.b15, build 70673
NA	ESC	4.0.0.104
NA	RH Kernel	RHEL Server 7.4
NA	OpenStack version	OSP10
UCS C220M5S	BIOS	3.1.3d
	CIMC	3.1(3h)
	MLOM	4.2(3b)
	XL710	2.4.10 [kernel driver]
Nexus 9364C (Leafs)	BIOS	05.28

## Open Bugs in this Release

HW	SW	Version
	NX-OS	7.0(3)I7(5)
	ENIC Version	2.3.0.42
	FNIC Version	1.6.0.34
Nexus 93108TC-FX	BIOS	05.28
	NX-OS	7.0(3)I7(5)

## Firmware Updates

There are no firmware upgrades required for this release.

## Open Bugs in this Release

The table below highlights the known bugs that remain open since USP 6.2.0 (non-StarOS) and StarOS 21.6.0.

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](#).

Bug ID	Headline	Product Found*
CSCvk10055	Task restart while handling delete bearer.	epdg
CSCvh67114	sessmgr restarts at function egtpc_validate_context_ack_rsp_evt	mme
CSCvh82217	sessmgr task restart during MME start Auth procedure.	mme
CSCvj40660	MME to support 10KB pkt size on Sbc interface	mme
CSCvm21245	Ghost enodeB associations after CSCvf74768	mme
CSCvi06043	aaamgr restarted multiple times on srp switch-over	pdn-gw
CSCvg95957	Single instance of Bulkstat facility restart seen on active CISCO ASR5500	pdn-gw
CSCvh67681	20% SM CPU increase when Traffic Optim is enabled with 100% heavy session in single event perf test	pdn-gw
CSCvk29371	gtpc peer-salvation keyword is missing under context level configuration	pdn-gw
CSCvk52505	Crypto map configuration on interface rejected, when maximum number of ikev1 ipsecmgr tasks reached	pdn-gw
CSCvm47811	Adding debug info to understand restart counter change from SGW causing PGW to mark sessions down	pdn-gw
CSCvm93977	Inconsistency between AAAAccServerUnreachable and AAAAccSvrUnreachable causing SNMP trap issues	pdn-gw
CSCvi06491	The default behaviour of diameter encode-supported-features has changed in 21.7	pdn-gw
CSCvm19430	NAT64 ipv6 fragment header identification field always zero	pdn-gw

## Resolved Bugs in this Release

Bug ID	Headline	Product Found*
CSCvi66788	VPC-DI incorrectly reports Standby SF when N+1 count is less	sae-gw
CSCvh64982	Planned SRP switchover followed by switchover due to BGP failure - aaamgr restarts	sae-gw
CSCvj48443	Cisco SAEGw sends incorrect ARP value after a IDFT procedure in DDN towards MME	sae-gw
CSCvi50398	core file size limited to 2048 bytes in VPC resulting in core file transfer failure	staros
CSCvh54162	[ePDG] performing iftask restart is causing SF to restart on ultraM with servicemode as epdg	staros
CSCvh68111	The beakerd process has a memory leak	staros
CSCvi65014	Restart of vpnmgr task adversely affecting the connectivity.	staros
CSCvh84131	defaut mcdma latency is 0 leading to inefficiency	staros
CSCvh99381	SDR cli output shows all Enaled/Disabled command at all times.	staros
CSCvi44228	Incorrect time format for msg-format rfc5424	staros
CSCvm73155	Unable to update module p2p after unplanned DPC migration	staros
CSCvi69775	ESC recovery is triggered with old ESC image after upgrade.	usp-uas
CSCvj04691	AutoVNF recovery post upgrade does not spawn the upgraded image	usp-uas
CSCvj04799	AutoVNF upgrade failure - rollback to secondary image does not happen	usp-uas
* Information in the "Product Found" column identifies the product in which the bug was initially identified.		

## Resolved Bugs in this Release

The following table lists the known bugs that are resolved in USP 6.2.b5 (non-StarOS) and StarOS 21.6.b15 releases.

**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](#).

Bug ID	Headline	Product Found*
CSCvj72476	sm restarts on assert at mme_abort_procedure	mme
CSCvj92869	sessmgr restart due to assertion failure at sess/mme/mme-app/app/mme_msg_utils.c	mme
CSCvn19507	IPv6 BFD - cross - sessions down after triggering EEM script on leaf	staros
CSCvn18519	StarOS DNS Client Issue with Fragmented Packets	staros
CSCvn02827	On DeMux Host reboot two additional SFs reset in the VNF	staros
CSCvn10787	Fault Management is not working for 3rd VNF	usp-uas
CSCvm98462	Stale ports left behind mapped to floating ips on activate failure	usp-uas

Operator Notes

Bug ID	Headline	Product Found*
CSCvn09365	netconf connection is out-of-sync after network disruption	usp-uas
* Information in the “Product Found” column identifies the product in which the bug was initially identified.		

## Operator Notes

### Elastic Services Controller

This version of the Cisco VPC has been validated for operation with Cisco Elastic Services Controller (ESC) version 4.0.0.104 ESC software can be downloaded here: <https://software.cisco.com/download/navigator.html>

Once on the page, navigate to the software location by selecting **Cloud and Systems Management > Service Management and Orchestration > Elastic Services Controller > Elastic Services Controller 4.0 > All Releases > 4.0.0**.

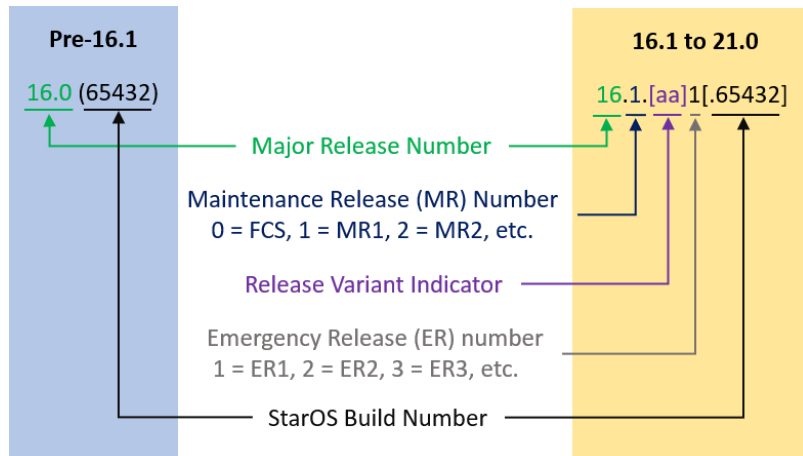
### StarOS Version Numbering System

The output of the show version command displays detailed information about the version of StarOS currently running on the ASR 5x00 or Cisco Virtualized Packet Core platform.

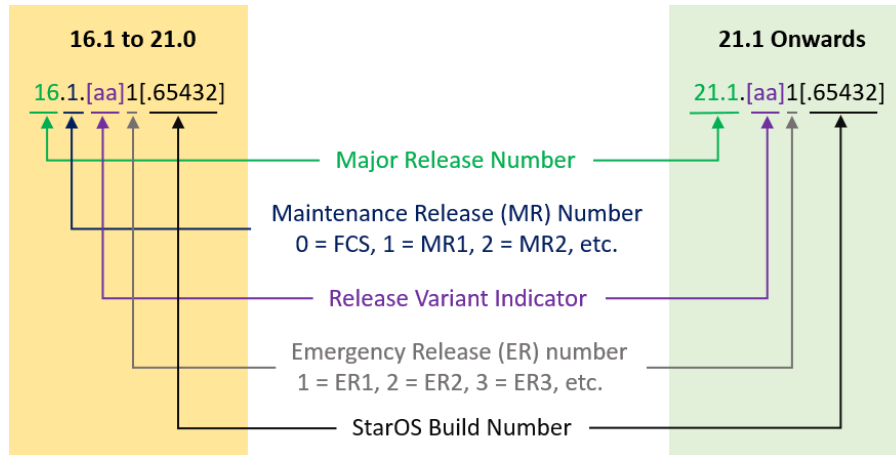
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example “16.0 (55435)”. Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build number.

From release 16.1 onwards, the output of the show version command, as well as the terminology used to describe the Build Version Number fields, has changed. Additionally, show version will display slightly different information depending on whether or not a build is suitable for deployment.

The Version Build Number for releases between 16.1 and 21.0 include a major, maintenance, and emergency release number, for example “16.1.2”.



The Version Build Number for releases 21.1 and later include a major and emergency release number, for example, “21.1.1”.



In either scenario, 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 will facilitate identifying the changes between releases when using Bug Search Tool to research software releases.

## 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*, at:

<https://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

Obtaining Documentation and Submitting a Service Request

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 are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at <https://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: <https://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)

© 2018 Cisco Systems, Inc. All rights reserved.