StarOS™ Software Version 21.6.b13 and Ultra Service Platform Software Version 6.2.b3 Release Notes

First Published: Oct 16, 2018
Last Updated: Oct 16, 2018

Introduction

This Release Note identifies the resolved/fixed and unresolved/open bugs that are related to 21.6.b13 StarOs and 6.2.b3 Ultra Service Platform (USP) Release.

Table 1 - Release Package Information

Package	Description	Version
StarOS packages	The StarOS package.	21.6.b13, build 70432
usp-6_2_b3-6576.iso	The USP software package containing component RPMs (bundles). Refer to Table 2 for information on the specific bundles.	6.2.b3.6576
ultram-manager-2.0.1-1.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.	2.0.1-1
usp_rpm_verify_utils-6.2.b3.tar	USP RPM Verification Utilities.	6.2.b3

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.b13, build 70432, Epoch 4597
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 4601

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-2.0.1-1.x86_64.rpm	The Ultra M Manager bundle RPM containing images for the event management functionality. This RPM is also provided separately from the USP ISO.	2.0.1, Epoch 282

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	6.2.b13
	StarOS	21.6.b13, build 70432
	ESC	4.0.0.104
	RH Kernel	RHEL Server 7.4
	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

	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
CSCvh59780	Sessmgr restart in egtpc event handler path	mme
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
CSCvm76444	SM crash occured due to Assertion failure on sn_gt_encode_bss_container_ie	mme
CSCvm78020	SM fail due to Assertion failure at egtpc_validate_evt	mme
CSCvk35798	Sessmgr task restart at egtpc_handle_bearer_res_cmd_req_evt	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
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
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

Bug ID	Headline	Product Found*
CSCvm87438	SM restarts at sess/egtp/egtpc/egtpc_interface.c:244 expr evt_data.evt_info.sess_info.pdn_rec	sgsn
CSCvm87099	At times HB failures lead to SF card reboot on SW (leaf) reload.	staros
CSCvm88928	Incorrect mapping of SRIOV VF to SF card SVC port in C2.1 UltraM	staros
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
CSCvi69775	ESC recovery is triggered with old ESC image after upgrade.	usp-uas
CSCvi93609	update-sw transaction remains in requested state even after it completes successfully.	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
CSCvm84117	UEM unable to maintain ha-state	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.b3 (non-StarOS) and StarOS 21.6.b13 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*
CSCvh61777	MME does not send res-TEID/eNB in RAB-set-info PS-HO 3G-4G when no data fwd	mme
CSCvk06097	High session manager memory usage observed for mme service	mme
CSCvi81579	collision of SMS inbetween the SRVCC procedure	mme
CSCvj90959	High memory usage due to caching of eNodeB on sessmgrs	mme
CSCvh32634	Sessmgr restart at gtapp_mm_fsm	sgsn

Bug ID	Headline	Product Found*
CSCvh50159	SM restart : Assertion failure at sess/egtp/egtpc/egtpc_evt_handler_func	sgsn
CSCvj30184	sessmgr assertion failure at sess/sgsn/sgsn-app/gtp_c/gtapp_db	sgsn
CSCvh03512	Task restart while handling bearer info command	sgsn
CSCvi25027	SM restart in at sess/sgsn/sgsn-app/access/access_main.c	sgsn
CSCvm34045	Few SF cards in booting state in VNFs in C2.1 deployment model	staros
CSCvm44007	[VPC-DI] SFs stuck in booting state following failed CF switchover and chassis reload.	staros
CSCvm44880	VPC-DI reload on simultaneous fault of active CF and one SF VM	staros
CSCvm58137	SF stuck in booting state - DI-Net bonding not functioning	staros
CSCvm67125	i40eVF driver upgrade	staros
CSCvm77236	SF/CF cards in Booting state on VNF deployment	staros
CSCvh97289	debug command for heartbeat should be made configurable	staros
CSCvm37182	[VPC-DI] Add configuration CLI for inter-CF heartbeat/masterd timeout duration.	staros
CSCvi51793	Update the VNFD yang file in confdmgr with port-id	usp-usf
CSCvj00859	Reboot requests in UEM are not honored.	usp-usf
* 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.**

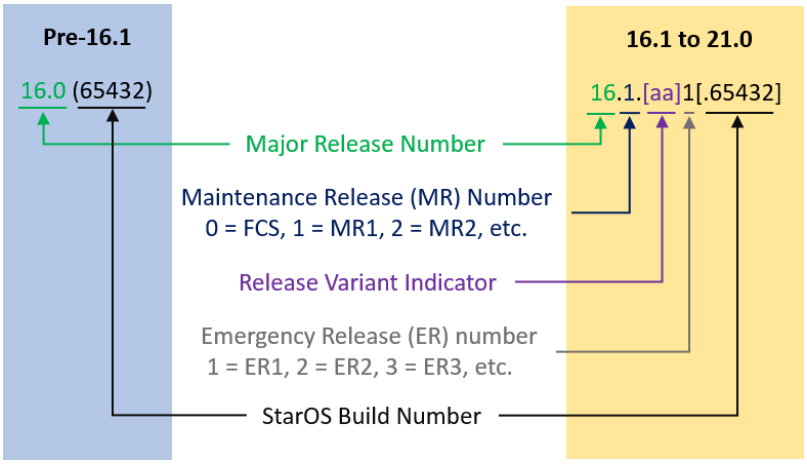
StarOS Version Numbering System

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.

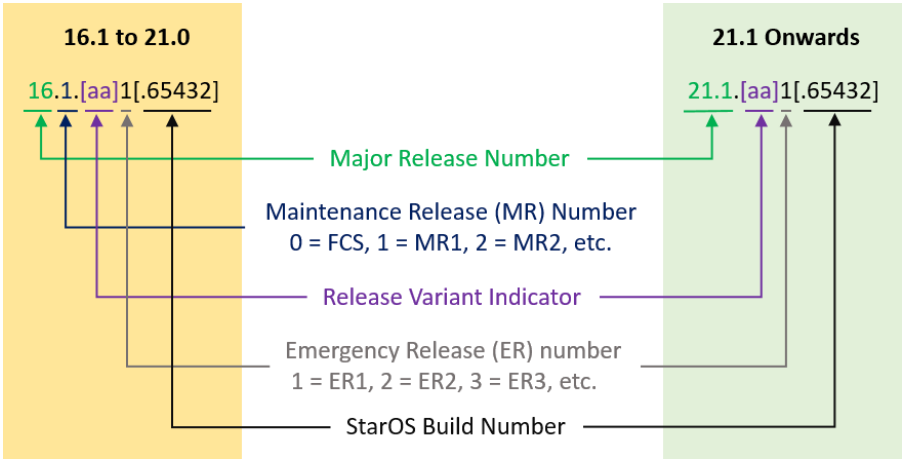
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example “16.0 (55435)”. Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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