AVAYA

Communication Server 1000

Release 7.6 Service Pack 10

Release Notes

Issue: 1.3

April 2019

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document might be incorporated in future releases.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product, while under warranty, is available through the Avaya Support Web site: http://support.avaya.com

License

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEB SITE http://support.avaya.com/LicenseInfo/ ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License type(s)

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Product that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/ThirdPartyLicense/

Preventing toll fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://support.avaya.com

Trademarks

Avaya and the Avaya logo are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions. All other trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: http://support.avaya.com

Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Support Web site: http://support.avaya.com

Contents

Revision history

Issue	Date	Reason for Reissue
1.0	26th October 2018	Initial version.
1.1	27th December 2018	Updated with a number of changes: - SMGR 8.0 hot fix is now available for Aura 8.0 support. Multiple sections were updated with info on SMGR 8.0. No change to the original SP10 content. - Introduced Appendix B with mapping for non-CSR3 / CSR3 vtrk serviceability updates.
1.2	25th March 2019	Updated with a number of changes: - Corrected titles for Tables 7-10 to indicate the correct platforms. - Removed special instructions for Jboss-Quantum SU for CSR3 platform from Table 6: Special Instructions for CSR3 Service Pack 10. - Clarified instructions in CS1000 Security Domain design changes in case of SMGR 7.1 / SMGR 8.0 section.
1.3	29th April 2019	Updated with a number of changes: - CS 1000 R7.6 is now End of Manufacturer Support for Software as per End of Sale Notice on Avaya Support Portal – updated CS1000 lifecycle notice section. - SMGR 8.0.1 hot fix is now available for Aura 8.0.1 support. Multiple sections were updated with info on SMGR 8.0.1. No change to the original SP10 content. - Introduced Known SMGR related issues section.

Introduction

This Release Note provides information about installation, downloads and the supported documentation of Communication Server 1000 7.6 GA Release and Service Pack 10. This Release Note also contains important information about new features added to Release 7.6, fixes included in Service Pack 10, known issues, and possible workarounds in this Release.

The offer definition contains other important information about the release. The offer definition is located on Avaya's **Sales Portal** site under the **Products and Solutions / CS1000 / pre sales technical**.

https://sales.avaya.com/en/pss/uc-communication-server-1000?view=collateral

A complete list of PI patches available for R7.6 can be found in ESPL.

The online Compatibility Matrix is recommended for Communication Server 1000 Release 7.6 interworking with the Avaya Aura® portfolio in particular. This can be accessed via the Avaya Support Portal at:

https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml

PLEASE NOTE that the latest interop information for Service Pack 10 is included in the "Notes section" under Communication Server Release 7.6.7 (i.e. Service Pack 7.)

What's new in CS1000 Release 7.6 Service Pack 10

Please ensure you review the section on Known Limitations and Operational Assistance in this document before proceeding to deploy Service Pack 10.

Linux Kernel upgrade

"PAE" (Physical Address Extension) is a special mechanism in some CPUs that allows addressing more than 3GB on 32-bit platforms. If a user needs to use more than 3GB of RAM on a Linux based server with arch i386 it will be required to use a kernel with PAE support.

PAE mode is already supported by the following CS1000 processors: CPDC, COTS 2 servers and all Common Servers.

Pentium M that is used on CPPM does not support the PAE mode so kernels with PAE support will not work on CPPM.

The kernel update in Service Pack 10 also allows installation of PAE kernels on CPMG, but it is still impossible to address 4GB of RAM, even if 4 GB are installed. This is related to CPMG architecture, and it is a current platform limitation.

Kernel SUs can be installed in the following way on different platforms with CS1000 Linux Base.

Platform	Kernel SU
CPPM with CS1000 Linux Base	kernel-2.6.18-434.el5.i686.000
CPMG, CPDC, COTS or Common Server R1/R2 with CS1000 Linux Base	kernel-PAE-2.6.18-434.el5.i686.000
CPDC, COTS or Common Server R1/R2 with AMS x64 load installed	kernel-2.6.18-434.el5.x86_64.000
Common Server R3 with CS1000 Linux Base	kernel-2.6.32-754.3.5.el6.i686.000
Common Server R3 with AMS x64 load installed	kernel-2.6.32-754.3.5.el6.i686.000

Each kernel and kernel-PAE serviceability update has some requirements. The main requirement is related to installation of the required cs1000-linuxbase SU prior to installation of the kernel/kernel-PAE SU. This ensures the appropriate kernel file is used depending on the processor type. If Service Pack 10 for the ordinary Linux Base or Service Pack 4 for amsx64 is being installed, a user should first install a proper cs1000-linuxbase/cs1000-linuxbase-amsx64 SU, which is required by the Service Pack, prior to **spload**. The appropriate kernel file will then be selected automatically depending on processor type.

AMS upgrade

Service Pack 10 for CS 1000 R7.6 is accompanied by Service Pack 4 for AMS 7.6 for CS 1000. The update includes a number of security fixes for the base system and some patching related enhancements. It does not introduce a new AMS build.

The following table provides a summary on AMS 7.6 builds across Service Packs for AMS 7.6 for CS1000.

amsx64 load version	amsx64 load, 7.65.16.26	amsx64 load for CSR3, 7.65.19
amsx64 GA	7.6.0.807	7.6.0.1008
amsx64 SP1	7.6.0.999	-
amsx64 SP2	7.6.0.1008	-
amsx64 SP3	7.6.0.1008	7.6.0.1008
amsx64 SP4	7.6.0.1008	7.6.0.1008

spstat command can be used by admin2 user to check what Service Pack is currently loaded.

cat /etc/mas.properties can be used by root user to check what AMS build is currently in-service.

Note that AMS 7.0 is end of software support as per PSN 3499 (Communication Server 1000 lifecycle bulletin) on the Support Portal. Customers are recommended to upgrade to AMS 7.6 to ensure software support is available.

Note that R7.6 SP8 and newer Service Packs are not tested along with AMS 7.0, and there are known issues with access to AMS 7.0 EM when Service Pack 9 / Service Pack 10 is in-service. Please check Known Limitations and Operational Assistance section for more info.

Security issues addressed with SP10

VxWorks based CS1000 targets

Patches were prepared to deny use of RC4 cipher suites and weak MAC algorithms by the SSH client/server on VxWorks based Call Servers, Media Gateways and Media Cards (MC32S only.)

Linux based CS1000 targets

Internal ticket	Update packages / comments	Associated CVEs
	Platform: CS1000 Linux Base	
CS1000-7723	kernel / kernel-PAE, glibc, nscd	CVE-2017-1000364, CVE-2017-1000366, CVE-2017-1000379, CVE-2017-7895
CS1000-7724	Required to limit the cipher suites list used by several CS1000 applications	-
CS1000-7756	jdk	CVE-2017-10053, CVE-2017-10102, CVE-2017-10108, CVE-2017-10115, CVE-2017-10116, CVE-2017-10135, CVE-2017-10198, CVE-2017-10243

Internal ticket	Update packages / comments	Associated CVEs
CS1000-7815	kernel	CVE-2017-1000253
CS1000-7876	jdk	CVE-2017-10281, CVE-2017-10295, CVE-2017-10345, CVE-2017-10355, CVE-2017-10356, CVE-2018-2579, CVE-2018-2588, CVE-2018-2599, CVE-2018-2603, CVE-2018-2618, CVE-2018-2629, CVE-2018-2633, CVE-2018-2637, CVE-2018-2657, CVE-2018-2663, CVE-2018-2678, CVE-2018-2783, CVE-2018-2794, CVE-2018-2795, CVE-2018-2797, CVE-2018-2798, CVE-2018-2800, CVE-2018-2815
CS1000-7907	kernel / kernel-PAE	CVE-2018-8897
CS1000-7918	curl	CVE-2014-0138, CVE-2014-3707
CS1000-7944	kernel / kernel-PAE	CVE-2017-14106
CS1000-7945	jdk	CVE-2018-2938, CVE-2018-2952
CS1000-7978	cppmUtil - rebuild CS1000 specific kernel modules with retpoline support	-
Platform: CS1000 amsx64 load for non-CSR3 servers		
CS1000-7793	kernel, glibc, nscd	CVE-2017-1000364, CVE-2017-1000366, CVE-2017-1000379, CVE-2017-7895
CS1000-7816	kernel	CVE-2017-1000253
CS1000-7908	kernel	CVE-2018-8897
CS1000-7909	kernel	CVE-2017-5715, CVE-2017-5753, CVE-2017-5754
CS1000-7951	sudo	CVE-2017-1000367, CVE-2017-1000368
CS1000-7952	kernel	CVE-2018-3639, CVE-2017-14106
CS1000-7979	cppmUtil - rebuild CS1000 specific kernel modules with retpoline support	-

Internal ticket	**Update packages / comments**	**Associated CVEs**
CS1000-8000	kernel	CVE-2018-3620, CVE-2018-3646
Platform: CS1000 Linux Base for CSR3		
CS1000-7689	bash	CVE-2016-7543, CVE-2016-9401
CS1000-7691	expat	CVE-2016-0718
CS1000-7745 CS1000-7874	Required to limit the cipher suites list used by several CS1000 applications	-
CS1000-7757	jre	CVE-2017-10053, CVE-2017-10102, CVE-2017-10108, CVE-2017-10115, CVE-2017-10116, CVE-2017-10135, CVE-2017-10198, CVE-2017-10243
CS1000-7794	kernel, glibc, nscd	CVE-2017-1000364, CVE-2017-1000366, CVE-2017-1000379, CVE-2017-7895
CS1000-7801	coreutils	CVE-2017-2616
CS1000-7805	libxml2	CVE-2016-1762, CVE-2016-1833, CVE-2016-1834, CVE-2016-1835, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, CVE-2016-1839, CVE-2016-1840, CVE-2016-3705, CVE-2016-3627, CVE-2016-4447, CVE-2016-4448, CVE-2016-4449
CS1000-7817	kernel	CVE-2017-1000253
CS1000-7863	kernel	CVE-2017-5715, CVE-2017-5753, CVE-2017-5754, CVE-2017-7645, CVE-2017-14106, CVE-2017-13166, CVE-2017-18017
CS1000-7879	jre	CVE-2017-10281, CVE-2017-10295, CVE-2017-10345, CVE-2017-10355, CVE-2017-10356, CVE-2018-2579, CVE-2018-2588, CVE-2018-2599, CVE-2018-2603, CVE-2018-2618, CVE-2018-2629, CVE-2018-2633, CVE-2018-2637, CVE-2018-2657, CVE-2018-2663, CVE-2018-2678, CVE-2018-2783, CVE-2018-2794, CVE-2018-2795, CVE-2018-2797, CVE-2018-2798, CVE-2018-2800, CVE-2018-2815
CS1000-7903	sudo	CVE-2016-7032, CVE-2016-7076, CVE-2017-1000367, CVE-2017-1000368
CS1000-7920	kernel	CVE-2018-3639
CS1000-7945	jre	CVE-2018-2938, CVE-2018-2952

Internal ticket	Update packages / comments	Associated CVEs
CS1000-7962	kernel	CVE-2012-6701, CVE-2015-8830, CVE-2016-8650, CVE-2017-2671, CVE-2017-6001, CVE-2017-7308, CVE-2017-7616, CVE-2017-7889, CVE-2017-8890, CVE-2017-9077, CVE-2017-18203, CVE-2018-3620, CVE-2018-3639, CVE-2018-3646, CVE-2018-3665, CVE-2018-3693, CVE-2018-5390, CVE-2018-10675, CVE-2018-10872
CS1000-7965	glibc	CVE-2017-15670, CVE-2017-15804
CS1000-7967	ntp	CVE-2015-7979, CVE-2016-1550, CVE-2016-2518, CVE-2016-1547, CVE-2016-1548, CVE-2016-7426, CVE-2016-7429, CVE-2016-7433, CVE-2016-9310, CVE-2016-9311, CVE-2017-6462, CVE-2017-6463, CVE-2017-6464
CS1000-7971	openssh	CVE-2016-6210
Platform: CS1000 amsx64 load for CSR3		
CS1000-7690	bash	CVE-2016-7543, CVE-2016-9401
CS1000-7692	expat	CVE-2016-0718
CS1000-7795	kernel, glibc, nscd	CVE-2017-1000364, CVE-2017-1000366, CVE-2017-1000379, CVE-2017-7895
CS1000-7802	coreutils	CVE-2017-2616
CS1000-7806	libxml2	CVE-2016-1762, CVE-2016-1833, CVE-2016-1834, CVE-2016-1835, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, CVE-2016-1839, CVE-2016-1840, CVE-2016-3705, CVE-2016-3627, CVE-2016-4447, CVE-2016-4448, CVE-2016-4449
CS1000-7818	kernel	CVE-2017-1000253
CS1000-7864	kernel	CVE-2017-5715, CVE-2017-5753, CVE-2017-5754, CVE-2017-7645, CVE-2017-14106, CVE-2017-13166, CVE-2017-18017
CS1000-7904	sudo	CVE-2016-7032, CVE-2016-7076, CVE-2017-1000367, CVE-2017-1000368
CS1000-7921	kernel	CVE-2018-3639
CS1000-7963	kernel	CVE-2012-6701, CVE-2015-8830, CVE-2016-8650, CVE-2017-2671, CVE-2017-6001, CVE-2017-7308, CVE-2017-7616, CVE-2017-7889, CVE-2017-8890, CVE-2017-9077, CVE-2017-18203, CVE-2018-3620, CVE-2018-3639, CVE-2018-3646, CVE-2018-3665, CVE-2018-3693, CVE-2018-5390, CVE-2018-10675, CVE-2018-10872

Internal ticket	Update packages / comments	Associated CVEs
CS1000-7966	glibc	CVE-2017-15670, CVE-2017-15804
CS1000-7968	ntp	CVE-2015-7979, CVE-2016-1550, CVE-2016-2518, CVE-2016-1547, CVE-2016-1548, CVE-2016-7426, CVE-2016-7429, CVE-2016-7433, CVE-2016-9310, CVE-2016-9311, CVE-2017-6462, CVE-2017-6463, CVE-2017-6464
CS1000-7972	openssh	CVE-2016-6210

Speculative execution issues

Service Pack 10 delivers fixes for several CVEs related to the speculative execution flaws.

- CVE-2017-5715 – Spectre, V2 (BTI: Branch Target Injection)
- CVE-2017-5753 – Spectre, V1 (BCB: Bounds Check Bypass)
- CVE-2017-5754 – Spectre, V3 / Meltdown (RDCL: Rogue Data Cache Load)
- CVE-2018-3620 – L1TF: L1 terminal fault
- CVE-2018-3639 – Spectre, V4 (SSB: Speculative Store Bypass)
- CVE-2018-3640 – Spectre, V3a (RSRE: Rogue System Register Read)

These fixes only cover products for Common Server R3: CS1000 Linux Base for CSR3 and CS1000 amsx64 load for CSR3.

Non-CSR3 CS1000 Linux based platforms can still be affected. Please check **PSN 5158** for more info and updates on availability of new fixes.

CS1000 Software MUST READ

General notes

- CPDC and CPMG cards now require 4GB of RAM. The accessible amount of DRAM for CPMG is 3 GB.
- CPPM and COTS1 servers are only capable of having 2GB of memory. Software Deployment model restrictions have been put in place in the Non-Dedicated deployment model. These platforms no longer support running all applications simultaneously. Please see the Release 7.6 Planning and Engineering guides for the latest guidance on system capacities.
- SSH/Rlogin/Telnet connection using IPv6 is not supported in CS1000. For SSH/Rlogin/Telnet/Web access, only IPV4 addresses are supported.
- The one-X Communicator for CS 1000 has been End of Sales since 4th March 2013. It is recommended for the small number of customers using one-X Communicator on the CS 1000 to consider migrating those users to IP Softphone 2050 or to one-X Communicator natively on Collab Pack 1.1 for CS 1000.
- Please consider interoperability implications for other Avaya applications / DevConnect applications / SIP trunking prior to any upgrade – there is information in Appendix A referencing the online Compatibility Matrix which is available on the Avaya Support Portal.

CS1000 lifecycle notice

CS 1000 R7.6 is now End of Manufacturer Support for Software as per End of Sale Notice on Avaya Support Portal. That does mean that there is **no more Tier IV / design support available for CS 1000 R7.6 software and no new bug fix**, as per Avaya Product Lifecycle Policy document.

It is expected that one final Service Pack 11 will be delivered in September 2019 time (dates subject to change); however no further Tier IV / design support will be available post April 9th 2019. That final SP11 will bundle those software updates delivered between R7.6 SP10 (October 2018) and End of Manufacturer Support in April 2019.

Supported Upgrades

For the Communication Server 1000 7.6 Release and Service Pack 10, upgrade paths from the following releases have been validated: 3.0, 4.0, 4.5, 5.0, 5.5, 6.0, 7.0, 7.5, and Meridian 1 Release 25.40B.

Special instructions / Points to remember before a fresh installation or an upgrade

Step by Step instructions for installing or upgrading your system can be found in the customer documentation.

Prior to upgrade/migration, please ensure that the latest Deplist/SP is installed for the **current release** of software on your system.

You can find the latest DEP list for your system on the Avaya ESPL Web site https://espl.avaya.com/espl/

Pre-Upgrade SUs files

ESPL hyperlink	Pre-Upgrade Description	File Name	Size (Mb)	MD5 Checksum
Release 6.0 Pre-Upgrade SU & Service Pack				
Linuxbase SU	Linuxbase SU	nortel-cs1000-linuxbase-6.00.18.65-08.i386.001.ntl	0.78	0089D1C8F1A11472F545B9BB4D1B6FF7
Linux SP	Linux SP	Service_Pack_Linux_6.00_18_20130315.zip	335	EB22C6566DF930ABCDE1321E614E0EE1

ESPL hyperlink	Pre-Upgrade Description	File Name	Size (Mb)	MD5 Checksum
Release 7.0 Pre-Upgrade SU				
Linuxbase SU	Linuxbase SU	nortel-cs1000-linuxbase-7.00.20.10-10.i386.000.ntl	1.25	5383E5E5B115E8DA0F512DCF84BFE41C
Release 7.5 Pre-Upgrade SU & Service Pack				
Linuxbase SU	Linuxbase SU	cs1000-linuxbase-7.50.17.16-21.i386.000.ntl	1.29	AF810AADF2A61D10FE2360E4C3C68B41
Linux SP	Linux SP	SP_7.5_24.zip	1018	816815757D3250A07CFF73DEDE383A0C

Common Server R3 (CSR3) support

The Common Server R3 program is a technology refresh driven by the lifecycle of the Intel processor. The current Common Server 2 (306202 – HP DL360 G8) went End of Sale in June 2016. It was replaced by Common Server R3 (383438 – HP DL360 G9).

The new HP DL360 G9 requires different versions of the Linux OS as well as different application images. The updated Linux ISO images contain "el6" in the file name. The old images will not install on the new Common Server R3. Likewise, the new images are not correct for the older server.

The Avaya Software order codes will remain the same. Across the introduction period, Avaya will ship both versions of the software DVDs together in an envelope. User will select which DVD to install based on the server type. The DVD's are labeled as being for either HP DL360 G8 or HP DL360 G9.

- NTE90768 - CS 1000 Applications on COTS Server DVD
- NTE90769 - CS 1000 Linux OS on COTS Server DVD
- NTE90770 - CS1K AMS R7.6 SW DVD

Deployment Manager now supports two types of targets – non-CSR3 and CSR3 ones. It is allowed to upload two different ISO images at the same time: one for the current CS1000 Linux Base release 7.6 (a file with name cs1000-linuxbase-x.xx.xx.xx.iso or nortel-cs1000-linuxbase-x.xx.xx.xx.iso) and one for the updated CS1000 Linux Base for CSR3 (a file with name cs1000-linuxbase-el6-x.xx.xx.xx.iso.)

MCM lifecycle – changing to EoMS for software with SP8

The Avaya Multimedia Convergence Manager (MCM) component was used for Communication Server 1000 interworking with Microsoft LCS 2005 / OCS 2007. Most customers have now migrated to Microsoft OCS 2010 or later, where the Avaya MCM component is no longer applicable for such interworking. MCM component moved to End of Manufacturing Support for software in CS1000 R7.6 Service Pack 8 in Calendar Year 2016. Please refer to **PSN 3499**.

PLUGIN 227 moved to PLUGIN 400

From SP8 onwards PLUGIN 227 has been moved to PLUGIN 400. PLUGIN 227 required PKG 366 or PKG 409 to be enabled as a pre-requisite. Now that the PLUGIN has moved to PLUGIN 400, it is available to all systems, even those without PKG 366 or PKG 409. This change was introduced as part of patch MPLR33675 (PLUGIN 227: Skip zeroes insertion when TRDN > DN length.)

Please be aware that if a CS1000 is upgraded from a previous software release to CS1000 7.6 Service Pack 8 or later, or the Service Pack is updated on an existing CS1000 R7.6 that previously had PLUGIN 227 enabled, then after the upgrade, PLUGIN 227 will be automatically disabled. PLUGIN 400 will need to be enabled using the pdt> **ple 400** command.

Enhancement introduced in Service Pack 7: Linux shutdown command

Service Pack 7 introduced a Linux **shutdown** command which is now accessible to the “**admin2**” user. The shutdown command will gracefully shut down the Linux operating system. All open files on the drive will be closed and drive heads will be parked. The **shutdown** command will work on all CS1000 Linux based processor packs and servers.

In absence of such a graceful shutdown, open files could be left in a partially written condition which in turn can result in unexpected server behavior on subsequent power-up. Typically this would be log files which can be cleaned up on next start up. There is a small chance of leaving other files open that may be damaged in an unplanned power outage.

Avaya **recommends** that in a planned pack or server shutdown, to use the Linux graceful **shutdown** command as a normal procedure.

Please note that physical access will be required to reboot the pack or server after using the **shutdown** command. The pack or server will not automatically restart due to watchdog timeout function. **The command should be used with caution as a result.**

Installing the Service Pack

Please ensure you review the section on Known Limitations and Operational Assistance in this document before proceeding to deploy Service Pack 10. Note that a System Manager hot fix is required in case of Avaya Aura® System Manager 6.3.22, Avaya Aura® System Manager 7.1.3, Avaya Aura® System Manager 8.0 and Avaya Aura® System Manager 8.0.1.

If you upgrade the system from Service Pack 4 or an earlier version, please follow the instructions mentioned in the section Before You Begin. Upgrading from Service Pack 5 or later, please skip this section.

Before You Begin

If you have System Manager deploy SMGR 6.3.22, SMGR 7.1.3, SMGR 8.0 or SMGR 8.0.1 load.

SMGR 6.3.22

The installation files can be downloaded from a following page.

https://support.avaya.com/downloads/download-details.action?contentId=C20188271954441210_6&productId=P0541

For more information refer to System Manager 6.3.22 Release Notes.

https://downloads.avaya.com/css/P8/documents/101051867

A hot fix is required for SMGR 6.3.22 to work with CS1000 R7.6. The download link can be found in the following table.

ESPL Service Pack 10 file listing & Avaya Support 7.6 Software Images

SMGR 7.1.3

The installation files can be downloaded from a following page.

https://support.avaya.com/downloads/download-details.action?contentId=C2018571719433300_3&productId=P0541

For more information refer to Avaya Aura 7.1 Release Notes.

https://downloads.avaya.com/css/P8/documents/101038598

A hot fix is required for SMGR 7.1.3 to work with CS1000 R7.6. The download link can be found in the following table.

ESPL Service Pack 10 file listing & Avaya Support 7.6 Software Images

SMGR 8.0

The installation files can be downloaded from a following page.

https://support.avaya.com/downloads/download-details.action?contentId=C2018791919527600_4&productId=P0541

For more information refer to Avaya Aura 8.0 Release Notes.

https://downloads.avaya.com/css/P8/documents/101050749

A hot fix is required for SMGR 8.0 to work with CS1000 R7.6. The download link can be found in the following table.

ESPL Service Pack 10 file listing & Avaya Support 7.6 Software Images

SMGR 8.0.1

The installation files can be downloaded from a following page.

https://support.avaya.com/downloads/download-details.action?contentId=C201812101442592100_6&productId=P0541

For more information refer to Avaya Aura 8.0.1 Release Notes.

https://downloads.avaya.com/css/P8/documents/101050749

A hot fix is required for SMGR 8.0.1 to work with CS1000 R7.6. The download link can be found in the following table.

ESPL Service Pack 10 file listing & Avaya Support 7.6 Software Images

Please review the following customer document: NN43001-407 CS1000_Patching_Fundamentals_7_6. This document contains critical information and procedures for installing the Service Pack on the various platforms:

http://support.avaya.com/css/P8/documents/100170376

You must install all elements of CS1000 7.6 Service Pack 10 on CS1000 7.6 software load.

For customers with all system elements on Release 7.6:

In some networks it is critical to have all the elements' certificates signed with SHA256. In this case, the re-installation of the Primary UCM (standalone) server is required, since its Default certificate can only be generated on installation. Following this, Service Pack 10 must be applied before configuring the server as Primary. Finally, re-join all the elements to the Security Domain. Also, please note that when the backup/restore procedure takes place, it backs up the certificates, so restoring backup (with SHA1) on the SHA256 server will roll back the server to SHA1.

However, in two scenarios, upgrading the Primary UCM server to provide SHA256 signatures may be undesirable:

- If it is not important what Signature Algorithm to use for the Default certificate on Primary UCM server
- If re-installation of Primary UCM server is unacceptable

When either applies, the server SHA256 update application is fully transparent and does not require any special handling with regard to x509 certificates – just follow the installation instructions. In this case, the Primary will still use the SHA1 Default certificate, though elements requesting a SHA 256 certificate will get SHA256-signed certificates after re-joining the Security Domain.

For customers with complex mixed releases (7.5, 7.0 or lower):

Before installing Service Pack 10 on Primary UCM server pay attention to the following:

After installing Service Pack 10 on Primary UCM server all newly created Default, WebSSL, DTLS and SIP TLS certificates are signed with SHA256 algorithm. This will cause problems if any **additional** members are joined, that use older releases (7.5 or prior). Note that any members already joined prior to Service Pack 10 deployment on Primary UCM will **not** be affected.

To join older release members after Service Pack 10 deployment, SHA1 certificate generation is required. For this the Linux command **defaultSAconfig** should be executed on Primary UCM server under user admin2. This allows to switch back to SHA1. This command should be invoked on Primary UCM server after service Pack 10 deployment. After this, all newly created Default, WebSSL, DTLS and SIP TLS certificates are signed with SHA1 algorithm.

With the help of the same **defaultSAconfig** command the Signature Algorithm could be switched to SHA256 again.

Upgrade the system to have 800 patch handles

Service Pack 6 introduced support for 800 patch handles (and also increased the amount of patch memory allocated).

When updating from Service Pack 5 and earlier, to Service Pack 6 or later, the steps below MUST be performed to increase to 800 patch handles. When updating from Service Pack 6 or later the below should not be necessary; however it is advised to check and confirm that 800 patch handles are indeed available, before deciding how to proceed.

To check:

- type **sl1Version** command in pdt and check Base is x210765q
  Example:
  pdt> **sl1Version**
  The output will be as follows:
  SL1: Date = Nov 1 2013, Time = 14:51:37, **Base = x210765q**
  x210765**q** confirms that 800 patch handles **are** supported; an output of x210765**p** would mean that the 800 patch handle activity has **not** yet been executed on the system.

For the CPPL platform, the new functionality is included within Service Pack 6 or later. The Service Pack should be installed, and that completes the process for the CPPL Platform to increase the patch handle limit to 800 (process below for CPPM and CPP4 is NOT required).

For CPPM and CPP4 platforms please follow the instructions below.

WARNING: SYSLOAD will automatically occur upon the successful completion of the following steps.

On single CPU machines please perform:

1. A. Download CS image 765q_cpm.zip archive and put it to "/u/pub" directory for CPPM machine.
   B. Download CS image 765q_pp4.zip archive and put it to "/u/pub" directory for CPP4 machine.
2. Install (**pload** + **pins**) MPLR33339 as an individual patch first as a pre-requisite.
3. Load the overlay 143 and type the command “**UPDATEPATCHLIMIT**”, enter “y”.

For High Availability systems please do:

1. A. Download CS image 765q_cpm.zip archive and put it to "/u/pub" directory for CPPM machine.
   B. Download CS image 765q_pp4.zip archive and put it to "/u/pub" directory for CPP4 machine.
2. Install (**pload** + **pins**) MPLR33339 as an individual patch first as a pre-requisite.
3. Perform **SPLIT** command from Overlay 135 on Active Core.
4. Install new build on former Standby Core using **UPDATEPATCHLIMIT** command from Overlay 143.
5. Perform **CUTOVR** command from Overlay 135 on Active Core.
6. Install new build on former Active Core using **UPDATEPATCHLIMIT** command from Overlay 143.
7. Perform **JOIN** command from Overlay 135 on Standby Core.

NOTE: the procedure **UPDATEPATCHLIMIT** ONLY updates the patch handle limit and available patch memory. It does NOT install the latest Call Server patches. LD 143 **mdp refresh** is still required to be done as a later step, to install SP Call Server patches, as per previous Service Packs.

NOTE: it is mandatory to do UPDATEPATCHLIMIT before installing Service Pack 6 or a newer one on the Call Server. If not, then the site is at risk of running out of patch memory, and may find that not all patches in the Service Pack will install.

To confirm that the **UPDATEPATCHLIMIT** has been completed successfully:

- type **sl1Version** command in pdt and check Base is x210765q
  Example:
  pdt> **sl1Version**
  The output will be as follows:
  SL1: Date = Nov 1 2013, Time = 14:51:37, **Base = x210765q**
- please enter the command **STAT CPU** in LD 135 and check Total amount of Protected Heap memory is about 20 megabytes
  Example:

```
Protected Heap (bytes)
----------------------
alloc   2304648
 free   18666872
total   20971520
```

Call Server DepList Installation Special Instructions

Several Call Server patches have special instructions. Please refer to Table 2 for details.

Linux Service Pack Installation Special Instructions

All SUs and patches noted in this section can be found on download pages for appropriate Service Pack bundles or inside the bundles. Please check Production Linux / Linux_EL6 / AMS_X64 Service Packs page in ESPL.

System Upgrade instructions for non-CSR3 systems:

The Service Pack 10 installation sequence for **Primary** Linux server load excluding CSR3 platform **after** upgrade/migration to 7.65.16:

- Install and configure the base system
- Install cs1000-**linuxbase**-x.xx.xx.xx-xx

- Install cs1000-**Jboss-Quantum**-x.xx.xx.xx-xx
- Install cs1000-**patchWeb**-x.xx.xx.xx-xx
- Install cs1000-**dmWeb**-x.xx.xx.xx-xx
- Install avaya-cs1000-**cnd**-x.x.xx-x
- Install **jdk** update
- Perform security configuration and applications deployment
- Install the Service Pack

The Service Pack 10 installation sequence for **Member** Linux servers excluding CSR3 platform **after** upgrade/migration to 7.65.16 load (**using Primary Patch and Deployment Managers**):

- Install and configure the base system
- Install cs1000-**linuxbase**-x.xx.xx.xx-xx
- Install cs1000-**Jboss-Quantum**-x.xx.xx.xx-xx
- Install avaya-cs1000-**cnd**-x.x.xx-x
- Install **jdk** update
- Join the member server to the security domain
- Perform applications deployment
- Install the Service Pack

The Service Pack 10 installation sequence for **Member** Linux servers excluding CSR3 platform **after** upgrade/migration to 7.65.16 load (**using Local Patch and Deployment Managers**):

- Install and configure the base system
- Install cs1000-**linuxbase**-x.xx.xx.xx-xx
- Install cs1000-**Jboss-Quantum**-x.xx.xx.xx-xx
- Install cs1000-**patchWeb**-x.xx.xx.xx-xx
- Install cs1000-**dmWeb**-x.xx.xx.xx-xx
- Install avaya-cs1000-**cnd**-x.x.xx-x
- Install **jdk** update
- Perform applications deployment
- Install the Service Pack

NOTE: Ensure that avaya-cs1000-cnd-x.x.xx-x, cs1000-Jboss-Quantum-x.xx.xx.xx-xx and jdk updates are in-service before configuring and joining member or backup server to security domain.

System Upgrade instructions for CSR3 systems:

The Service Pack 10 installation sequence for **Primary** Linux server on CSR3 **after** upgrade/migration to 7.65.19 load:

- Install and configure the base system
- Install cs1000-**linuxbase**-el6-x.xx.xx.xx-xx
- Install cs1000-**Jboss-Quantum**-el6-x.xx.xx.xx-xx
- Install **jre** update
- Install **MPLR33773**
- Perform security configuration and applications deployment
- Install the Service Pack

The Service Pack 10 installation sequence for **Member** Linux servers on CSR3 **after** upgrade/migration to 7.65.19 load (**using Primary Patch and Deployment Managers**):

- Install and configure the base system
- Install cs1000-**linuxbase**-el6-x.xx.xx.xx-xx
- Install cs1000-**Jboss-Quantum**-el6-x.xx.xx.xx-xx
- Install **jre** update

- Install **MPLR33773**
- Join the member server in the security domain
- Perform applications deployment
- Install the Service Pack

The Service Pack 10 installation sequence for **Member** Linux servers on CSR3 **after** upgrade/migration to 7.65.19 load (**using Local Patch and Deployment Managers**):

- Install and configure the base system
- Install cs1000-**linuxbase**-el6-x.xx.xx.xx-xx
- Install cs1000-**Jboss-Quantum**-el6-x.xx.xx.xx-xx
- Install **jre** update
- Install **MPLR33773**
- Perform applications deployment
- Install the Service Pack

(If non-SMGR Patch Manager is used for Service Pack installation: all previously loaded Service Packs, Deplists, Patches and Loadwares will be deleted to save disk space before uploading a new Service Pack/Deplist)

NOTE: Ensure that cs1000-Jboss-Quantum-x.xx.xx.xx-xx, jre updates and MPLR33773 are in-service before configuring and joining member or backup server to security domain.

After installing Service Pack 10:

1. Login to Element Manager
2. Go to IP Network – Nodes and save and synchronize every Node, which has IP Media Services enabled.

   If High Scalability system with IP Tones feature is deployed login to Element Manager:
3. Go to IP Network – Nodes – Node Details – IP Media Services and manually set Local Media Server Role to “SIP Media Gateway”.

Instructions for existing Non-CSR3 CS1000 Release 7.6 System (i.e. running an older Service Pack version)

In general, if the Service Pack contains the following SUs and if they have changed, they will be available on ESPL as standalone files. They must be installed individually first via CLI, **before** installing the Service Pack

The Service Pack 10 installation sequence for a Primary UCM server:

- Install cs1000-**linuxbase**-x.xx.xx.xx-xx
- Install cs1000-**Jboss-Quantum**-x.xx.xx.xx-xx
- Install cs1000-**patchWeb**-x.xx.xx.xx-xx
- Install the Service Pack

The Service Pack 10 installation sequence for Member Linux servers (using Primary Patch Manager / Local CLI):

- Install cs1000-**linuxbase**-x.xx.xx.xx-xx
- Install the Service Pack

The Service Pack 10 installation sequence for Member Linux servers (using Local Patch Manager):

- Install cs1000-**linuxbase**-x.xx.xx.xx-xx
- Install cs1000-**Jboss-Quantum**-x.xx.xx.xx-xx
- Install cs1000-**patchWeb**-x.xx.xx.xx-xx
- Install the Service Pack

Instructions for existing CS1000 Release 7.6 System, CSR3 platform (i.e. running an older Service Pack version)

In general, if the SP contains the following SU's and if they have changed, they will be available on ESPL as standalone files. They must be installed individually first via CLI, **before** installing the SP

The Service Pack 10 installation sequence for Primary Linux server:

- Install cs1000-**linuxbase**-el6-x.xx.xx.xx-xx
- Install cs1000-**Jboss-Quantum**-el6-x.xx.xx.xx-xx
- Install the Service Pack

The Service Pack 10 installation sequence for Member Linux servers (using Primary Patch Manager / Local CLI):

- Install cs1000-**linuxbase**-el6-x.xx.xx.xx-xx
- Install the Service Pack

The Service Pack 10 installation sequence for Member Linux servers (using Local Patch Manager):

- Install cs1000-**linuxbase**-el6-x.xx.xx.xx-xx
- Install cs1000-**Jboss-Quantum**-el6-x.xx.xx.xx-xx
- Install the Service Pack

Special Instructions for SUs provided with the Service Pack

Several SUs that have special Instructions. Please refer to Table 4 and Table 6 for details.

AMS Service Pack Installation Special Instructions for AMS 7.0

Note that AMS 7.0 is end of software support as per PSN 3499 (Communication Server 1000 lifecycle bulletin) on Support Portal. Customers are recommended to upgrade to AMS 7.6 to ensure software support is available.

All SUs and patches noted in this section can be found on download pages for appropriate Service Pack bundles or inside the bundles. Please check Production Linux / Linux_EL6 / AMS_X64 Service Packs page in ESPL.

Please find details of AMS QFE installation in chapter 10 of NN43001-407 CS1000_Patching_Fundamentals_7_6.

The order of patching AMS 7.0 servers is as follows:

- Install cs1000-**linuxbase**-x.xx.xx.xx-xx
- Install the Service Pack
- Ensure that the AMS targets have QFE-platform 1-12 patches and QFE-EM 1 patch applied prior to the SP installation. The QFEs can be downloaded via ESPL. Click here to see details for QFE files.

  To install AMS patches use the following command under admin2:

  maspatch apply </path/to/patch/file> -n

AMS Service Pack Installation Special Instructions for AMS 7.6

All SUs and patches noted in this section can be found on download pages for appropriate Service Pack bundles or inside the bundles. Please check Production Linux / Linux_EL6 / AMS_X64 Service Packs page in ESPL.

AMS 7.6 Service Pack 4 installation sequence:

- Install cs1000-**linuxbase**-amsx64-x.xx.xx.xx-xx
- Stop Avaya applications with use of **appstart stop** command.
- Install the Service Pack

After installing AMS 7.6 Service Pack 4 reboot the server.

AMS 7.6 Special Information

A technical white paper on "CS1000 Linux Base for AMS 7.6" is available via Support Portal @ https://downloads.avaya.com/css/P8/documents/101012827

It can also be accessed as follows

- Go to http://support.avaya.com
- Click on "Support by Product" and then "Documents" link on the dashboard menu.
- Enter product name as "Communication Server 1000"
- Select "7.6" from the Choose Release dropdown
- Filter based on "White Paper" content type

Notes on migration of AMS 7.0 database with use of an USB flash

If it is necessary to migrate the AMS 7.0 database using a USB flash drive, appropriate AMS backup files should be copied into the "amsinfo" directory on the USB flash drive.

Configuration of SNMP

Since registration in UCM security domains is not supported for servers with AMS 7.6, it is no longer possible to configure SNMP profiles and configure a list of destinations for SNMP traps in the SNMP Profile Manager.

Instead of SNMP Profile Manager, AMS Element Manager should be used for configuration of SNMP traps and SNMP agent. Appropriate settings can be changed on the AMS EM page:

System Configuration -> Network Settings -> General Settings

For more information on use of AMS Element Manager for configuration of SNMP, please refer to "Implementing and Administering Avaya Media Server 7.6".

In case of a need to change "System Name", "System Contact" or "System Location" strings, which are used for identification of a system by network management systems, use ***basesnmpconfig*** command in cli.

In case of a need to change "Navigation System Name" or "Navigation Site Name" identification strings that are included into SNMP traps from CS1000 Linux Base use ***basesnmpconfig*** command in cli.

Please note, any changes in AMS EM related to SNMP traps or to SNMP agent should be followed by a reboot of the system. This is required for restart of SNMP related services. The services can also be restarted with use of ***basesnmpconfig --restart*** command. In this case the reboot can be avoided.

CS1000 Download and Installation

Download the files listed under **Communication Server 1000 7.6 Service Pack 10 / Deplist and AMS QFEs** files from the Avaya ESPL Web site https://espl.avaya.com. These files will be required during the installation of Release 7.6 Service Pack 10.

Also note that System Manager 6.3.22, System Manager 7.1.3, System Manager 8.0 and System Manager 8.0.1 hot fixes are required – more information in Known Limitations and Operational Assistance in this document.

For more information, see "**Installing the Service Pack**" section.

ESPL Service Pack 10 file listing & Avaya Support 7.6 Software Images

ESPL hyperlink	Description	File Name	Size (Mb)	MD5 Checksum
Communication Server 1000 7.6 Service Pack 10/Deplist, AMS QFEs and DSP loadware. **Note: Links below open only the main page. Select Version 7.6 and specify the content to be downloaded.** **Service Pack 10 New Content.**				
Service Pack 10	7.6. Service Pack 10	SP_7.6_10.zip	1194.31	6DD6EBEEC1ACE635CF3DACACAFC5F2E8
Service Pack 10 for CSR3	7.6. Service Pack 10 for CSR3	SP_el6_7.6_10.zip	701.38	58B0F4DF7C87FC864852EF789BC2A7FA
CS deplists SP10	CPPM deplist	CPM_7.6_10.zip	~ 1.72	-
	CPP4 deplist	PP4_7.6_10.zip	~ 1.73	-
	CPPL deplist	CPL_7.6_10.zip	~ 1.67	-
MGC and UDT loadware	MGC and UDT loadware	MGC_UDT_loadware_SP10.zip	4.14	5BCAEBC92136FD2785B7994F17C82F90
SMC deplist	SMC deplist	SMC_7.6_10.zip	~ 0.01	-
MC32S deplist	MC32S deplist	MC32S_7.6_10.zip	~ 0.02	-
AMS X64 SP4	AMS_X64 Service Pack 4, AMS 7.6	SP4_amsx64_17092018.ntl	324.96	ED4CB52F16AC339867D1F3D5844BD69C
AMS X64 SP4 for CSR3	AMS_X64 Service Pack 4 for CSR3, AMS 7.6	SP4_el6_amsx64_17092018.ntl	85.20	CC566434C62A4877C217EAEA0C1D35E9

ESPL hyperlink	Description	File Name	Size (Mb)	MD5 Checksum
Mandatory System Manager hot fixes for SMGR releases 6.3.22, 7.1.3 and 8.0 **Note: This is available from ESPL and PLDS**				
SMGR 6.3.22 HF	SMGR 6.3.22 hot fix Hot fix Rev No: 5918454	System_Manager_R6.3_FP4_SP22_HF_5918454.bin	29.15	32607525AA6275991962D20D4177D460
SMGR 7.1.3 HF	SMGR 7.1.3 hot fix Hot fix Rev No: 713008415	System_Manager_R7.1.3.0_HF_713008415.bin	268.00	C640F38E7824920C0A42A168C13DCF47
SMGR 8.0 HF	SMGR 8.0 hot fix Hot fix Rev No: 800008954	System_Manager_R8.0.0.0_GA_HF_800008954.bin	686.92	F13556BA7517772FEC474834AAF0D283
SMGR 8.0.1 HF	SMGR 8.0.1 hot fix Hot fix Rev No: 801009225	System_Manager_R8.0.1.0_HF_801009225.bin	485.12	95EDB2746262438C561FE5F4F5BCB34F
The content carried forward from previous Service Packs **Note: This is available from ESPL**				
CS image	CPPM	765q_cpm.zip	13.60	3FC30006CB551B769F7CA486B48DC07A
	CPP4	765q_pp4.zip	13.53	490374D73558E645537ED078DB4B2609
DSP loadware	DSP loadware	DSP_loadware.zip	10.06	9D2BCAA0F7745FFE5B6D60E3F4F860C7
MC32 (SA) and MC32S loadware	IPL 7.65.17 loadware for MC32 and MC32S	IPL76517_loadware.zip	9.77	A192571CDC8A4B199FF3E2EC59DE0664
MGP loadware (fresh installs only)	MGP loadware files for fresh installations	mgp010138_fresh_install_files.zip	3.09	6E0674986122F2DBE686D74E1EA8427A
AMS 7.0 QFEs	AMS 7.0 QFE-platform patches #1-12 and QFE-EM patch #1	QFE_7.0.0.623.zip	12.67	2A71BAD877412BBA7A9BA2F81126CD0A
Communications Server 1000 7.6 S/W files **Note: In PLDS, select Application: Communication Server 1000 and Version = 7.6**				
CS1K0000227	CPPM Call Server	07.65P_B00_P100_M00_CPPM.zip	62.35	B8B97909E3DCE54F023A1A6A6C3D0DC3
CS1K0000228	CPP4 Call Server	07.65P_B00_P100_M00_CPP4.zip	82.61	B2D59771FCCB25964BEA3340D1DBB08E
CS1K0000300	Linux Base	cs1000-linuxbase-7.65.16.23.iso	930.91	A0344A55D609491576EC05196C082F9B
CS1K0000230	Linux Base CF Zip	cs1000-linuxbase-7.65.16.00_cf.zip	929.89	70352FF88DD51671C5FB1CFC354BCFCF
CS1K0000231	Linux Apps	cs1000-linux-76516-P103-M00.nai	773.50	BFE8F571E5A18DA7A47741C77BD299AC

ESPL hyperlink	Description	File Name	Size (Mb)	MD5 Checksum
Communications Server 1000 7.6 S/W files **Note: In PLDS, select Application: Communication Server 1000 and Version = 7.6**				
CS1K0000320	Linux Base for CSR3	cs1000-linuxbase-el6-7.65.19.00.iso	850.39	AA5BC82ECE79244742381D87B939F157
CS1K0000322	Linux Apps for CSR3	cs1000-linux-el6-76519-P100-M00.nai	825.96	CE1E5798962761E258953A1A51BB2BC2
CS1K0000301	Linux Apps, AMS 7.0, MAS 7.0	cs1000-linux-mas-76516-P100-M01.nai	856.80	F0E2314FEECD541AA637CCC3ADA35679
CS1K0000312	AMS_X64 ISO, AMS 7.6	cs1000-linuxbase-amsx64-7.65.16.27.iso	843.39	C425BAD23E45949B1CE57A6D6C4FA68C
CS1K0000306	AMS_X64 CF Zip, AMS 7.6	cs1000-linuxbase-amsx64-7.65.16.26_cf.zip	827.66	42C6F80313467928A540964C26E1822A
CS1K0000324	AMS_X64 ISO for CSR3, AMS 7.6	cs1000-linuxbase-amsx64-7.65.19.00.iso	690.72	C8C884C5F08571E9773A60DC3D1AAA90
Communication Server 1000 7.6 BIOS upgrade files **Note: In PLDS, select Application: Communication Server 1000 and Version = 7.6**				
CS1K0000110	CPP4 BIOS	cpp4v16.zip	0.29	A3590EFA5D8EC0B7980CB19BDA77B761
CS1K0000111	CPPM BIOS	CPPM_CS_BIOS_UPGRADE.zip	0.35	8D1F957BA07270879CC4B80D5544BA73
CS1K0000274	CPDC BIOS	CPDC_Version_9_BIOS_UPGRADE.zip	0.76	BD9FF4F440CD991D3BC05BEAAF85CE92
Communication Server 1000 7.6 Standalone Tools and Applications **Note: These are available from ESPL**				
DECT MANAGER	Dect Manager-1.01.11335	DectManagerSetup_1.01.11335.exe	101.93	CAE3C113D5B9A5E4DDF3A5C607736CC4
DBA TOOLKIT	DBA Toolkit version 2.0.0.20	DBA_Setup_2.0.0.20.exe	3.29	E3E78229D3695E008CDEE1FFE65AE9A1
HEALTH CHECK MONITOR	Health Check Monitor	HealthCheck_v1.02.07.00.msi	4.68	4ECFC629957651A09FE36E03C03EE0D9

Problems fixed in Avaya CS1000 Service Pack 10

The following are the fixes delivered in Avaya CS1000 7.6 Service Pack 10 software release. These fixes are in addition to the Release 7.6 software load.

Table 1: Fixes delivered with Call Server Deplist for Service Pack 10

Patches with RED fill have special instructions that are documented in Table 2.

Patch Id	Previous Version	Patch Title	CPL	PP4	CPM
MPLR33789		VxWorks based servers should send correct ARP requests		Y	Y
MPLR33795		IP ATTN: Duplicate SIP session caused by Attendant Lockout feature. Lead to speechpath issue (speech is present when it shouldn't).	Y	Y	Y
MPLR33805	MPLR32726	MERGE: MPLR33805 (INI after BERR0705 in GF utility code related to a 3rd party MWI system connected over QSIG trunks) + MPLR32726 (EUROISDN DCH going down after DTA103, WITH ECTO (EXPLICIT CALL TRANSFER) FEATURE)	Y	Y	Y
MPLR33806		SIG SERVER MESSAGES: pbx: (ERROR) tPBX: itgMsgSend blocked, qid 80, noMsgs 1, size 359, error: Message too long.	Y	Y	Y
MPLR33811		Backups to remote SCSs fail with TEMU141 reported		Y	Y
MPLR33816		INI after BERR0705 in tSL1 from IOWRITE	Y	Y	Y
MPLR33817		MERGE: MPLR33817 "No busy announcement on attendant from callpilot" + [REPLACE] MPLR33810 ""No busy announcement on attendant from callpilot [fix for AML message conversation and CP port stuck in BUSY state issue]	Y	Y	Y
MPLR33819		Callpilot shutdown AML Link but callpilot ports and CDN stay acquired.	Y	Y	Y
MPLR33821		Required to deny a delayed deplist installation	Y	Y	Y
MPLR33822		A wrong uptime value can be reported by VxWorks based targets during SNMP walks		Y	Y
MPLR33823		Trunk Barring fails for Call Forward No Answer (CFNA) treatment when FDN = ACOD+DN	Y	Y	Y
MPLR33824		Required to deny use of RC4 cipher suites and weak MAC algorithms by the SSH client/server on VxWorks based targets		Y	Y
MPLR33826		BUG9026 (5) associated with QSIG Path Replacement	Y	Y	Y
MPLR33827		When MobileX calls Analog phone with display, Mobile Number is shown on display instead of MobileX DN	Y	Y	Y

Patch Id	Previous Version	Patch Title	CPL	PP4	CPM
MPLR33835	MPLR33767	MERGE: MPLR33835 - REWORK of MPLR33767 / MPLR33760 / MPLR33320 (PI: additional requirement to expand the solution for all UDP calls) + MPLR33086(Aura TR87/CS1000 SIP - Call forwarding or redirectCall/Call Notification v.3.8 - Incomplete notifications) + MPLR32870 (CS1000 is deleting starting digits from the dialed number and sending it to AACC Over AML link in CRS message) *** SPECIAL INSTRUCTIONS: Need to put MPLR21945 in service to activate MPLR33835 functionality. Please refer to external notes for more details. ***	Y	Y	Y
MPLR33836		Short Hunt fails when active caller sent digit to fullfill CCMS script. BUG266 printed.	Y	Y	Y
MPLR33847	MPLR33793	MERGE: MPLR33847 (No ringback tone when SIP client -> ACD #1 -> NCFW -> Call Pilot -> ACD #2 -> NCFW -> PCA -> target DN) + MPLR33793 (No ringback when SIP client calls ACDN forwarding (NCFW) to CallPilot forwarding to IP client) + MPLR33548 (No ringback provided to SIP line when calling an ACDN forwarded (NCFW) to analog TN)	Y	Y	Y
MPLR33848	MPLR33787	MERGE: MPLR33848 The call remains stuck in the attn. queue if the caller disconnects within 1 second. BUG5006 and BUG5027.+ MPLR33787 Workaround for Lineside issue with quick disconnect. Implement new solution from MPLR33785 + MPLR33663(Issue with ACD BCS) + MPLR33492 Issues Observed on Lineside E1 card + MPLR33293(Issues Observed on Lineside E1 card) + MPLR32491(DECT MSMN (Mulit-site Mobility Networking) do not work at visitor site) + MPLR33154(BUG6504 after EOVR camp- on to DCS set) *** ACT MPLR33284 is needed to activate patch functionality ***	Y	Y	Y
MPLR33850	MPLR32828 MPLR33729	MERGE:MPLR33850 "DDGD not working for MCDN calls when plugin 218 is enabled" + MPLR33838 "DDGD not working to SIPL when plugin 218 is enabled." + MPLR33839 "[Rework of MPLR32828] PI : SIGMA_CLID path uses RDL data space on 500 set to store DN of PHTN that it DCFW to. Similar to MPLR31977. *** NOTE: MPLR25180 is needed to activate PI functionality ***" + MPLR33729 "CLID not being passed from Callpilot to CS1K, CS1K in Tandem via SIP, with CLS CLBA and Plugin 218"	Y	Y	Y
MPLR33851		SCH5508 when trying to configure a DCH on a PRI GW	Y	Y	Y
MPLR33854		Required to provide a way to re-register the monitor keys for Call Server log files	Y	Y	Y

Patch Id	Previous Version	Patch Title	CPL	PP4	CPM
MPLR33855	MPLR33764	MERGE: MPLR33855 (INI after BERR705 from vcmGetFarUpdateSupport) + MPLR33764 (No-way speech after CallPilot transfers with early media) + MPLR33668(BUG330 - TAT related scenarios) + MPLR33631 (AAC 8.0 Alpha: Some users are unable to associate phone with web blade in CA) + MPLR33506 (SIP Line Set thru-dials over SIP trunk. There is no ringback tones. No speechpath after answer) + MPLR33440 (Originator does not hear ringback tone after SIP Line blind transfer to AACC) + MPLR33547 (Rework of MPLR33337: SRPT4653 in unknown scenario, REPLACES MPLR33243 MPLR33130 MPLR33173) + MPLR33432 (BUG341 is printed after upgrade to R7.6) + MPLR33415 (TAT interaction with AACC & CallPilot) + MPLR33360 (Collaboration Pack: Pass extended AAC Web Collaboration Capabilities through CS1000) + MPLR32895 (Calls to ACD agents drop (call disconnect) unexpectedly; BUG359/BUG342 printed.) + MPLR33098 (IP Call Recording does not work properly when TAT is used) + MPLR32192 (TAT Not Working on SIP trunks When ACD Agent Answers After RAN Connects) + MPLR32710 (CS1K does not forward CCMP INFO message from flare to AAC) + MPLR32466 (CS1K Collab Pack & AAC integration) + MPLR32609 (IPV6-SIPL (dual stack) can't hear greeting message to leave voice mail on CallPilot mailbox.) + MPLR32597 (TELSET A calls TELSET B, blind transfer to SIPL, FNA to another SIPL, is not working if SIP trunks are used.)	Y	Y	Y
MPLR33858		**ecnt fw** executed at ld 117 leads to a Warm Start on a system with SIPLine sets	Y	Y	Y
MPLR33859		Required to limit a number of active XMSG sessions on Call Server	Y	Y	Y
MPLR33861	MPLR33675	MERGE: MPLR33861 (MPLR33675 (Move PLUGIN 227 to PLUGIN 400) rework) + MPLR32638 (pdt> **ple 236** Response comes back that plugin is not supported This patch converts fix from patch MPLR25106 to a plugin (plugin 236))	Y	Y	Y
MPLR33862		BERR705 and INI in mmihQBuf::nextBufInQ() called from txExpBuf::purgeQueue()	Y	Y	Y
MPLR33863		INI after BERR705 in tSL1 from ACD_REPORTS:ACD_START_TRAF	Y	Y	Y
MPLR33864		**LD 20: REQ PRT; TYPE GRP; CUST :** Resulting print excludes GRP list 0.	Y	Y	Y
MPLR33868		A memory leakage in RLM module is observed on a Call Server when LTPS is down on a Sig Server	Y	Y	Y
MPLR33874	MPLR25747 MPLR33481	MERGE: MPLR33874 (BUG266 is printed without proper diagnostic info) + MPLR33481 (Rework of MPLR33439 (ESA enhanced routing does not reroute the call for MALT/QALT causes). ** PI enabler is ACT MPLR33465; it works only with SL1, QSIG, EURO trunks; using U_JUNK_WORDS[192]) + MPLR33306 (Speechpath issue with calls that fails SIP and go out TDM) + MPLR33236 (ERR118 from 2216 sets with MCA adapters. ** PI enabler is ACT MPLR33246) + MPLR32773 (R7.6 Concurrency Sustaining: Diagnostic for BUG266 call scenarios. ** using U_JUNK_WORDS[197-198]) + MPLR32716 (BUG759 and BUG467 messages printed frequently) + MPLR25747 (Plugin 35 causes one-way speechpath on Orion/Aries sets)	Y	Y	Y
MPLR33876		**CLIDVER** in LD 20 prints CLID table parameter DIDN incorrectly	Y	Y	Y

Patch Id	Previous Version	Patch Title	CPL	PP4	CPM
MPLR33877		Ability to list unregistered/registered SIP Line sets	Y	Y	Y
MPLR33879		Clean SIP user name (SIPU) table corruption	Y	Y	Y
MPLR33881	MPLR33856	MobileX conference fails with MPLR33856 (Crosstalk; BUG6504, BUG342, AUD126 related to MobileX calls ** using P_JUNK_WORDS[17])	Y	Y	Y

Table 2: Special Instructions for Call Server Deplist for Service Pack 10

Patch ID	Sysload/INI/ Required	Special instructions
MPLR33824	Yes	A reboot (a Warm Start) is required after the patch installation / uninstallation.
MPLR33835	No	Patch contains PI functionality: - The patch inserts AC in dialed DN for all outgoing UDP calls from AML acquired devices. - User should use DAPC feature for incoming calls. Please put MPLR21945 in service to activate the patch functionality.
MPLR33848	No	Notes for MPLR33787 ================================ The issue occurs due to unrecommended preferences of SYSP block and LE1 hardware issue. Need to configure recommended SYSP preferences: FLASH TIMERS 120 0896 ACT MPLR33284 needed to activate patch functionality

Patch ID	Sysload/INI/ Required	Special instructions
MPLR33855	No	From MPLR32710/MPLR33360 ================================ This patch is merged with MPLR32710/MPLR33360. So it must be used with SU cs1000-vtrk-7.65.16.23-19.i386.000 or newer; From MPLR32466 ================================ This patch is merged with MPLR32466 which has inactive PI functionality. To enable PI functionality MPLR32477 is required. Software lineup 1. CM version FP2 6.3 Load 120 or newer. 2. CS1K version GA load x210765p and 7.65.16 + following patches MPLR32466 is for call server GEN patch MPLR32477 is MPLR32466 ‘s patch enabler cs1000-vtrk-7.65.16.21-29.i386.000.ntl is for VTRK SU patch MPLR32474 is vtrk's patch enabler Tips 1. The CS1K recommended Collaboration pack configuration need to be followed. 2. Make sure there is no SIPS & SIP mix configuration in the deployment, because the CS1K does not support SIPS and SIP mix configuration, if the SIPS & SIP is mixed, the CS1K will reject the call. From MPLR32895 ================================ 2 ways to put the patch in service: 1. They can avoid CS INI (warm start) and put the patch in service at any time. They could still have few calls (max 30 per TDS loop) that could be potentially dropped after installation of the patch because of the fact that some VGWs are still not cleaned from TDS unprotected loop block. 2. They can to CS INI after putting patch in service if they want to make sure there are no dropped call at all. In this case, they need to do the patch installation using maintenance window when the traffic is low.

Patch ID	Sysload/INI/ Required	Special instructions
MPLR33861	Yes	Special Instructions for MPLR32638: ================================== Patch makes possible to enable plugin. pdt> **ple 236** PLUG-IN 236 IS ENABLED Special Instructions for MPLR ld 22 REQ:**prt** TYPE **Plugin** 236 ENABLED Q01777861 MPLR25106 DTMF for ADL INSTRUCTIONS 0F THE PATCH USAGE: ================================ In order the patch brings effect 1) it should be activated as retain patch 2) cold start should be done to CS. Special Instructions for MPLR33861: ================================== Patch changes plug-in number 227 to 400. Set status of plug-in 400 to enabled if plug-in 227 was enabled previously. INSTRUCTIONS 0F THE PATCH USAGE: ================================ In order the patch brings effect 1)it should be activated as retain patch 2) SYSLOAD IS REQUIRED.

Patch ID	Sysload/INI/ Required	Special instructions
MPLR33874	No	MPLR32773 special instructions: ================================ MPLR32733 (Tool Management) should be activated. To enable "Diagnostic for BUG266" tool: pdt> **PATCH_1 1 2** To disable "Diagnostic for BUG266" tool: pdt> **PATCH_1 1 3** To display "Diagnostic for BUG266" tool status: pdt> **PATCH_1 1 1** MEMORY REQUIREMENTS: Roughly (NCR * 32) words of unprotected SL-1 memory, where NCR is the number of call registers available in the system. MPLR33236 external notes: ================================ This patch contains inactive PI functionality. To activate PI functionality ACT MPLR33246 should be installed. MPLR33481 (MPLR33439) special instructions: ================================ Please put ACT MPLR33465 in service to activate the patch functionality. MEMORY REQUIREMENTS: (NCR * 8) words of unprotected SL-1 memory, where NCR is the number of call registers available in the system.

Patch ID	Sysload/INI/ Required	Special instructions
MPLR33881	No	To display available commands: pdt> **PATCH_6** To display status: pdt> **PATCH_6 1** To enable basic diagnostic: pdt> **PATCH_6 2** To enable enhanced diagnostic: pdt> **PATCH_6 3** To disable diagnostic: pdt> **PATCH_6 4** ----- NOTES: 1. Default configured diag. state: basic diagnostic. 2. Diag. state survives an INI. 3. Diag. state is reset to default (basic diag.) after SYSLOAD.

Table 3: Fixes Delivered with Service Pack 10

Patches and SUs with RED fill have special instructions that are documented in Table 4.

SU ID	Description of Fixes included in Each SU
MPLR33830	Obsoletes MPLR33584. INI is required. Required to update glibc and nscd packages on Linux Base because of CVE-2017-1000366
MPLR33833	Obsoletes MPLR33774. Required to align versions of used openssh packages
MPLR33837	Remove unnecessary packages to free disk space on the root partition
MPLR33870	rsyslog can crash because of very high traffic
MPLR33886	Required to update microcode_ctl package because of microcode updates [20180703]
MPLR33895	Required to update curl package because of dependency issues
avaya-cs1000-cnd-4.0.51-1.el5.i386.000	Required to limit the cipher suites used by CND
cs1000-Jboss-Quantum-7.65.16.23-16.i386.000	Required to disable intensive SSO logging
	Jboss wsdl directories are filled with files until /opt is 100% full
	Required to rebuild quantum for the current CND version
	OVL0428 error window when accessing Element Manager
cs1000-auth-7.65.16.23-1.i386.000	The first login attempt with use of a new UCM account fails
cs1000-cppmUtil-7.65.16.23-7.i686.000	Required to rebuild cppmUtil with the latest changes
cs1000-emWebLocal_6-0-7.65.16.23-1.i386.000	Need to remove Virtual Terminal from CS1000 Element Manager
cs1000-emWeb_6-0-7.65.16.23-10.i386.000	"Call Server Initialization" link is not available under Tools in the Element Manager for CoRes Call Server
	Need to remove Virtual Terminal from CS1000 Element Manager
cs1000-linuxbase-7.65.16.23-41.i386.000	The first login attempt with use of a new UCM account fails
	Required to address multiple linuxbase issues
	freeDiskSpace can remove old logs from /var/log partition
	Required to address a number of patching issues
cs1000-mscAnnc-7.65.16.23-2.i386.000	Required to limit the cipher suites list used by CS1000 applications
cs1000-mscAttn-7.65.16.23-16.i386.000	Required to limit the cipher suites list used by CS1000 applications
cs1000-mscConf-7.65.16.23-2.i386.000	Required to limit the cipher suites list used by CS1000 applications
cs1000-mscMusc-7.65.16.23-2.i386.000	Required to limit the cipher suites list used by CS1000 applications
cs1000-mscTone-7.65.16.23-2.i386.000	Required to limit the cipher suites list used by CS1000 applications
cs1000-patchWeb-7.65.16.23-4.i386.000	Patch Manager shows as "ready to install" patches which are not applicable for selected target platform

SU ID	Description of Fixes included in Each SU
	Unable to install some FRU patches (like MPLR33886) via the central Patch Manager
cs1000-pd-7.65.16.23-2.i386.000	Required to limit the cipher suites list used by CS1000 applications
cs1000-sps-7.65.16.23-5.i386.000	Required to limit the cipher suites list used by CS1000 applications
cs1000-tps-7.65.16.23-23.i386.000	Agents don't see the calling extension Name (only DN) when transferring from their in calls key
cs1000-vtrk-7.65.16.23-140.i386.000	Tandem Node is not sending PRACK and call fails
	Required to limit the cipher suites list used by CS1000 applications
	Moving SIPL uext-tn causes VTRK application down on SS
	More than one 183 with SDP in reply for slow start INVITE in tandem case
	SIP calls fail because of a SIP session leakage triggered by an unsupported PUBLISH method
	J129 set cannot re-register after a vtrk restart
jdk-1.6.0_201-fcs.i586.000	Required to update Oracle JDK package on Linux Base to 6u191 because of multiple CVEs
	Required to update Oracle JDK package on Linux Base to 6u201 because of CVE-2018-2938 and CVE-2018-2952
kernel-2.6.18-434.el5.i686.000	Required to update kernel packages on Linux Base because of CVE-2017-1000364 and CVE-2017-7895
	Required to update kernel packages on Linux Base because of CVE-2017-1000253
	Required to update kernel package on Linux Base because of CVE-2018-8897
	Required to update kernel packages on Linux Base because of CVE-2017-14106
	Required to align the patching level for kernel package
kernel-PAE-2.6.18-434.el5.i686.000	Required to update kernel packages on Linux Base because of CVE-2017-1000364 and CVE-2017-7895
	Required to update kernel packages on Linux Base because of CVE-2017-1000253
	Required to update kernel-PAE package on Linux Base because of CVE-2018-8897
	Required to update kernel packages on Linux Base because of CVE-2017-14106

SU ID	Description of Fixes included in Each SU
	Required to align the patching level for kernel package
tzdata-2018e-3.el5.i386.000	Required to update time zone info on Linux Base to 2018e level

Table 4: Special Instructions for Service Pack 10

SU ID	Special Instructions for Each SU
MPLR33830	A reboot of the server is recommended after installation of this patch because of necessity to restart system services and CS1000 applications. Please note that uninstallation of the patch will not lead to recovery of the previous glibc/nscd packages.
MPLR33833	A reboot of the server or a restart of sshd daemon is recommended after installation of this patch. E.g.: # **/sbin/service sshd restart** Please note that uninstallation of this patch will not lead to downgrade of new OpenSSH packages.
MPLR33870	cs1000-linuxbase-7.65.16.23-18.i386 SU or a newer one must be in-service prior installation of this patch. Please note that uninstallation of the patch will not lead to complete removal of updated packages.
MPLR33886	A reboot of the server is recommended after installation of this patch because of necessity to update the CPU microcode if the update is available. Please note that uninstallation of the patch will not lead to complete removal of microcode_ctl.
MPLR33895	A server reboot or a restart of Avaya applications is recommended after installation of this update. Please note that uninstallation of the patch will not lead to complete removal of updated packages.
avaya-cs1000-cnd-4.0.51-1.el5.i386.000	Please note that a restart of all Avaya applications is required for installation / uninstallation of this SU.
cs1000-Jboss-Quantum-7.65.16.23-16.i386.000	This SU requires avaya-cs1000-cnd-4.0.51-1.el5.i386.000 or a newer one for proper work.

SU ID	Special Instructions for Each SU
cs1000-auth-7.65.16.23-1.i386.000	Please note that MPLR33833 and cs1000-linuxbase-7.65.16.23-37.i386.000 or their replacements should be installed before installation of this SU.
cs1000-emWebLocal_6-0-7.65.16.23-1.i386.000	This patch requires patch Jboss-Quantum-7.65.16.22-1 or higher to be installed.
cs1000-emWeb_6-0-7.65.16.23-10.i386.000	This patch requires patch Jboss-Quantum-7.65.16.22-1 or higher to be installed. Traffic report collection (EM -> Tools -> Logs and Reports -> Operational Measurements -> Traffic Report Collection) should be disabled before SU activation.
cs1000-linuxbase-7.65.16.23-41.i386.000	1. Please note that this patch must be installed before a Service Pack. 2. Please note that tzdata-2018e-3.el5.i386.000 is required for this SU. 3. Upgrading from cs1000-linuxbase-7.65.16.21-01.i386 or prior SU, please do the following under root user before patch installation: **chmod 444 /var/opt/nortel/base-apps/*** **chmod 755 /opt/nortel/Jboss-Quantum/run/jbossd** 4. If it is required to minimize risks related to use of CBC block ciphers and weak MAC algorithms for SSH, please reboot the server or restart sshd service after installation of this SU. 5. If it is required to eliminate issues related to false alarms from sshd service related to monit health checks, please reboot the server after installation of this SU. 6. If it is required to mitigate risks related to CVE-2013-5211, please reconfigure NTP after installation of this SU.
cs1000-mscAnnc-7.65.16.23-2.i386.000	1. The following patches/SUs or newer ones must be in service together: - MPLR33231; - cs1000-mscAnnc-7.65.16.22-2; - cs1000-mscMusc-7.65.16.22-4; - cs1000-mscConf-7.65.16.22-2; - cs1000-mscTone-7.65.16.22-2; - cs1000-mscAttn-7.65.16.22-2. 2. This SU limits cipher suites used for TLS connections. If this leads to interop issues, it should be possible to revert the changes with use of MPLR33812.

SU ID	Special Instructions for Each SU
cs1000-mscAttn-7.65.16.23-16.i386.000	1. The following patches/SUs or newer ones must be in service together: - MPLR33231; - cs1000-mscAnnc-7.65.16.22-2; - cs1000-mscMusc-7.65.16.22-4; - cs1000-mscConf-7.65.16.22-2; - cs1000-mscTone-7.65.16.22-2; - cs1000-mscAttn-7.65.16.22-2. 2. This SU limits cipher suites used for TLS connections. If this leads to interop issues, it should be possible to revert the changes with use of MPLR33812.
cs1000-mscConf-7.65.16.23-2.i386.000	1. The following patches/SUs or newer ones must be in service together: - MPLR33231; - cs1000-mscAnnc-7.65.16.22-2; - cs1000-mscMusc-7.65.16.22-4; - cs1000-mscConf-7.65.16.22-2; - cs1000-mscTone-7.65.16.22-2; - cs1000-mscAttn-7.65.16.22-2. 2. This SU limits cipher suites used for TLS connections. If this leads to interop issues, it should be possible to revert the changes with use of MPLR33812.
cs1000-mscMusc-7.65.16.23-2.i386.000	1. The following patches/SUs or newer ones must be in service together: - MPLR33231; - cs1000-mscAnnc-7.65.16.22-2; - cs1000-mscMusc-7.65.16.22-4; - cs1000-mscConf-7.65.16.22-2; - cs1000-mscTone-7.65.16.22-2; - cs1000-mscAttn-7.65.16.22-2. 2. This SU limits cipher suites used for TLS connections. If this leads to interop issues, it should be possible to revert the changes with use of MPLR33812.

SU ID	Special Instructions for Each SU
cs1000-mscTone-7.65.16.23-2.i386.000	1. The following patches/SUs or newer ones must be in service together: - MPLR33231; - cs1000-mscAnnc-7.65.16.22-2; - cs1000-mscMusc-7.65.16.22-4; - cs1000-mscConf-7.65.16.22-2; - cs1000-mscTone-7.65.16.22-2; - cs1000-mscAttn-7.65.16.22-2. 2. This SU limits cipher suites used for TLS connections. If this leads to interop issues, it should be possible to revert the changes with use of MPLR33812.
cs1000-patchWeb-7.65.16.23-4.i386.000	This patch requires patch Jboss-Quantum-7.65.16.22-1 and patch linuxbase-7.65.16.23-21 or higher to be installed.
cs1000-pd-7.65.16.23-2.i386.000	This SU limits cipher suites used for TLS connections. If this leads to interop issues, it should be possible to revert the changes with use of MPLR33812.
cs1000-sps-7.65.16.23-5.i386.000	This SU limits cipher suites used for TLS connections. If this leads to interop issues, it should be possible to revert the changes with use of MPLR33812.
cs1000-tps-7.65.16.23-23.i386.000	1. This SU should be loaded with Call Server patch MPLR32744. 2. If it is required to use the mutual authentication for DTLS, please also install following SUs/patches or newer ones: cs1000-csv-7.65.16.23-4.i386.000 cs1000-shared-pbx-7.65.16.23-2.i386.000. MPLR33569 If the mutual authentication is not required, but the DTLS is in use, please ensure that an appropriate option is disabled in the node settings.
cs1000-vtrk-7.65.16.23-140.i386.000	1. This SU should be loaded when a deplist from Service Pack 7 or a newer one is in-service on the Call Server. 2. If it is required to fix the issue with QoS-marking for SIPLine related traffic, please install cs1000-linuxbase-7.65.16.23-32.i386.000 SU or a newer one before installation of this vtrk SU. 3. This SU limits cipher suites used for TLS connections. If this leads to interop issues, it should be possible to revert the changes with use of MPLR33812.
jdk-1.6.0_201-fcs.i586.000	Please note that this SU requires cs1000-Jboss-Quantum-7.65.16.23-6.i386.000 or a newer one for proper work and installation.

SU ID	Special Instructions for Each SU
kernel-2.6.18-434.el5.i686.000	1. This SU is applicable to CPPM based Signaling Servers only. 2. Please note that a reboot is required after installation of this SU. 3. cs1000-linuxbase-7.65.16.23-6.i386.000 SU or a newer one is required for proper installation. 4. cppmUtil-7.65.16.23-3.i386.000 SU or a newer one is required for proper work.
kernel-PAE-2.6.18-434.el5.i686.000	1. This SU is not applicable to CPPM based Signaling Servers. 2. Please note that a reboot is required after installation of this SU. 3. cs1000-linuxbase-7.65.16.23-6.i386.000 SU or a newer one is required for proper installation. 4. cppmUtil-7.65.16.23-3.i386.000 SU or a newer one is required for proper work.

Table 5: Fixes Delivered with CSR3 Service Pack 10

Patches and SUs with RED fill have special instructions that are documented in Table 6.

SU ID	Description of Fixes included in Each SU
MPLR33831	Required to update coreutils packages because of multiple bug fixes and CVE-2017-2616
MPLR33832	Required to update libxml2 packages because of multiple CVEs
MPLR33837	Remove unnecessary packages to free disk space on the root partition
MPLR33883	Required to update glibc packages on Linux Base for CSR3 because of CVE-2017-15670 and CVE-2017-15804
MPLR33884	Required to update ntp packages on Linux Base for CSR3 because of multiple CVEs
MPLR33885	Required to update openssh packages on Linux Base for CSR3 because of CVE-2016-6210
MPLR33886	Required to update microcode_ctl package because of microcode updates [20180703]
MPLR33893	Required to limit cipher suites used by CND service
bash-4.1.2-48.el6.i686.000	Required to update bash package on Linux Base because of CVE-2016-7543 and CVE-2016-9401
cs1000-Jboss-Quantum-el6-7.65.19.00-6.i686.000	Jboss wsdl directories are filled with files until /opt is 100% full
	Required to rebuild quantum for the current CND version
	OVL0428 error window when accessing Element Manager
cs1000-auth-el6-7.65.19.00-1.i686.000	The first login attempt with use of a new UCM account fails
cs1000-cppmUtil-el6-7.65.19.00-1.i686.000	Required to rebuild cppmUtil with the latest changes
cs1000-emWebLocal_6-0-el6-7.65.19.00-1.noarch.000	Need to remove Virtual Terminal from CS1000 Element Manager
cs1000-emWeb_6-0-el6-7.65.19.00-3.noarch.000	Need to remove Virtual Terminal from CS1000 Element Manager
cs1000-linuxbase-el6-7.65.19.00-9.i686.000	A cumulative update #2 for CSR3 Linux Base
	Required to address multiple linuxbase issues
	freeDiskSpace can remove old logs from /var/log partition
	Required to address a number of patching issues
cs1000-mscAnnc-el6-7.65.19.00-1.i686.000	Required to limit the cipher suites list used by CS1000 applications
cs1000-mscAttn-el6-7.65.19.00-3.i686.000	Required to limit the cipher suites list used by CS1000 applications
cs1000-mscConf-el6-7.65.19.00-1.i686.000	Required to limit the cipher suites list used by CS1000 applications
cs1000-mscMusc-el6-7.65.19.00-1.i686.000	Required to limit the cipher suites list used by CS1000 applications

SU ID	Description of Fixes included in Each SU
cs1000-mscTone-el6-7.65.19.00-1.i686.000	Required to limit the cipher suites list used by CS1000 applications
cs1000-pass_harden-el6-7.65.19.00-3.i686.000	The new PAM configuration leads to login issues for internal and UCM users
cs1000-patchWeb-el6-7.65.19.00-2.noarch.000	Patch Manager shows as "ready to install" patches which are not applicable for selected target platform.
	Unable to install some FRU patches (like MPLR33886) via the central Patch Manager
cs1000-pd-el6-7.65.19.00-2.i686.000	Required to limit the cipher suites list used by CS1000 applications
cs1000-sps-el6-7.65.19.00-1.i686.000	Required to limit the cipher suites list used by CS1000 applications
cs1000-tps-el6-7.65.19.00-2.i686.000	Agents don't see the calling extension Name (only DN) when transferring from their in calls key
cs1000-vtrk-el6-7.65.19.00-10.i686.000	Required to limit the cipher suites list used by CS1000
	Moving SIPL uext-tn causes VTRK application down on SS
	PROP:More than one 183 with SDP in reply for slow start INVITE in tandem case
	SIP calls fail because of a SIP session leakage triggered by an unsupported PUBLISH method
	J129 set cannot re-register after a vtrk restart
expat-2.0.1-13.el6_8.i686.000	Required to update expat package on Linux Base because of CVE-2016-0718
jre-1.6.0_201-fcs.i586.000	Upgrade of JRE to 6u161
	Required to update Oracle JRE package on Linux Base to 6u191 because of multiple CVEs
	Required to update Oracle JRE package on Linux Base to 6u201 because of CVE-2018-2938 and CVE-2018-2952
kernel-2.6.32-754.3.5.el6.i686.000	Required to update kernel packages on Linux Base because of CVE-2017-1000364 and CVE-2017-7895
	Required to update kernel packages on Linux Base because of CVE-2017-1000253
	Required to update kernel packages on Linux Base because of CVE-2017-5715, CVE-2017-5753, CVE-2017-5754, CVE-2017-7645, CVE-2017-14106, CVE-2017-13166 and CVE-2017-18017

SU ID	Description of Fixes included in Each SU
	Required to update kernel packages on Linux Base for CSR3 because of multiple CVEs
sudo-1.8.6p3-29.el6_9.i686.000	Required to update sudo package on Linux Base because of CVE-2016-7032, CVE-2016-7076, CVE-2017-1000367 and CVE-2017-1000368
tzdata-2018e-3.el6.noarch.000	Required to update time zone info on Linux Base to 2018e level

Table 6: Special Instructions for CSR3 Service Pack 10

SU ID	Special Instructions for Each SU
MPLR33832	A reboot of the server is recommended after installation of this patch because of necessity to restart system services and CS1000 applications. Please note that uninstallation of the patch will not lead to recovery of the original packages.
MPLR33883	A reboot of the server is recommended after installation of this patch because of necessity to restart system services and CS1000 applications. Please note that uninstallation of the patch will not lead to recovery of the previous glibc/nscd packages.
MPLR33885	A reboot of the server or a restart of sshd daemon is recommended after installation of this patch.
MPLR33886	A reboot of the server is recommended after installation of this patch because of necessity to update the CPU microcode if the update is available. Please note that uninstallation of the patch will not lead to complete removal of microcode_ctl.
MPLR33893	Please note that installation of this patch requires a restart of all Avaya applications.
cs1000-linuxbase-el6-7.65.19.00-9.i686.000	1. Please note that tzdata-2018e-3.el6.noarch.000 is required for this SU. 2. If it is required to mitigate risks related to CVE-2013-5211, please reconfigure NTP after installation of this SU.
cs1000-mscAnnc-el6-7.65.19.00-1.i686.000	This SU limits cipher suites used for TLS connections. If this leads to interop issues, it should be possible to revert the changes with use of MPLR33812.

SU ID	**Special Instructions for Each SU**
cs1000-mscAttn-el6-7.65.19.00-3.i686.000	1. This SU should be used when MPLR33231 or a suitable replacement is in-service on the Call Server. 2. This SU limits cipher suites used for TLS connections. If this leads to interop issues, it should be possible to revert the changes with use of MPLR33812.
cs1000-mscConf-el6-7.65.19.00-1.i686.000	This SU limits cipher suites used for TLS connections. If this leads to interop issues, it should be possible to revert the changes with use of MPLR33812.
cs1000-mscMusc-el6-7.65.19.00-1.i686.000	This SU limits cipher suites used for TLS connections. If this leads to interop issues, it should be possible to revert the changes with use of MPLR33812.
cs1000-mscTone-el6-7.65.19.00-1.i686.000	This SU limits cipher suites used for TLS connections. If this leads to interop issues, it should be possible to revert the changes with use of MPLR33812.
cs1000-pd-el6-7.65.19.00-2.i686.000	This SU limits cipher suites used for TLS connections. If this leads to interop issues, it should be possible to revert the changes with use of MPLR33812.
cs1000-sps-el6-7.65.19.00-1.i686.000	This SU limits cipher suites used for TLS connections. If this leads to interop issues, it should be possible to revert the changes with use of MPLR33812.
cs1000-vtrk-el6-7.65.19.00-10.i686.000	1. This SU should be loaded when a deplist from Service Pack 7 or a newer one is in-service on the Call Server. 2. If it is required to fix the issue with QoS-marking for SIPLine related traffic, please install cs1000-linuxbase-el6-7.65.19.00-3.i686.000 SU or a newer one before installation of this vtrk SU. 3. This SU limits cipher suites used for TLS connections. If this leads to interop issues, it should be possible to revert the changes with use of MPLR33812.
expat-2.0.1-13.el6_8.i686.000	A reboot of the server is recommended after installation of this patch because of necessity to restart system services and CS1000 applications.
kernel-2.6.32-754.3.5.el6.i686.000	1. Please note that a reboot is required after installation of this update. 2. cs1000-linuxbase-el6-7.65.19.00-1.i686.000 SU or a newer one is required for proper installation. 3. This SU provides fixes for Meltdown/Spectre vulnerabilities. The fixes can cause performance issues. Please check PSN 5158 for more info.

Note:
1. The following requirement can safely be ignored in case of cs1000-Jboss-Quantum-el6-7.65.19.00-6.i686.000 serviceability update: *This SU requires avaya-cs1000-cnd-5.0.10-1.el6.i686.000 or a newer one for proper work.*

Table 7: Fixes Delivered with Non-CSR3 Service Pack 4 for amsx64

Patches and SUs with RED fill have special instructions that are documented in Table 8.

SU ID	Description of Fixes included in Each SU
MPLR33830	Required to update glibc and nscd packages on Linux Base because of CVE-2017-1000366
MPLR33886	Required to update microcode_ctl package because of microcode updates [20180703]
MPLR33888	Required to rework MPLR33837 to keep ncurses.i386
cs1000-cppmUtil-amsx64-7.65.16.26-3.i686.000	Required to rebuild cppmUtil with the latest changes
cs1000-linuxbase-amsx64-7.65.16.26-14.i386.000	Required to address a number of patching issues
kernel-2.6.18-434.el5.x86_64.000	Required to update kernel packages on Linux Base because of CVE-2018-3620 and CVE-2018-3646
pass_harden-amsx64-7.65.16.26-2.i386.000	The account locking policy is not well defined
pcap-amsx64-7.65.16.26-1.i386.000	Increase the maximal size of pcap files captured by pcapTool
sudo-1.7.2p1-31.el5_11.x86_64.000	Required to update sudo package on Linux Base because of CVE-2017-1000367 and CVE-2017-1000368
tzdata-2018e-3.el5.x86_64.000	Required to update time zone info on Linux Base to 2018e level

Table 8: Special Instructions for Non-CSR3 Service Pack 4 for amsx64

SU ID	Special Instructions for Each SU
MPLR33830	A reboot of the server is recommended after installation of this patch because of necessity to restart system services and AMS services. Please note that uninstallation of the patch will not lead to recovery of the previous glibc/nscd packages.
MPLR33886	A reboot of the server is recommended after installation of this patch because of necessity to update the CPU microcode if the update is available. Please note that uninstallation of the patch will not lead to complete removal of microcode_ctl.
cs1000-linuxbase-amsx64-7.65.16.26-14.i386.000	1. This SU must be installed prior a Service Pack. 2. tzdata-2018e-3.el5.x86_64.000 is required for this SU. It can be installed after installation of this SU. 3. It is required to reconfigure NTP service with use of ntpconfig command to ensure that the system is not affected by CVE-2013-5211. The reconfiguration should be performed after installation of this SU once. 4. If it is required to eliminate issues related to false alarms from sshd service related to monit health checks, please reboot the server after installation of this SU.
kernel-2.6.18-434.el5.x86_64.000	1. Please note that a reboot is required after installation of this SU. 2. cs1000-linuxbase-amsx64-7.65.16.26-1.i386.000 SU or a newer one is required for proper installation.

Table 9: Fixes Delivered with CSR3 Service Pack 4 for amsx64

Patches and SUs with RED fill have special instructions that are documented in Table 10.

SU ID	Description of Fixes included in Each SU
MPLR33831	Required to update coreutils packages because of multiple bug fixes and CVE-2017-2616
MPLR33832	Required to update libxml2 packages because of multiple CVEs
MPLR33837	Remove unnecessary packages to free disk space on the root partition
MPLR33883	Required to update glibc packages on Linux Base for CSR3 because of CVE-2017-15670 and CVE-2017-15804
MPLR33884	Required to update ntp packages on Linux Base for CSR3 because of multiple CVEs
MPLR33885	Required to update openssh packages on Linux Base for CSR3 because of CVE-2016-6210
MPLR33886	Required to update microcode_ctl package because of microcode updates [20180703]
bash-4.1.2-48.el6.i686.000	Required to update bash package on Linux Base because of CVE-2016-7543 and CVE-2016-9401
cs1000-cppmUtil-amsx64-7.65.19.00-1.i686.000	Required to rebuild cppmUtil with the latest changes
cs1000-linuxbase-amsx64-7.65.19.00-10.i686.000	Required to address a number of patching issues
cs1000-pass_harden-amsx64-7.65.19.00-2.i686.000	The account locking policy is not well defined
cs1000-pcap-amsx64-7.65.19.00-1.i686.000	Increase the maximal size of pcap files captured by pcapTool
expat-2.0.1-13.el6_8.i686.000	Required to update expat package on Linux Base because of CVE-2016-0718
kernel-2.6.32-754.3.5.el6.i686.000	Required to update kernel packages on Linux Base for CSR3 because of multiple CVEs
sudo-1.8.6p3-29.el6_9.i686.000	Required to update sudo package on Linux Base because of CVE-2016-7032, CVE-2016-7076, CVE-2017-1000367 and CVE-2017-1000368
tzdata-2018e-3.el6.noarch.000	Required to update time zone info on Linux Base to 2018e level

Table 10: Special Instructions for CSR3 Service Pack 4 for amsx64

SU ID	Special Instructions for Each SU
MPLR33832	A reboot of the server is recommended after installation of this patch because of necessity to restart system services. Please note that uninstallation of the patch will not lead to recovery of the original packages.
MPLR33883	A reboot of the server is recommended after installation of this patch because of necessity to restart system services and CS1000 applications. Please note that uninstallation of the patch will not lead to recovery of the previous glibc/nscd packages.

SU ID	Special Instructions for Each SU
MPLR33885	A reboot of the server or a restart of sshd daemon is recommended after installation of this patch.
MPLR33886	A reboot of the server is recommended after installation of this patch because of necessity to update the CPU microcode if the update is available. Please note that uninstallation of the patch will not lead to complete removal of microcode_ctl.
cs1000-linuxbase-amsx64-7.65.19.00-10.i686.000	1. This SU must be installed prior a Service Pack. 2. tzdata-2018e-3.el6.noarch.000 is required for this SU. It can be installed after installation of this SU. 3. It is required to reconfigure NTP service with use of ntpconfig command to ensure that the system is not affected by CVE-2013-5211. The reconfiguration should be performed after installation of this SU once.
expat-2.0.1-13.el6_8.i686.000	A reboot of the server is recommended after installation of this patch because of necessity to restart system services.
kernel-2.6.32-754.3.5.el6.i686.000	1. Please note that a reboot is required after installation of this update. 2. cs1000-linuxbase-amsx64-7.65.19.00-1.i686.000 SU or a newer one is required for proper installation. 3. This SU provides fixes for Meltdown/Spectre vulnerabilities. The fixes can cause performance issues. Please check **PSN 5158** for more info.

Table 11: Fixes delivered with MC32/MC32S Service Pack 10

Patch ID	Title	Patch Category
MPLR33711	An active SSH session is closed after an hour of work	SMC[1], MC32S
MPLR33789	VxWorks based servers should send correct ARP requests	SMC[1], MC32S
MPLR33822	A wrong uptime value can be reported by VxWorks based targets during SNMP walks	SMC[1], MC32S
MPLR33824	Required to deny use of RC4 cipher suites and weak MAC algorithms by the SSH client/server on VxWorks based targets Special Instructions: A reboot is required after the patch installation / uninstallation.	MC32S
MPLR33828	Use of MPLR33713 on SMC can lead to a memory corruption *** THIS PATCH IS NOT APPLICABLE TO MGC/MC32S *** Special Instructions: It is recommended to reboot a card after installation of MPLR33828. If MPLR33713 is already in-service it can be required to remove it from the disk firstly and reboot the card. After that it should be okay to proceed with installation of MPLR33828.	SMC[1,2]

Note:

1. Please note that the patch is not included into the deplist archive for SMC. It is required to install the patch manually if it is reasonable.

2. Because of issues with MPLR33713 in case of SMC, the patch was replaced by MPLR33828. Please check MPLR33713 related corruption in case of SMC section for more info on the issue and steps to replace MPLR33713 if it is already installed on an SMC card.

Table 12: Fixes Delivered for MGC Service Pack 10

Loadware	Fix delivered
MGCCDC11[1]	1. MPLR33711 - CS1000-7781 -- An active SSH session is closed after an hour of work 2. MPLR33822 - CS1000-7771 -- A wrong uptime value can be reported by VxWorks based targets during SNMP walks 3. MPLR33824 - CS1000-7775 -- Required to deny use of RC4 cipher suites and weak MAC algorithms by the SSH client/server on VxWorks based targets 4. MPLR33845 - CS1000-7847 -- Some revisions of NT7K20AB cannot be re-enabled at ld 32 because of MPLR33762

Note:

1. Please note that installation of MGCCDC11 loadware over any earlier CSP loadware requires an MGC reboot because of special instructions for MPLR33824. The reboot is performed automatically if appropriate upgrade policies allow this.

Table 13: Fixes Delivered along with SMGR hot fixes

Special instructions for SMGR hot fixes are documented in appropriate sections in this document (SMGR 6.3.22 hot fix installation, SMGR 7.1.3 hot fix installation, SMGR 8.0 hot fix installation and SMGR 8.0.1 hot fix installation)

SMGR Release	Hot fix revision	Fix delivered
6.3.22	5918454	Unable to install some FRU patches (like MPLR33886) via the central Patch Manager
7.1.3.0	713008415	Unable to load a Service Pack.
		Unable to install some FRU patches (like MPLR33886) via the central Patch Manager
8.0	800008954	Add CS1000 support for SMGR 8.0.
		Unable to install some FRU patches (like MPLR33886) via the central Patch Manager
8.0.1	801009225	Add CS1000 support for SMGR 8.0.1.

Known Limitations and Operational Assistance

Common Server R3 limitations

- HP DL360 G9 (CSR3) server is the only supported server to run new CSR3 specific Linux Base system and appropriate CS1000 applications.
- CoRes Call Server is not supported on the new (CSR3) base system.
- Primary and secondary NRSs cannot be deployed on systems with different base systems (non-CSR3 and CSR3 ones) because of possible issues with data replication.
- CS1000 applications can only be deployed on applicable Linux Base systems. Different application sets are provided for systems based on non-CSR3 and CSR3 Linux Base.
- System backups prepared on a system with the old (non-CSR3) base system can be restored on a system with the new (CSR3) base system. The reverse operation is not possible.
- AMS 7.0 cannot be deployed on the new (CSR3) base system. Note also that AMS 7.0 is End of Manufacture Support for software and customers are recommended to upgrade to latest Avaya Media Server (AMS) 7.6.
- ISO management is restricted on Avaya CPPM platform (the original non-CSR3 based ISO is used with no option to upload more or delete existing) to allow for known storage space limitation.

Web browsers support

1. The currently supported browsers are as follows:

- Microsoft Internet Explorer 11.x
- Mozilla Firefox 60.0, 61.0 or 62.0

2. The recent changes in a list of allowed cipher suites used for access to the Web interface can cause access issues to UCM (in case of non-SMGR configurations) or EM.

In such a case it is recommended to upgrade the used Web browsers or switch to supported versions. If this is not possible, it can be acceptable to enable the legacy cipher suites with use of **harden jboss_web level low** command as a temporary workaround.

3. A number of browsers discontinued support of Oracle Java NPAPI plugin. As result it can be impossible to preconfigure a CS1000 CoRes Call Server with a non-default database in the deployment manager. In such a case it is advised to preconfigure the CoRes Call Server with the default database first and recover the custom database backup after the applications are deployed or use Microsoft Internet Explorer that still supports Java plugins.

Mozilla Firefox discontinued support of NPAPI plugins since release 52. Please check a following link for more info.

https://www.java.com/en/download/help/firefox_java.xml

Google Chrome discontinued support of NPAPI plugins since version 45. Please check a following link for more info.

https://www.java.com/en/download/faq/chrome.xml

UCM Central Patch Manager issue

If non-SMGR Patch Managers are used for Service Pack installation: all previously loaded Service Packs, Deplists, Patches and Loadwares will be deleted to save disk space before uploading a new Service Pack/Deplist.

This can create difficulties when it is required to maintain systems with different patching levels.

AMS 7.0 EM access issue

It is known that AMS 7.0 Element Manager is not accessible when Service Pack 9 or a newer one is installed on the base system. It is a known limitation and customers are recommended to upgrade to Avaya Media Server (AMS) 7.6.

Please check **PSN 3499** for more info on the AMS 7.0 life stage.

MPLR33713 related corruption in case of SMC

It was found that use of MPLR33713 can lead to a lock of the patching subsystem and memory corruptions in case of SMC (MC32) platform. Other VxWorks based CS1000 platforms are not affected and no actions are required.

In case of SMC it is recommended to replace MPLR33713 by MPLR33828. The safest procedure is explained below.

1. Ensure that the problem card is not used for call processing – it can be required to disable appropriate VGW channels at ld 32 on a Call Server.

2. Transfer MPLR33828 into /u/patch directory on the affected card.

3. Access the IPL shell over SSH or a serial connection, after that please access the VxWorks shell with use of **vxshell** command.

4. Remove the problem patch from the disk with use of **rm** command:
rm "/C:/u/patch/p33713_1.lsa"

5. Reboot the card with use of reboot command at the VxWorks shell or with use of the reset button on card's faceplate.

6. When the card is up after the reboot, please access the IPL shell and install MPLR33828 as usual.

7. After that it is recommended to reboot the card again. This can help to minimize risks of the heap corruptions.

If MPLR33713 is not installed, it will be enough to install MPLR33828 and reboot the card after the patch installation. The SMC deplist was not updated additionally because MPLR33713 was not a part of the deplist anyway.

Please also note that MPLR33828 addresses one more patching related issue, so it is recommended to install it even if the issue fixed by MPLR33713 is not considered as a critical one.

Virtual Terminal no longer supported by CS1000 EM

The Virtual Terminal feature provided by CS1000 Element Manager is removed in Service Pack 10.

Please check **PSN 5304** for more info on the subject and use other ways for access to system elements instead.

SMGR 7.1 / SMGR 8.0 / SMGR 8.0.1: CND Insecure access is denied

The insecure access to the Common Network Directory (CND) is denied since SMGR 7.1. Customers are advised to adjust the configuration to use the secure mode for access to CND instead.

SMGR 7.1 / SMGR 8.0 / SMGR 8.0.1: CS1000 Security Domain design changes

The improved security hardening requires use of SMGR admin accounts for joining of CS1000 VxWorks based targets (like VxWorks based Call Server, Media Gateways, Media Cards) into the CS1000 security domain. This is applicable to SMGR releases since SMGR 7.1.

Please note that this change does not affect Linux based CS1000 targets.

CS1000 VxWorks based targets can be registered in the security domain as it is explained below.

1. In SMGR Dashboard open Users -> Administrators and click Add.

2. Enter User ID, full name and password and click Commit and Continue.

3. Select System Administrator role and click Continue.

4. Login under new user to SMGR GUI.

5. In Settings (🔧 or ☰ icon) -> Manage Command Line Access click Enable.

6. Use this user for joining all VxWorks targets.

7. Disable/delete the user if it is not required anymore.

Known SMGR related issues

The following table contains info on known SMGR related issues that can affect CS1000 customers

Internal ticket	SMGR Release	Description and solution
CS1000SMGR-434	SMGR 8.0 SMGR 8.0.1	**CS1000 System Backups issues** The deployment manager provides functionality to prepare system backups of CS1000 members. This feature is currently limited in case of SMGR 8.0.x. The backups can still be generated, but they cannot be stored on the SMGR server. Please use other servers as destinations for system backups instead.
CS1000SMGR-493	SMGR 8.0.1	**NFS installation of CS1000 Linux Based members can fail** Use a non-NFS installation procedure to install software on existing or new servers.
CS1000SMGR-498	SMGR 8.0 SMGR 8.0.1	**IPSec policies are not recovered during a migration to SMGR 8.0.x** It is required to verify presence of the IPSec policies after a migration and if they are missed, it will be required to recreate them.
SMGR-45556	SMGR 7.1	**CS1000 Deployment Manager access issues** It was discovered that the CS1000 Deployment Manager can become inaccessible because of a default active session limit value. The current solution is to increase the limit when the issue is observed. This can be done in the following way. 1. Go to Communication Server 1000 -> Security -> Policies page. 2. Click Edit button in 'Session Properties' section and set 'Maximum Sessions Per User' to 25.
SMGR-48107	SMGR 8.0.1	**Cannot add a new user if "Commit & Continue" button is used** Use "Commit" button to add a new user instead.

SMGR 6.3.22 hot fix installation

Download

The hot fix can be downloaded from the ESPL or PLDS portals. Please check an appropriate table in this document for more info.

Backup before applying the patch

Recommended

Patch install instructions

Service-interrupting?

IMPORTANT: If System Manager installation is a Geo-Redundancy enabled deployment, Geo-Redundancy should be disabled, the patch should be applied to both Primary and Secondary System Manager systems, and then re-enable Geo-Redundancy.

Note: This patch **MUST** be applied on Avaya Aura® System Manager 6.3 Service Pack #22.

Follow the instructions below to install the patch through System Platform Web Console:
Installing the service pack through System Platform Web Console is the preferred method of installation.

1. Log on to System Platform Web Console with admin credentials.
2. Download the service pack:
    a. Click Server Management > Patch Management.
    b. Click Download/Upload.
    c. On the Search Local and Remote Patch page, select the location to search for the service pack from the following list:
        i. Avaya Downloads (PLDS)
        ii. HTTP
        iii. SP Server
        iv. SP CD/DVD
        v. SP USB Disk
        vi. Local File System
    d. If you select HTTP or SP Server, provide the URL to the patch file.
    e. In case of HTTP, click Configure Proxy to specify a proxy server if required.
    f. If you select Local File System, click Add to locate the patch file on your computer and then upload.
    g. Use Search to search the patch file **System_Manager_R6.3_FP4_SP22_HF_5918454.bin**.
    h. Choose the patch file, and click Select.
3. Install the patch by performing the following steps:
    a. Select Server Management > Patch Management.
    b. Click on Manage.
    c. On the Patch List page, the status of the patch ID **System_Manager_R6.3_FP4_SP22_HF_5918454** must be Not Installed.
    d. Click on a patch ID **System_Manager_R6.3_FP4_SP22_HF_5918454** to see the details.
    e. On the Patch Detail page, click Install.
    f. Wait for the patch installation to complete.
4. Verify the installation and commit the patch by performing the following steps:
    a. If the patch installation is successful, commit the service pack installation using the following steps:
        i. Click Server Management > Patch Management.
        ii. Click Manage.
        iii. On the Patch List page, the status of the patch ID **System_Manager_R6.3_FP4_SP22_HF_5918454** must be Pending.

Yes. During the patch installation the System Manager services (web access to System Manager) will be disrupted for approximately 30+ minutes.

        iv. Click the patch ID **System_Manager_R6.3_FP4_SP22_HF_5918454** to see the details.
        v. On the Patch Detail page, click Commit.
    b. If the patch installation fails, click Rollback on the same page.

Verification

To verify the successful installation of the patch:

- Log on to System Manager Console.
- On the top - right corner click on the 🔧 icon and then select the “About” link. Verify that the system displays the version information in the following format:
  System Manager 6.3.22
  Build No. - 6.3.0.8.5682-6.3.8.6325
  Software Update Revision No: 6.3.22.19.8454

Failure

In case of issues with the patch, you can:

1. Retry the action. Carefully follow the instructions in this document.
2. Contact Avaya Support, with following information: Problem description, detailed steps to reproduce the problem, if any and the release version in which the issue occurs

Patch rollback instructions

If System Manager is based on System Platform deployment then rollback the patch from system platform web console.

If System Manager is based on VMWare deployment then revert the snapshot taken prior to patch installation.

In case if you still have issues with the patch rollback, you can:

1. Contact Avaya Support, with following information: Problem description, detailed steps to reproduce the problem, if any and the release version in which the issue occurs.

SMGR 7.1.3 hot fix installation

Download	
The hot fix can be downloaded from the ESPL or PLDS portals. Please check an appropriate table in this document for more info.	
Backup before applying the patch	
Recommended	
Patch install instructions	**Service-interrupting?**
IMPORTANT: If System Manager installation is a Geo-Redundancy enabled deployment, Geo-Redundancy should be disabled, the patch should be applied to both Primary and Secondary System Manager systems, and then re-enable Geo-Redundancy. **Note**: This patch **MUST** be applied on Avaya Aura® System Manager 7.1. **Follow the instructions below to install the patch through System Manager CLI for Virtualization Enablement (VMWare) environment or Avaya Virtualization Platform based deployment:** 1. Take a snapshot of System Manager virtual machine. **Note**: This activity might impact the service. 2. Copy the patch installer file (**System_Manager_R7.1.3.0_HF_713008415.bin**) to the System Manager server under the /swlibrary/ directory. 3. Access the System Manager virtual machine CLI using the user that was configured during 7.1 OVA installation. 4. Verify md5sum of the bin file with the value mentioned on PLDS (C640F38E7824920C0A42A168C13DCF47) 5. Run the patch installer using the following command: > **SMGRPatchdeploy <absolute path to System_Manager_R7.1.3.0_HF_713008415.bin file >** **Note:** you will be prompted to accept the EULA. You must accept the EULA in order to install the patch. 6. Wait for the system to execute the patch installer and display the installer prompt. 7. Log on to System Manager Console, and verify whether the System Manager UI is displayed correctly. • On the top - right corner click on the 🔧 icon and then select the “About” link. Verify that the system displays the version information in the following format: **System Manager 7.1.3.0** **Build No. - 7.1.0.0.1125193** **Software Update Revision No: 7.1.3.0.038415** 8. Remove the hot fix file (**System_Manager_R7.1.3.0_HF_713008415.bin**) from the /swlibrary/ directory once the patch has been successfully deployed. 9. Remove the snapshot taken in step #1 once all functionality has been verified. **Note**: This activity might impact the service.	Yes. During the patch installation the System Manager services (web access to System Manager) will be disrupted for approximately 30+ minutes.
Verification	
To verify the successful installation Patch: • Log on to System Manager Console. • On the top - right corner click on the 🔧 icon and then select the “About” link. Verify that the system displays the version information in the following format: **System Manager 7.1.3.0** **Build No. - 7.1.0.0.1125193**	

Software Update Revision No: 7.1.3.0.038415

Failure

In case of issues with the patch, you can:

1. Retry the action. Carefully follow the instructions in this document.
2. Contact Avaya Support, with following information: Problem description, detailed steps to reproduce the problem, if any and the release version in which the issue occurs

Patch rollback instructions

If System Manager is on VMWare deployment so revert the snapshot taken prior to patch installation.

In case if you still have issues with the patch rollback, you can:

1. Contact Avaya Support, with following information: Problem description, detailed steps to reproduce the problem, if any and the release version in which the issue occurs.

SMGR 8.0 hot fix installation

Download

The hot fix can be downloaded from the ESPL or PLDS portals. Please check an appropriate table in this document for more info.

Backup before applying the patch

Recommended

Patch install instructions

Service-interrupting?

Yes. During the patch installation the System Manager services (web access to System Manager) will be disrupted for approximately 30+ minutes.

IMPORTANT: If System Manager installation is a Geo-Redundancy enabled deployment, Geo-Redundancy should be disabled, the patch should be applied to both Primary and Secondary System Manager systems, and then re-enable Geo-Redundancy.

Note: This patch **MUST** be applied on Avaya Aura® System Manager 8.0.

Follow the instructions below to install the patch through System Manager CLI for Virtualization Enablement (VMWare) environment or Avaya Virtualization Platform based deployment:

1. Take a snapshot of System Manager virtual machine.
   Note: This activity might impact the service.
2. Copy the patch installer file (**System_Manager_R8.0.0.0_GA_HF_800008954.bin**) to the System Manager server under the /swlibrary/ directory.
3. Access the System Manager virtual machine CLI using the user that was configured during 8.0 OVA installation.
4. Verify md5sum of the bin file with the value mentioned on PLDS (F13556BA7517772FEC474834AAF0D283)
5. Run the patch installer using the following command:
   > **SMGRPatchdeploy <absolute path to System_Manager_R8.0.0.0_GA_HF_800008954.bin file>**
   Note: you will be prompted to accept the EULA. You must accept the EULA in order to install the patch.
6. Wait for the system to execute the patch installer and display the installer prompt.
7. Log on to System Manager Console and verify whether the System Manager UI is displayed correctly.
   - On the top - right corner click on the ☰ icon and then select the "About" link. Verify that the system displays the version information in the following format:
     System Manager 8.0.0.0
     Build No. - 8.0.0.0.931077
     Software Update Revision No: 8.0.0.0.098954
8. Remove the hot fix file (**System_Manager_R8.0.0.0_GA_HF_800008954.bin**) from the /swlibrary/ directory once the patch has been successfully deployed.
9. Remove the snapshot taken in step #1 once all functionality has been verified.
   Note: This activity might impact the service.

Verification

To verify the successful installation Patch:

- Log on to System Manager Console.
- On the top - right corner click on the ☰ icon and then select the "About" link. Verify that the system displays the version information in the following format:
  System Manager 8.0.0.0
  Build No. - 8.0.0.0.931077

Failure

In case of issues with the patch, you can:

1. Retry the action. Carefully follow the instructions in this document.
2. Contact Avaya Support, with following information: Problem description, detailed steps to reproduce the problem, if any and the release version in which the issue occurs

Patch rollback instructions

If System Manager is on a VMWare deployment revert the snapshot taken prior to patch installation.

In case if you still have issues with the patch rollback, you can:

1. Contact Avaya Support, with following information: Problem description, detailed steps to reproduce the problem, if any and the release version in which the issue occurs.

SMGR 8.0.1 hot fix installation

Download

The hot fix can be downloaded from the ESPL or PLDS portals. Please check an appropriate table in this document for more info.

Backup before applying the patch

Recommended

Patch install instructions

Service-interrupting?

Yes. During the patch installation the System Manager services (web access to System Manager) will be disrupted for approximately 30+ minutes.

IMPORTANT: If System Manager installation is a Geo-Redundancy enabled deployment, Geo-Redundancy should be disabled, the patch should be applied to both Primary and Secondary System Manager systems, and then re-enable Geo-Redundancy.

Note: This patch **MUST** be applied on Avaya Aura® System Manager 8.0.1.

Follow the instructions below to install the patch through System Manager CLI for Virtualization Enablement (VMWare) environment or Avaya Virtualization Platform based deployment:

1. Take a snapshot of System Manager virtual machine.
   Note: This activity might impact the service.
2. Copy the patch installer file (**System_Manager_R8.0.1.0_HF_801009225.bin**) to the System Manager server under the /swlibrary/ directory.
3. Access the System Manager virtual machine CLI using the user that was configured during 8.0.1 OVA installation.
4. Verify md5sum of the bin file with the value mentioned on PLDS (95EDB2746262438C561FE5F4F5BCB34F)
5. Run the patch installer using the following command:
   > SMGRPatchdeploy <absolute path to System_Manager_R8.0.1.0_HF_801009225.bin file>
   Note: you will be prompted to accept the EULA. You must accept the EULA in order to install the patch.
6. Wait for the system to execute the patch installer and display the installer prompt.
7. Log on to System Manager Console and verify whether the System Manager UI is displayed correctly.
   - On the top - right corner click on the ☰ icon and then select the “About” link. Verify that the system displays the version information in the following format:
     System Manager 8.0.1.0
     Build No. - 8.0.0.0.931077
     Software Update Revision No: 8.0.1.0.039225
8. Remove the hot fix file (**System_Manager_R8.0.1.0_HF_801009225.bin**) from the /swlibrary/ directory once the patch has been successfully deployed.
9. Remove the snapshot taken in step #1 once all functionality has been verified.
   Note: This activity might impact the service.

Verification

To verify the successful installation Patch:

- Log on to System Manager Console.
- On the top - right corner click on the ☰ icon and then select the “About” link. Verify that the system displays the version information in the following format:
  System Manager 8.0.1.0
  Build No. - 8.0.0.0.931077

Failure

In case of issues with the patch, you can:

1. Retry the action. Carefully follow the instructions in this document.
2. Contact Avaya Support, with following information: Problem description, detailed steps to reproduce the problem, if any and the release version in which the issue occurs

Patch rollback instructions

If System Manager is on a VMWare deployment revert the snapshot taken prior to patch installation.

In case if you still have issues with the patch rollback, you can:

1. Contact Avaya Support, with following information: Problem description, detailed steps to reproduce the problem, if any and the release version in which the issue occurs.

Avaya and 3rd Party Software License Agreements

Please reference the following link for the Avaya Software License agreement and 3rd Party Software License agreements:

http://support.avaya.com/LicenseInfo/

http://support.avaya.com/ThirdPartyLicense/

In order to comply with the conditions of use needed to obtain a blanket authorization to distribute Linux OSS along with its corresponding binaries the following image has been made available. There is no need to download this image.

PLDS hyperlink	Description	File Name	Size (Mb)	MD5 Checksum
CS1K0000250	Linux el5	LinuxSource_7.6.zip	600.25	2EC474941238A46DEB69FE14C6BB152F
CS1K0000326	Linux el6	LinuxSource_7.6_el6.zip	615.12	276F6361663FDE28A16386F12AEBAD42

Product Support and Correction Notices

It is highly recommended that you read the Product Support and Correction Notices for the latest information on product changes.

To read a PSN or PCN description online:

- Go to the Avaya Support website at http://support.avaya.com.
- On the main menu, click **Downloads and Documents**.
- In the **Enter Your Product Here** field, enter **Communication Server 1000**
- In the **Choose Release** field, click **7.6.x**.
- Click **Documents**.
- Check **Product Support Notices and Product Correction Notices**.
- Click **Enter**.
- To open a specific PSN or PCN, click the PSN or PCN title link.

Technical support

Avaya Technical Support provides support for CS1000 Release 7.6

In case you find any problems with CS1000 Release 7.6:

- Retry the action. Carefully follow the instructions in the printed or online documentation.
- See the documentation that ships with your hardware for maintenance or hardware-related problems.
- Note the sequence of events that led to the problem and the exact messages that the system displays. For more information, see the troubleshooting section of the Avaya product documentation.

If you continue to have problems, contact Avaya Technical Support using one of the following methods:

- Log on to the Avaya Support website at http://support.avaya.com.
- Call or send a fax message to Avaya Support on one of the telephone numbers in the Support Directory listings on the Avaya Support website.

Using Avaya Global Services Escalation Management, you can escalate urgent service issues. For more information, see the list of Escalation Contacts on the Avaya Support website.

Before contacting Avaya Support, keep the following information handy:

- Problem description.
- Detailed steps to reproduce the problem, if any.
- The release version in which the issue occurs.

Contact support tasks

Avaya Support might request for email notification files for analysis of your application and the application environment.

For information about patches and product updates, see the Avaya Support website at http://support.avaya.com

Appendix A: Detailed Release 7.6 SW and Loadware Lineups

The online Compatibility Matrix is recommended for Communication Server 1000 Release 7.6 interworking with the Avaya Aura® portfolio. This can be accessed via the Avaya Support Portal at: https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml

PLEASE NOTE that the latest interop information for Service Pack 10 is included in the "Notes section" under Communication Server Release 7.6.7 (i.e. Service Pack 7.)

R7.6 Service Pack 10 aligns with Avaya Aura® 7.1, Avaya Aura® 8.0 and Avaya Aura® 8.0.1 – please reference **PSN 3995** (CS1000 interop with Avaya Aura) for ongoing updates.

Please note that Avaya Aura® System Manager 6.3, Avaya Aura® Session Manager 6.3 and Avaya Aura® Communication Manager 6.3 were tested with CS1000 R7.6 SP10 but have now reached the end of manufacture support as of July 2018 (End of Sale Notice / Aura 6.x and Avaya Product Lifecycle Matrix.) As result Tier IV / design support is no longer available for any interop issues raised against Avaya Aura® 6.3.

System Manager 6.3.22, 7.1.3, 8.0 and 8.0.1

Session Manager 6.3.22, 7.1.3, 8.0 and 8.0.1

Communication Manager 6.3.18, 7.1.3, 8.0 and 8.0.1

Presence Services 7.1

Core Software Element	**Version Number**
Unified Communications Manager	7.65.16 version (02.30.0120.00)
Unified Communications Manager for CSR3	7.65.19 version (02.31.0011.00)
Call Server	X210765P
Call Server with the patch limit enhancement applied	X210765Q
PSWV	100
Linux Base & Applications	7.65.16
Linux Base & Applications for CSR3	7.65.19
Subscriber Manager	submgr-2.3.0-22
IP Media (AMS 7.0 Element) (included in Linux image)+ QFE-platform 1-12 patches and QFE-EM 1 patch *(Note that AMS 7.0 is end of software support as per* ***PSN 3499****)*	7.0 (7.0.0.623)
IP Media (AMS 7.6 image)	7.65.16.26 (7.6.0.1008)
IP Media (AMS 7.6 image) for CSR3	7.65.19.00 (7.6.0.1008)
MC32S	7.65.17
MC32S Gold	6.00.15
MC32S Boot	6.00.15

Digital Set Firmware	Version Number	RELEASED WITH Service Pack 10
3902	84	-
3903	91	-
3904	94	-
3905	94	-

IP Client Model	UNIStim Firmware ID	UNIStim Firmware[1]	SIPLine Firmware[2]
IP Phone 2004 Phase 0/1[3]	0x00 (0602)	B76	-
IP Phone 2004 Phase 2[3]	0x02 (0604)	DCO	-
IP Phone 2002 Phase 1[3]	0x01 (0603)	B76	-
IP Phone 2002 Phase 2	0x02 (0604)	DCO	-
IP Phone 2001 Phase 2	0x02 (0604)	DCO	-
IP Audio Conference Phone 2033[4]	0x10 (2310)	S96 / S99	-
IP Phone 2007 Phase 2	0x21 (0621)	C96	-
IP Phone 1110	0x23 (0623)	C96	-
IP Phone 1120E	0x24 (0624)	C96	SIP1120e04.04.33.00
IP Phone 1140E	0x25 (0625)	C96	SIP1140e04.04.33.00
IP Phone 1150E	0x27 (0627)	C96	-
IP Phone 1165E	0x26 (0626)	C96	SIP1165e04.04.33.00
IP Phone 1210	0x2a (062A)	C96	-
IP Phone 1220	0x2a (062A)	C96	SIP12x004.04.33.00
IP Phone 1230	0x2a (062A)	C96	SIP12x004.04.33.00
B179 SIP Conference phone[5]	-	-	SIP 2.4 SP1

IP Softphone Model	Version Number
2050 IP Softphone[6]	4.4 SP9

Note:

1. Please check 'UNIStim Software Release 5.5.8 for 11xx/12xx/2007 IP Deskphones' download page for more info on the latest supported release. The currency file was updated accordingly.

2. Please check 'Software Release 4.4 Service Pack 10 for 1100/1200 Series IP Deskphones' download page for more info on the latest supported release.

3. Phase 0 and Phase 1 IP phones are not supported in Release 7.6. Note: Phase 0 and Phase 1 registration to the LTPS is not blocked.

4. Please check '2033 IP Conference Phone Software - 2310S99' download page for more info on the latest supported release.

5. B76 is at End of life

6. Please check '2050 IP Softphone for Windows PC Release 4.4 Service Pack 9' download page for more info on the latest supported release.

MGC Loadware	X21 0765P PSWV100	RELEASED WITH SP
CSP	DC06	DC11
MSP	AB02	
APP	BA18	
FPGA (MGCF)	AA22	
BOOT	BA18	
DSP1	AB07	
DSP2	AB07	
DSP3	AB07	
DSP4	AB07	
DSP6	AB07	
Other Loadware		
UDTC	AB31	
MGP	1.01.38	
FIJI	V29	

LOADWARE	X21 0765P PSWV100
LCRI	LOADAA02
XNET	LOADAC23
XPEC	LOADAC45
FNET	LOADAA07
FPEC	LOADAA10
MSDL	LOADAJ73
ASYN (SDI)	LOADAH51
DCH1 (DCH)	LOADAA72
MLNK (AML)	LOADAK81
BRIL	LOADAK83
BRIT	LOADAK82
MISP	LOADAJ71
MPHA (MPH)	LOADAH51
BRSC	LOADAJ71
BBRI	LOADAH54
PUPE (PRIE)	LOADAA88
BRIE	LOADAK90
ISIG	LOADAA33
SWE1	LOADBA53
UKG1	LOADBA51
AUS1	LOADBA49
DEN1	LOADBA48
FIN1	LOADBA49
GER1	LOADBA54
ITA1	LOADAA54
NOR1	LOADBA49
POR1	LOADBA49
DUT1	LOADBA50
EIR1	LOADBA49
SWI1	LOADBA53
NET1	LOADBA48
FRA1	LOADBA52
CIS1	LOADBA48
ETSI	LOADBA48
SPA1	LOADBA51

LOADWARE	X21 0765P PSWV100
BEL1	LOADBA49
E403	LOADBA07
N403	LOADBA05
JTTC	LOADAC08
TCNZ	LOADAA13
AUBR	LOADAA14
AUPR	LOADAA04
HKBR	LOADAA06
HKPR	LOADAA08
SING	LOADAA15
THAI	LOADAA07
NI02	LOADAA26
T1IS	LOADAA10
T1ES	LOADAA09
ESGF	LOADAC30
ISGF	LOADAC31
TEGF (ESGFTI)	LOADAC29
TIGF (ISGFTI)	LOADAC31
INDO	LOADAA06
JAPN	LOADAA16
MSIA	LOADAA04
CHNA	LOADAA04
INDI	LOADAA03
PHLP	LOADAA02
TAIW	LOADAA03
EAUS	LOADAA02
EGF4	LOADAC14
DCH3	LOADAA10
PUP3	LOADAA15
T1E1	LOADAA19
DITI	LOADAA40
CLKC[NTRB53]	LOADAA20

Appendix B: Details on vtrk serviceability updates

Addressed vtrk issues	vtrk serviceability update	vtrk serviceability update for CSR3
There is no speech path when call is forwarded by CM back to CS1000	cs1000-vtrk-7.65.16.23-107.i386.000	cs1000-vtrk-el6-7.65.19.00-1.i686.000[1]
TAT doesn't work on SIP trunks between CS1000 and Trio	cs1000-vtrk-7.65.16.23-109.i386.000	
Incoming PSTN SIP call CFW'ed to external number on the same SIP trunk fails with no speech path	cs1000-vtrk-7.65.16.23-111.i386.000	
Multiple coredumps per day	cs1000-vtrk-7.65.16.23-117.i386.000	
No speech path when CP transfers SIP call to PSTN	cs1000-vtrk-7.65.16.23-120.i386.000	
No speechpath issue if 200 OK contains more than one type of codecs	cs1000-vtrk-7.65.16.23-121.i386.000	
No Speech path when the call is going to Mitel system from CS1K	cs1000-vtrk-7.65.16.23-122.i386.000	
Wrong DSCP values are used for signaling traffic by Sip Line gateway	cs1000-vtrk-7.65.16.23-123.i386.000	cs1000-vtrk-el6-7.65.19.00-2.i686.000
Required to limit the cipher suites list used by CS1000 applications	cs1000-vtrk-7.65.16.23-126.i386.000	cs1000-vtrk-el6-7.65.19.00-4.i686.000
Tandem Node is not sending PRACK and call fails	cs1000-vtrk-7.65.16.23-127.i386.000	-[2]
Moving SIPL uext-tn causes VTRK application down on SS	cs1000-vtrk-7.65.16.23-129.i386.000	cs1000-vtrk-el6-7.65.19.00-5.i686.000
More than one 183 with SDP in reply for slow start INVITE in tandem case	cs1000-vtrk-7.65.16.23-130.i386.000	cs1000-vtrk-el6-7.65.19.00-6.i686.000
SIP calls fail because of a SIP session leakage triggered by an unsupported PUBLISH method	cs1000-vtrk-7.65.16.23-134.i386.000	cs1000-vtrk-el6-7.65.19.00-7.i686.000
200 OK final response contains “Require: timer" header	cs1000-vtrk-7.65.16.23-138.i386.000	cs1000-vtrk-el6-7.65.19.00-8.i686.000
Cannot establish a call because of # in PAI in SIP 200 OK sent by SLG	cs1000-vtrk-7.65.16.23-139.i386.000	cs1000-vtrk-el6-7.65.19.00-9.i686.000
J129 set cannot re-register after a vtrk restart	cs1000-vtrk-7.65.16.23-140.i386.000	cs1000-vtrk-el6-7.65.19.00-10.i686.000

Note:

1. All vtrk fixes delivered before CS1000 load for CSR3 was released are included into the GA version of vtrk for CSR3.

2. cs1000-vtrk-7.65.16.23-127.i386.000 was reworked as cs1000-vtrk-7.65.16.23-130.i386.000. Please check cs1000-vtrk-el6-7.65.19.00-6.i686.000 if the fix is required for CSR3.