Product Correction Notice (PCN)

Issue Date: 08-FEB-2010
Supplement 4 Date: 02-APR-2012
Archive Date:
PCN Number: 1692P

SECTION 1 - CUSTOMER NOTICE

Products affected by this PCN:

Avaya S8xx0 Servers and Common Server HP® ProLiant DL360 G7 running Avaya Aura® Communication Manager 5.2.1 software load R015x.02.1.016.4 or Avaya Aura® SIP Enablement Services 5.2.1 software load SES-5.2.1.0-016.4

Description:

April 2, 2012 - Supplement 4 introduces Kernel Service Pack #5 for Communication Manager 5.2.1 and SIP Enablement Services 5.2.1 for Avaya S8xx0 Servers and the HP® ProLiant DL360 G7 server.

This kernel service pack, KERNEL-2.6.18-128.AV7i.tar.gz, applies to S8xx0 Servers and HP® ProLiant DL360 G7 servers running Communication Manager 5.2.1 (software load R015x.02.1.016.4) or SIP Enablement Services 5.2.1 (software load SES-5.2.1.0-016.4) only. This service pack is not applicable to any other servers, software loads, or releases of Communication Manager or SIP Enablement Services.

More specifically, this Kernel Service Pack does **NOT** apply to Communication Manager 5.2.1 and/or SIP Enablement Services 5.2.1 running on the Mid-sized Business Template (MBT).

Note that by design this kernel service pack can be installed on any supported S8xx0 or HP® ProLiant DL360 G7 server running the specified release and software load of Communication Manager or SIP Enablement services regardless of the kernel version running on the server.

June 20, 2011 – Supplement 3 introduced Kernel Service Pack #4 (KERNEL-2.6.18-128.AV7g.tar.gz) for Communication Manager 5.2.1 and SIP Enablement Services 5.2.1.

December 6, 2010 – Supplement 2 introduced Kernel Service Pack #3 (KERNEL-2.6.18-128.AV7d.tar.gz) for Communication Manager 5.2.1 and SIP Enablement Services 5.2.1.

April 5, 2010 – Supplement 1 introduced Kernel Service Pack #2 (KERNEL-2.6.18-128.AV7c.tar.gz) for Communication Manager 5.2.1 and SIP Enablement Services 5.2.1.

February 8, 2010 - The original PCN introduced Kernel Service Pack #1 (KERNEL-2.6.18-128.AV7b.tar.gz) for Communication Manager 5.2.1 and SIP Enablement Services 5.2.1. This was the first Kernel Service Pack for these releases.

To determine the release of Communication Manager software that is being run on a server you can:

- *execute the swversion* command from the bash shell
- launch the Communication Manager System Management Interface (CM-SMI) from a browser. From the top navigation bar select **Server (Maintenance)** under the **Administration** pull-down menu. Then select the **Software Version** page under the **Server** links on the left hand menu.
- *execute the list configuration software-versions* command from the SAT

	The release of SIP Enablement Services that is running on a server can be determined by running the *swversion* command from the bash shell.
Level of Risk/Severity Class 1=High Class 2=Medium Class 3=Low	Class 2
Is it required that this PCN be applied to my system?	This PCN is not required but is recommended for S8xx0 and HP® ProLiant DL360 G7 servers running Communication Manager 5.2.1 software load R015x.02.1.016.4 or SIP Enablement Services 5.2.1 software load SES-5.2.1.0-016.4.
The risk if this PCN is not installed:	The system will be exposed to the security vulnerabilities referenced in Section 1B and the issues described below in the section titled "**Release notes and workarounds are located:"**
Is this PCN for US customers, non-US customers, or both?	This applies to both US and non-US customers.
Does applying this PCN disrupt my service during installation?	This service pack will disrupt service in that it requires a full Linux reboot to take effect.
Installation of this PCN is required by:	Customer or Avaya Remote/On-Site Services or Avaya Authorized BusinessPartner. This service pack is customer installable and remotely installable.
Release notes and workarounds are located:	There are no release notes or workarounds. Kernel Service Packs resolve security vulnerabilities in the Linux operating system kernel used by Communication Manager 5.2.1 and SIP Enablement Services 5.2.1. These vulnerabilities are described by Avaya Security Advisories that are referenced in Section 1B – Security Information. The Avaya Security Advisories referenced in Section 1B can be viewed by performing the following steps from a browser: 1. Go to http://support.avaya.com 2. Click **More Resources** in the left hand navigation list 3. Click **Security Advisories** 4. Click **Security Advisories** for the year of interest. 5. Search for the ASA numbers referenced in Section 1B.

Kernel Service Packs are cumulative and all fixes in Kernel Service Packs #1 through #4 are included in Kernel Service Pack #5.

In addition, Kernel Service Pack #5 resolves the following issues which are not classified as security vulnerabilities:

Fixes delivered to Kernel Service Pack #2
(KERNEL-2.6.18-128.AV7c.tar.gz)

Problem	Keywords	Workaround
Services can now use Avaya's debugger on CM processes	093908	
Coredumps for CM processes that contain "duplicated" memory can now be read by gdb	100260	

Fixes delivered to Kernel Service Pack #3
(KERNEL-2.6.18-128.AV7d.tar.gz)

Problem	Keywords	Workaround
CM systems with CMM could reset due to a fixed semaphore deadlock in the interrupt thread of the cdc-acm modem driver	100689	

Fixes delivered to Kernel Service Pack #5
(KERNEL-2.6.18-128.AV7i.tar.gz)

Problem	Keywords	Workaround
RST socket kernel bug in tcp keepalive probe count can cause dropped calls.	113167	

Note that Kernel Service Pack #3 or greater can be used in place of and includes all the fixes in Kernel Patch KERNEL-2.6.18-128.7dt4.tar.gz which is specified in PCN 1690P.

What materials are required to implement this PCN (If PCN can be customer installed):

This PCN is being issued as a customer installable PCN. The kernel service pack KERNEL-2.6.18-128.AV7i.tar.gz is required. To obtain the kernel service pack, refer to the **How do I order this PCN section** below.

IMPORTANT – Installation of a kernel service pack is different than installation of traditional software updates on S8xx0 Series Servers or HP® ProLiant DL360 G7 Servers running Communication Manager and SIP Enablement Services, so the installation instructions must be followed carefully. Refer to the **Finding the installation instructions** section of this PCN.

How do I order this PCN (If PCN can be customer installed):

The kernel service pack KERNEL-2.6.18-128.AV7i.tar.gz can be obtained by performing the following steps from a browser:

1. Go to http://support.avaya.com and click **sign in** then enter your login information
2. Click **Downloads** in the left hand navigation list
3. Begin to type **Communication Manager** in the Product Name field of the pop-up window and when **Avaya Aura™ Communication Manager** appears as a selection below, select it. If instead the A-Z List is clicked in the pop-up window and **Avaya Aura™ Communication Manger** is selected, you will once again need to click **Downloads** in the left hand navigation list.

4. Click on **Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates**
5. Scroll down to the table titled **Kernel Service Packs for Communication Manager and SIP Enablement Services** and click on GA load **016.4** in the **Avaya Aura Communication Manager 5.2.1 / SIP Enablement Services 5.2.1** Release row.
6. You are currently viewing the content of the Summary tab. Click on the **Downloads** tab at the top of the screen.
7. Click on the link titled **KERNEL-2.6.18-128.AV7i.tar.gz**

The kernel service pack KERNEL-2.6.18-128.AV7i.tar.gz is also available on the download pages for the following products: Communication Manager, SIP Enablement Services, S8300 Server, S8400 Server, S8500 Server, S8510 Server, S8710 Server, S8720 Server, S8730 Server, S8800 Server and Avaya Common Servers (HP DL360 G7 Server). Select 5.2.x in the release pull-down menu or release 1.0.x for Common Servers.

The MD5 sum for the kernel service pack is:
a94dedddf616bf0b372a689fbb254b6e

Finding the installation instructions (If PCN can be customer installed):

This PCN is being issued as a customer installable PCN. The instructions for installing a Kernel Service Pack are in the document titled "Avaya Aura™ Communication Manager Change Description for Release 5.2.1." This document can be obtained by performing the following steps from a browser:

1. Go to http://support.avaya.com and click **Documentation** in the left hand navigation list
2. Click **Administration & System Programming**
3. Select **Avaya Aura® Communication Manager** from the A-Z list (under "A").
4. Select 5.2.1 in the release pull down menu if necessary
5. Click on the link for "Avaya Aura™ Communication Manager Change Description for Release 5.2.1."
6. In **Chapter 1: Communication Manager Changes** find the section titled Kernel Replacement.

Note that:

1. Kernel service packs are independent of all other Communication Manager or SIP Enablement Services software updates activated on a server including service packs, security service packs, stand alone patches or custom patches. None of these other software updates should be deactivated before installing a kernel service pack.
2. Kernel service packs are cumulative for the release they apply to. In other words the current kernel service pack for a release will include the fixes from all previous kernel service packs for that release.
3. Software Update Manager (SUM) supports installation of kernel service packs for Communication Manager 5.2.1 and SIP Enablement Services 5.2.1.
4. It is not necessary to deactivate an existing kernel service pack installed on a server before activating a new kernel service pack. Doing so will result in a second unnecessary server reboot.
5. **Important** - An automatic server reboot will occur about one minute after successful activation of a kernel service pack. Wait at least five minutes for the server reboot to complete and for all Communication Manager processes to restart before committing the Kernel Service Pack. Use the following procedure to verify the reboot has completed successfully and to commit the Kernel Service Pack:

- Start the CM-SMI and under the **Administration** menu select **Server (Maintenance)**
- Select **Server > Process Status -** The system displays the default settings for the output of the process status report
- Select **View -** The system displays the process status results
- Verify that all processes show "UP" before returning to the CM-SMI **Manage Updates** page and clicking **continue**
- If the Kernel Service Pack you want to activate shows Pending_Commit in the Status column, select the file (radio button) and click **Commit**.

SECTION 1A – SOFTWARE SERVICE PACK INFORMATION

Note: Customers are required to backup their systems before applying the Service Pack.

How to verify the installation of the Service Pack has been successful:

Refer to the Kernel Replacement instructions in the "Avaya Aura™ Communication Manager Change Description for Release 5.2.1" referenced above.

What you should do if the Service Pack installation fails?

Escalate to Avaya **Global Support Services (GSS)** or an Avaya authorized Business Partner.

How to remove the Service Pack if malfunction of your system occurs:

After the kernel service pack installation is complete (the update is committed) you can deactivate it using the following method. Note that a full Linux reboot will be required to completely deactivate the changes after which the server will be running on the original Linux kernel installed with Communication Manager 5.2.1 or SIP Enablement Services 5.2.1:

Run the following bash command on the Server:
> update_deactivate KERNEL-2.6.18-128.AV7i

The system will display a warning that a server reboot is required to deactivate the update. Enter "y" to continue.

After the reboot is complete run the following bash command on the Server:
> update_show
This should show the status of kernel service pack (Update ID)
"KERNEL-2.6.18-128.AV7i" as "pending_deactivate".

Run the following bash command to commit the deactivation:
> update_commit KERNEL-2.6.18-128.AV7i

*Note - If you do not run the update_commit command within ten minutes of the server reboot, a minor platform alarm is generated.

>update_show
This should show the status of kernel service pack (Update ID) "KERNEL-2.6.18-128.AV7i" as "unpacked".

SECTION 1B – SECURITY INFORMATION

Are there any security risks involved?

Issues described by Avaya Security Advisories referenced in the following section are corrected by Kernel Service Pack #5 (KERNEL-2.6.18-128.AV7i.tar.gz).

Avaya Security Vulnerability Classification:

Note: A Classification of None in the tables below means either:
a. the affected components are installed, but the vulnerability is not exploitable, or
b. the components are not installed.

Kernel Service Packs are cumulative and all fixes in Kernel Service Packs #1 through #4 are included in Kernel Service Pack #5.

Security Vulnerabilities Resolved in Kernel Service Pack #1
(KERNEL-2.6.18-128.AV7b.tar.gz)

ASA Number	Communication Manager 5.2.x	SIP Enablement Services 5.2.x
ASA-2009-409	Low	Low
ASA-2009-502	Medium	Medium
ASA-2010-001	Low	Low
ASA-2010-012	Medium	Medium

Security Vulnerabilities Resolved in Kernel Service Pack #2
(KERNEL-2.6.18-128.AV7c.tar.gz)

ASA Number	Communication Manager 5.2.x	SIP Enablement Services 5.2.x
ASA-2010-026	Medium	Medium

Security Vulnerabilities Resolved in Kernel Service Pack #3
(KERNEL-2.6.18-128.AV7d.tar.gz)

ASA Number	Communication Manager 5.2.x	SIP Enablement Services 5.2.x
ASA-2010-122	Low	None
ASA-2010-130	Low	None
ASA-2010-144	Low	None
ASA-2010-186	Low	Medium

Security Vulnerabilities Resolved in Kernel Service Pack #4
(KERNEL-2.6.18-128.AV7g.tar.gz)

ASA Number	Communication Manager 5.2.x	SIP Enablement Services 5.2.x
ASA-2010-291	Low	None
ASA-2010-372	Low	None
ASA-2011-046	Low	None

ASA-2011-086	Low	None
ASA-2011-089	Medium	None

Security Vulnerabilities Resolved in Kernel Service Pack #5
(KERNEL-2.6.18-128.AV7i.tar.gz)

ASA Number	Communication Manager 5.2.x	SIP Enablement Services 5.2.x
ASA-2011-166	Low	None
ASA-2011-208	Low	None
ASA-2011-238	Low	None

Mitigation: Apply Kernel Service Pack KERNEL-2.6.18-128.AV7i.tar.gz to S8xx0 Servers and HP® ProLiant DL360 G7 Servers running Communication Manager 5.2.1 or SIP Enablement Services 5.2.1.

SECTION 1C – ENTITLEMENTS AND CONTACTS

Material Coverage Entitlements: There is no incremental charge for the material in this PCN. The software updates are available on support.avaya.com.

Avaya Customer Service Coverage Entitlements: Avaya is issuing this PCN as installable by the customer. If the customer requests Avaya to install this PCN, it is considered a billable event as outlined in Section 4 (*Software Updates and Product Correction Notices*) of the Avaya Service Agreement Supplement (Full Maintenance Coverage) unless the customer has purchased an Avaya Services enhanced offer such as the Avaya Services Product Correction Support offer.

Additionally, Avaya on-site support is not included. If on-site support is requested, Avaya will bill the customer current Per Incident charges unless the customer has purchased an Avaya Services enhanced offer such as the Avaya Services Product Correction Support offer.

Customers under the following Avaya coverage: -Full Coverage Service Contract* -On-site Hardware Maintenance Contract*	
Remote Installation	Current Per Incident Rates Apply
Remote or On-site Services Labor	Current Per Incident Rates Apply

- Service contracts that include both labor and parts support – 24x7, 8x5.

Customers under the following Avaya coverage: -Warranty -Software Support -Software Support Plus Upgrades -Remote Only -Parts Plus Remote -Remote Hardware Support -Remote Hardware Support w/ Advance Parts Replacement

Help-Line Assistance	Per Terms of Services Contract or coverage
Remote or On-site Services Labor	Per Terms of Services Contract or coverage

Avaya Product Correction Notice Support Offer
The Avaya Product Correction Support Offer provides out-of-hours support for remote and on-site technician installable PCNs, and Avaya installation for all Avaya issued PCNs that are classified as "Customer-Installable". Refer to the PCN Offer or contact your Avaya Account Representative for complete details.

Avaya Authorized Partner Service Coverage Entitlements:

Avaya Authorized Partner
Avaya Authorized Partners are responsible for the implementation of this PCN on behalf of their customers.

Avaya Contacts: For assistance with this PCN contact your local or regional Service group.

Refer to the Global Support Services – Support Directory at the following link:
http://support.avaya.com/directories