

Product Correction Notice (PCN)

Issue Date: February 8, 2010
Archive Date: NA
PCN Number: 1712P

SECTION 1 - CUSTOMER NOTICE

This PCN address issues with the following products and systems:

Avaya S8300C, S8500B, S8500C and S8730 Servers running Communication Manager 4.0.5 software load R014x.00.5.742.0, or SIP Enablement Services 4.0.2 software load SES04.0.2-04.0.036.0

Does this PCN apply to me?

PCN 1712P introduces **Kernel Service Pack #1** for Communication Manager 4.0.5 and SIP Enablement Services 4.0.2 for Avaya S8300C, S8500B, S8500C and S8730 Servers.

This kernel service pack, KERNEL-2.6.11-AV18m.tar.gz, applies to S8300C, S8500B, S8500C and S8730 Servers running Communication Manager 4.0.5 (software load R014x.00.5.742.0) or SIP Enablement Services 4.0.2 (software load SES04.0.2-04.0.036.0) only. This service pack is not applicable to any other software loads, or releases of Communication Manager or SIP Enablement Services.

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

Kernel service pack KERNEL-2.6.11-AV18m.tar.gz is recommended for S8300C, S8500B, S8500C and S8730 since it fixes a driver used only by these servers. Other servers supported by Communication Manager 4.0.5 and SIP Enablement Services 4.0.2 do not use this driver.

This is the first Kernel Service Pack for Communication Manager 4.0.5 and SIP Enablement Services 4.0.2.

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
- Check the Software Version page under the Server section of the Maintenance Web Interface.
- *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.

What you should do when you receive this PCN:

You should install the specified Communication Manager 4.0.5 / SIP Enablement Services 4.0.2 kernel service pack on all S8300C, S8500B, S8500C and S8730 Servers running the specified loads of Communication Manager or SIP Enablement Services.

Description of PCN:	This notice specifies Communication Manager 4.0.5 / SIP Enablement Services 4.0.2 Kernel Service Pack KERNEL-2.6.11-AV18m.tar.gz and Software Update Procedures. This kernel service pack should be installed on all S8300C, S8500B, S8500C and S8730 Servers running the specified load of Communication Manager 4.0.5 or SIP Enablement Services 4.0.2.
What is the nature of the PCN?	Communication Manager 4.0.5 / SIP Enablement Services 4.0.2 Kernel Service Pack number 1 for Avaya S8300C, S8500B, S8500C and S8730 Servers.
This PCN addresses and resolves the following issues:	Kernel Service Pack KERNEL-2.6.11-AV18m.tar.gz resolves security vulnerabilities in the Linux operating system kernels used by Communication Manager 4.0.5 and SIP Enablement Services 4.0.2. Each of these vulnerabilities are described by Avaya Security Advisories that are referenced in Section 1B – Security Information.
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 highly recommended for S8300C, S8500B, S8500C and S8730 Servers running Communication Manager 4.0.5 software load R014x.00.5.742.0 or SIP Enablement Services 4.0.2 software load SES04.0.2-04.0.036.0.
The risk if this PCN is not installed:	The system will be exposed to the vulnerabilities referenced in Section 1B.
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?	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 Authorized Service Provider. This service pack is customer installable and remotely installable.
Release notes and workarounds are located:	There are no release notes or workarounds. The Avaya Security Advisories referenced in Section 1B can be reviewed 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 2010 5. Search for the ASA numbers referenced in Section 1B.

How to determine if your product is affected:

All S8300C, S8500B, S8500C and S8730 Servers running Communication Manager 4.0.5 software load R014x.00.5.742.0 or SIP Enablement Services 4.0.2 software load SES04.0.2-04.0.036.0 are affected.

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
- Check the Software Version page under the Server section of the Maintenance Web Interface.
- *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.

**Required materials
(If PCN can be
customer installed):**

This PCN is being issued as a customer installable PCN. The kernel service pack KERNEL-2.6.11-AV18m.tar.gz is required. To obtain the kernel service pack refer to the **Provisioning Instructions** section of this PCN.

IMPORTANT – Installation of a Kernel Service Pack is different than installation of traditional software updates on S8xx0 Series Servers running Communication Manager or SIP Enablement Services, so the installation instructions must be followed carefully. Refer to the **Finding the installation instructions** section of this PCN.

**Provisioning instructions
(If PCN can be
customer installed):**

The kernel service pack KERNEL-2.6.11-AV18m.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
6. Click **Downloads** in the left hand navigation list
7. Begin to type **Communication Manager** in the Product Name field of the pop-up window and when it appears as a selection below, select it. If instead the A-Z List is clicked in the pop-up window and Communication Manger is selected, you will once again need to click **Downloads** in the left hand navigation list.
8. Click on **Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates**
9. Scroll down to the table titled **Kernel Service Packs for Communication Manager and SIP Enablement Services** and click on GA load **742.0** in the **Communication Manager 4.0.5 / SIP Enablement Services 4.0.2** Release row.
10. You are currently viewing the content of the Summary tab. Click on the **Downloads** tab at the top of the screen.
11. Click on the link titled **KERNEL-2.6.11-AV18m.tar.gz**

The kernel service pack KERNEL-2.6.11-AV18m.tar.gz is also available on the download pages for the following products: Communication Manager, SIP Enablement Services, S8300 Server, S8500 Server and S8730 Server. Select 4.0.x in the release pull-down menu.

The MD5 sum for the kernel service pack is:
2466279e11e4250e86bbd11e3ef15e19

**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 included in the Communication Manager 4.0.5 Release Notes document. 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 **Release Notes & Software Update Notes**
3. Select **Communication Manager** from the A-Z list
4. Select **4.0.x** in the release pull down menu
5. Click on the link for **Communication Manager 4.0.5 Release Notes**

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. SIP Enablement Services 4.0.2 only supports installation of kernel service packs using Linux commands.
4. Software Update Manager (SUM) does not support installation of kernel service packs for Communication Manager 4.0.5 or SIP Enablement Services 4.0.2.
5. 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.
6. **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:
 - a. Launch the Maintenance Web Interface and under the **Server** menu select **Process Status**
 - b. The system displays the default settings for the output of the process status report
 - c. Select **View**
 - d. The system displays the process status results
 - e. Verify that all processes show "UP" before returning to the **Manage Updates** page and clicking **continue**
 - f. If the Kernel Service Pack you want to activate shows Pending_Commit in the Status column, select the file (radio button) and click **Commit**.

When using Linux commands to activate the Kernel Service Pack use the *statapp* command after the reboot to verify that all

SECTION 1A – PATCH INFORMATION

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

How to verify the installation of the patch has been successful:

Refer to the Kernel Replacement instructions in the Communication Manager 4.0.5 Release Notes referenced above.

What you should do if the patch installation fails?

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

How to remove the patch 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 4.0.5 or SIP Enablement Services 4.0.2:

Run the following bash command on the Media Server:
> update_deactivate KERNEL-2.6.11-AV18m

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

Wait 5 minutes for the reboot to complete then run the *statapp* command to insure all applications are up before proceeding.

Run the following bash command on the Media Server:
> update_show
This should show the status of kernel service pack (Update ID) "KERNEL-2.6.11-AV18m" as "pending_deactivate".

Run the following bash command to commit the deactivation:
> update_commit KERNEL-2.6.11-AV18m

*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-2.6.11-AV18m" as "unpacked".

SECTION 1B – SECURITY INFORMATION

Are there any security risks involved?

Avaya Security Advisory ASA-2010-0020 for the Intel PRO/1000 Linux Driver is corrected in KERNEL-2.6.11-AV18m.tar.gz.

Avaya Security Vulnerability Classification:

ASA Number	Communication Manager	SIP Enablement Services
ASA-2010-20	Medium	Medium

Mitigation: Apply Kernel Service Pack KERNEL-2.6.11-AV18m.tar.gz to S8300C, S8500B, S8500C and S8730 servers running Communication Manager 4.0.5 or SIP Enablement Services 4.0.2.

Material Coverage Entitlements:

There is no incremental charge for the material in this PCN. The service pack is available on support.avaya.com. The file is available during the warranty period or if a valid maintenance contract is in force.

Avaya Customer Service Coverage Entitlements:

Avaya is issuing this PCN as remotely 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:	
-Warranty -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:	
-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 the Terms of the Service Contract
Remote or On-site Services Labor	Per the Terms of the Service Contract

Per Incident Customer (No Avaya Warranty or Avaya Service Contract)	
Help-Line Assistance	Current Per Incident Rates Apply
Remote or On-site Services Labor	Current Per Incident Rates Apply

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
BusinessPartner
Service Coverage
Entitlements:**

Authorized BusinessPartner

Avaya authorized BusinessPartners are responsible for the implementation of this PCN on behalf of their customers. Any support or work performed by Avaya may result in Per Incident charges.

Avaya Contact List:

Avaya Contact	Telephone Number
Global Support Services (GSS)	800 – 242 - 2121
Canada Customer Care Center	800 – 387 - 4268
Remote Service Center – Hungary	361 - 345 - 4334
Caribbean and Latin America	786 – 331 - 0860
EMEA Services - Post Sales Technical Support	31-70-414-8720
Asia/Pacific Regional Support Center	+800-2-28292-78 / +65 6872 5141 and +008006501243 (India)

© 2010 Avaya Inc. All Rights Reserved. All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.
