

Product Correction Notice (PCN)

Issue Date: 10-DEC-2010
Supplement 5 Date: 11-August-2014
Archive Date: NA
PCN Number: 1719S

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: **11 August 2014** – Supplement 5 introduces Security Service Pack #5 (PLAT-rhel4-1015.tar.gz) for 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.

This Security Service Pack also applies to Communication Manager 5.2.1 or SIP Enablement Services 5.2.1 running as virtual machines on Midsize Business Template 5.2.1 (MBT).

This service pack is not applicable to any other servers, software loads, or releases of Communication Manager or SIP Enablement Services.

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.

1 April 2013 – Supplement 4 introduced Security Service Pack #4 (PLAT-rhel4-1014.tar.gz) for 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.

2 April 2012 – Supplement 3 introduced Security Service Pack #3 (PLAT-rhel4-1013.tar.gz) for S8xx0 Servers and the HP ProLiant DL360 G7 servers running Communication Manager 5.2.1 or SIP Enablement Services 5.2.1.

20 June 2011 – Supplement 2 introduced Security Service Pack #2 (PLAT-rhel4-1012.tar.gz) for S8xx0 Servers and the HP ProLiant DL360 G7 servers running Communication Manager 5.2.1 or SIP Enablement Services 5.2.1.

21 February 2011 – Supplement 1 extended support of Security Service Pack #1 (PLAT-rhel4-1010.tar.gz) to SIP Enablement Services 5.2.1 software load SES-5.2.1.0-016.4 and added precautions to the section titled **Finding the installation instructions (If PCN can be customer installed)**

10 December 2010 – The original PCN introduced Security Service Pack #1 (PLAT-rhel4-1010.tar.gz) for S8xx0 Servers and the HP ProLiant DL360 G7 servers running Communication Manager 5.2.1.

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.
Is this PCN for US customers, non-US customers, or both?	This PCN 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 Authorized Service Provider. This service pack is customer installable and remotely installable.
Release notes and workarounds are located:	<p>The Security Service Pack resolves vulnerabilities described by the Avaya Security Advisories 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:</p> <ol style="list-style-type: none"> 1. Go to http://support.avaya.com and login. 2. Scroll to the bottom of the page and click on Policies & Legal under the HELP & POLICIES menu. 3. Click Security Advisories 4. Click Security Advisories for 20xx (the year of interest) and Search for the ASA numbers referenced in Section 1B.
What materials are required to implement this	This PCN is being issued as a customer installable PCN. The Security Service Pack PLAT-rhel4-1015.tar.gz is required. To obtain the Security Service Pack, refer to the How do I order this PCN section below.

PCN
(If PCN can be
customer
installed):

IMPORTANT – Some installation steps are different for this update compared to traditional software updates. These differences are explained in the **Finding the installation instructions** section of this PCN.

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

The Security Service Pack PLAT-rhel4-1015.tar.gz can be obtained by performing the following steps from a browser:

1. Go to <http://support.avaya.com> then enter your **Username** and **Password** and click **LOG IN**.
2. Click **DOWNLOADS** at the top of the page.
3. Begin to type **Communication Manager** in the **Enter Product Name** box and when Avaya Aura® Communication Manager appears as a selection below, select it.
4. Select 5.2.x from the **Choose Release** pull down menu to the right.
5. Scroll down (may have to page down) and Click on **Avaya Aura Communication Manager 5.2.1 / SIP Enablement Services 5.2.1 Security Service Pack 5**.
6. Scroll down the page to find the download link for **PLAT-rhel4-1015.tar.gz**. This link will take you to the PLDS system with the **Download pub ID** already entered.

The Security Service Pack PLAT-rhel4-1015.tar.gz is also available on the download pages for the following products: Communication Manager, SIP Enablement Services, Midsize Business Template, S8300 Server, S8400 Server, S8500 Server, S8510 Server, S8710 Server, S8720 Server, S8730 Server, S8800 Server and Common Servers (HP DL360 G7 server). Select 5.2.x in the release pull-down menu or 1.0.x for Common Servers.

The service pack can also be downloaded directly from the PLDS system at <http://plds.avaya.com>.

1. Enter your login ID and password. You may have to search for and enter your company name and/or accept the one time EULA to gain access to software downloads.
2. Click **View Downloads**.
3. In the **Search by Download** tab enter **CM000000587** in the **Download pub ID:** search field to access the Communication Manager Security service pack download (PLAT-rhel4-1015.tar). Click the **Download** link to begin the download.

Hint: In the PLDS **View Downloads** section under the **Suggested Downloads** tab, select **Communication Manager** in the **Product Line** search field to display recent Communication Manager software, including service packs.

Previous Communication Manager 5.2.1 Service Packs and System Platform updates are also available on PLDS. In the PLDS **View Downloads** section under the **Search by Download** tab, select **Communication Manager** in the **Application** search field and **Version 5.2.1** to display all available Communication Manager 5.2.1 software downloads.

The MD5 sums for the Security service pack are:

PLAT-rhel4-1015.tar.gz: bd4f431e1cba30553d1de54b1bb688e6

PLAT-rhel4-1014.tar.gz: d39be7860113267ce7124ef7692c3662

Finding the
installation
instructions

This PCN is being issued as a customer installable PCN. The instructions for installing this Communication Manager security service pack can be obtained by performing the following steps from a browser. See the notes below for deviations from the standard installation instructions:

(If PCN can be
customer
installed):

1. Go to <http://support.avaya.com> then enter your **Username** and **Password** and click **LOG IN**.
2. Click **DOWNLOADS** at the top of the page.
3. Begin to type **Communication Manager** in the **Enter Product Name** box and when Avaya Aura® Communication Manager appears as a selection below, select it.
4. Select 5.2.x from the **Choose Release** pull down menu to the right.
5. In the **DOWNLOADS** table (may have to page down) find and Click on **Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates, 5.2.x**.
6. Click on **Communication Manager 2.0 and Later Software Update Procedures** to access detailed command line instructions on how to install the service pack. Use the appropriate non-call preserving procedures (for either simplex or duplex servers).

Important Installation Notes:

1. Security Service Packs are independent of other Communication Manager software updates activated on a server including service packs, kernel service packs, stand-alone patches or custom patches. None of these other software updates should be deactivated before installing a Security Service Pack.
2. Security Service Packs are cumulative for the release they apply to. In other words the current Security Service Pack for a release will include the fixes from all previous Security Service Packs for that release.
3. The previous Security Service Pack must be deactivated before activating a new Security Service Pack.
4. Before activating the Security Service Pack, check that the system has network connectivity to all configured Network Time Protocol (NTP) servers by checking the System Management Interface Web page "Configure Time Server" under "Configure Server". If the system can ping the IP address or hostname of all NTP servers configured on this page, Security Service Pack PLAT-rhel4-1015 may be activated. The system will reboot automatically shortly after activation is successful (see below).
5. If the system cannot reach the IP address or hostname for an NTP server, remove it from the NTP configuration. After removing any unreachable NTP servers, activate Security Service Pack PLAT-rhel4-1015. The system will reboot automatically shortly after activation is successful. If desired, previously removed NTP servers may be re-added to the NTP configuration after the system has rebooted.
6. If patch PLAT-rhel4-1015 fails to activate despite performing these steps, escalate to Avaya Global Support Services.
7. **Important** - An automatic server reboot will occur after successful activation of a Security Service Pack. The activation steps for a Security Service Pack are:
 - Run the following bash command on the server:
> `update_unpack PLAT-rhel4-1015`
> `update_activate PLAT-rhel4-1015`
 - Enter "y" to confirm automatic reboot NOTE: If using the CM_SMI Manage Updates web page to activate the Security Service Pack you are only warned of the reboot if the server has Communication Manager 5.2.1 SP #6 (18576) or greater activated at the time.
 - After successful activation of the Security Service Pack the server will automatically do a full Linux reboot in about 2 minutes.

- After the reboot nothing else needs to be done, the Security Service Pack will be fully activated and in use by the server.

On Midsize Business Template, CM and SES patches are applied via the System Platform Web Console Patch Management capability. Patch installation instructions for Midsize Business Template can be obtained by performing the following steps from a browser:

1. Go to <http://support.avaya.com> then enter your **Username** and **Password** and click **LOG IN**.
2. Click **DOCUMENTS** at the top of the page
3. Begin to type **Midsize Business** in the **Enter Your Product Here** box and when Midsize Business Template appears as a selection below, select it.
4. Check the box for **Administration & System Programming**.
5. Click **ENTER**.
6. Click on the document titled **Administering Avaya Midsize Business Template**.
7. See the **Server Management: Managing patches** section in Chapter 1.

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:

To verify the service pack is successfully installed using the Communication Manager System Management Interface web pages perform the following steps from a web browser:

- Access the Communication Manager System Management Interface web pages by entering the Server name or IP address in the browser Address box.
- Login to the web pages.
- 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.
- Verify that under "UPDATES:" service pack "PLAT-rhel4-1015" shows "activated."

Or, using the Communication Manager Command Line Interface run the following bash command:

```
> update_show
```

This should show the status of service pack (Update ID)

"PLAT-rhel4-1015" as "activated."

On Midsize Business Templates systems access the **Server Management > Patch Management** page which should show the status of the patch as "active."

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

Although Security Service Pack PLAT-rhel4-1015 can be deactivated, the updates that it installs will still

the Service Pack if malfunction of your system occurs:

be in use by the server and cannot be removed or backed out to the previous versions.

SECTION 1B – SECURITY INFORMATION

Are there any security risks involved?

Issues described by the Avaya Security Advisories listed in the next section are corrected by Security Service Pack #5 (PLAT-rhel4-1015.tar.gz).

The Avaya Security Advisories (ASA) can be referenced by following the steps outlined in the “**Release notes and workarounds**” portion of Section 1 of this PCN.

Avaya Security Vulnerability Classification:

Note: A Classification of None in the tables below means the affected components are installed, but the vulnerability is not exploitable. In this case the fix is included in the service pack anyway.

Security Vulnerabilities Resolved in Security Service Pack 1 (PLAT-rhel4-1010.tar.gz)

ASA Number	Communication Manager 5.2.x Classification	SIP Enablement Services 5.2.x Classification
ASA-2009-476	Low	Low
ASA-2009-497	Low	Low
ASA-2009-591	Low	Low
ASA-2010-003	Low	Low
ASA-2010-004	Low	Low
ASA-2010-090	Low	Low
ASA-2010-110	None	None
ASA-2010-116	Low	Low
ASA-2010-117	None	None
ASA-2010-118	None	None
ASA-2010-127	None	None
ASA-2010-133	Low	Low
ASA-2010-134	None	None
ASA-2010-160	Low	Low
ASA-2010-176	Low	None
ASA-2010-260	Low	None
ASA-2010-306	Low	Low

Security Vulnerabilities Resolved in Security Service Pack 2 (PLAT-rhel4-1012.tar.gz)

ASA Number	Communication Manager 5.2.x Classification	SIP Enablement Services 5.2.x Classification
ASA-2010-373	Low	Low
ASA-2010-374	Low	Low
ASA-2011-003	Low	Low

ASA-2011-005	Low	None
ASA-2011-010	Low	Low
ASA-2011-058	Low	Low
ASA-2011-087	Low	Low
ASA-2011-113	Low	Low
ASA-2011-117	Low	Low
ASA-2011-118	None	None
ASA-2010-154	Medium	Low

Security Vulnerabilities Resolved in Security Service Pack 3

(PLAT-rhel4-1013.tar.gz)

ASA Number	Communication Manager 5.2.x Classification	SIP Enablement Services 5.2.x Classification
ASA-2011-197	Low	Low
ASA-2011-274	Low	Low
ASA-2011-281	Low	Low
ASA-2011-353	Low	Low
ASA-2011-355	Low	Low

Security Vulnerabilities Resolved in Security Service Pack 4

(PLAT-rhel4-1014.tar.gz)

ASA Number	Communication Manager 5.2.x Classification	SIP Enablement Services 5.2.x Classification
ASA-2012-005	None	None
ASA-2012-043	Low	Low
ASA-2012-068	Low	Low
ASA-2012-094	Low	Low
ASA-2012-126	None	None
ASA-2012-155	Low	Low
ASA-2012-231	Low	Low
ASA-2012-239	Low	None
ASA-2012-247	Low	Low
ASA-2012-298	Low	None
ASA-2012-311	None	None
ASA-2012-428	None	None

Security Vulnerabilities Resolved in Security Service Pack 5

(PLAT-rhel4-1015.tar.gz)

ASA Number	Communication Manager 5.2.x Classification	SIP Enablement Services 5.2.x Classification
ASA-2014-268	Medium	Medium

Mitigation: Apply Security Service Pack PLAT-rhel4-1015.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 and from plds.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.

**Who to contact
for more
information:**

If you require further information or assistance please contact your Authorized Service Provider, or visit support.avaya.com. There you can access more product information, chat with an Agent, or open an online Service Request. Support is provided per your warranty or service contract terms unless otherwise specified in the Avaya support [Terms of Use](#).