Product Correction Notice (PCN)

Issue Date:	**05-August-2013**
Supplement 4 Date:	**22-December-2014**
Archive Date:	**NA**
PCN Number:	**1921S**

SECTION 1 - CUSTOMER NOTICE

Products affected by this PCN:	Avaya Aura® Communication Manager 6.3 Solution Templates running on System Platform R6.3 equipped S8300D, S8510, S8800 and Common Servers (HP® DL360 G7 and Dell® R610 Servers, plus the newly released HP® DL360 G8, and Dell® R620 Servers). Avaya Aura® Communication Manager 6.3 Simplex VAppliance and Duplex VAppliance running on VMware® vSphere® ESXi 5.0/5.1/5.5 infrastructures.
Description:	**22 December 2014 –** Supplement 4 of this PCN introduces Security Service Pack #5 (PLAT-rhel5.3-3018.tar) for System Platform R6.3 equipped S8300D, S8510, S8800 and Common Servers (HP® DL360 G7 and Dell® R610 Servers, plus the newly released HP® DL360 G8 and Dell® R620 Servers) running Communication Manager 6.3 software load R016x.03.0.124.0. This Security Service Pack #5 also applies to Avaya Aura® Communication Manager 6.3 Simplex VAppliance and Duplex VAppliance running on VMware® vSphere® ESXi 5.0/5.1/5.5 infrastructures with Communication Manager 6.3 software load R016x.03.0.124.0. **4 August 2014 –** Supplement 3 of this PCN introduced Security Service Pack #4 (PLAT-rhel5.3-3016.tar) for System Platform R6.3 equipped S8300D, S8510, S8800 and Common Servers (HP® DL360 G7 and Dell® R610 Servers, plus the newly released HP® DL360 G8 and Dell® R620 Servers) running Communication Manager 6.3 software load R016x.03.0.124.0. This Security Service Pack #4 also applied to Avaya Aura® Communication Manager 6.3 Simplex VAppliance and Duplex VAppliance running on VMware® vSphere® ESXi 5.0/5.1/5.5 infrastructures with Communication Manager 6.3 software load R016x.03.0.124.0. **2 June 2014 – Supplement 2 of** this PCN introduced Security Service Pack #3 (PLAT-rhel5.3-3014.tar) for System Platform R6.3 equipped S8300D, S8510, S8800 and Common Servers (HP® DL360 G7 and Dell® R610 Servers, plus the newly released HP® DL360 G8 and Dell® R620 Servers) running Communication Manager 6.3 software load R016x.03.0.124.0. This Security Service Pack #3 also applied to Avaya Aura® Communication Manager 6.3 Simplex VAppliance and Duplex VAppliance running on VMware® vSphere® ESXi 5.0/5.1/5.5 infrastructures with Communication Manager 6.3 software load R016x.03.0.124.0. **7 October 2013 – Supplement 1 of** this PCN introduced Security Service Pack #2 (PLAT-rhel5.3-3011.tar) for System Platform R6.3 equipped S8300D, S8510, S8800 and Common Servers (HP® DL360 G7 and Dell® R610 Servers, plus the newly released HP® DL360 G8 and Dell® R620 Servers) running Communication Manager 6.3 software load R016x.03.0.124.0.

	This Security Service Pack #2 also applied to Avaya Aura® Communication Manager 6.3 Simplex VAppliance and Duplex VAppliance running on VMware® vSphere® ESXi 5.0/5.1 infrastructures with Communication Manager 6.3 software load R016x.03.0.124.0. **5 August 2013 –** This PCN introduced Security Service Pack #1 (PLAT-rhel5.3-3010.tar) for System Platform R6.3 equipped S8300D, S8510, S8800 and Common Servers (HP® DL360 G7 and Dell® R610 Servers) running Communication Manager 6.3 software load R016x.03.0.124.0. This Security Service Pack #1 also applied to Avaya Aura® Communication Manager 6.3 Simplex VAppliance and Duplex VAppliance running on VMware® vSphere® ESXi 5.0/5.1 infrastructures with Communication Manager 6.3 software load R016x.03.0.124.0.
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.
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 since it requires a full Linux reboot of the Communication Manager Virtual Machine (VM) 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	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

workarounds are located:	viewed by performing the following steps from a browser:

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.

In addition to the Avaya Security Advisories referenced in Section 1B, the follow problems were also corrected in this update(fixes are cumulative):

Other Problems Resolved in Security Service Pack 2
(PLAT-rhel5.3-3011.tar)

Problem	Keywords
LDAP connections to Communication Manager from System Platform or from a customer LDAP server were severed after updating the system packages in a previous security service pack. The resulting condition caused LDAP logins to fail.	131931
Locale information necessary for Avaya Aura Messaging was unlinked after updating system packages in a previous security service pack. The resulting condition could make adding new users fail.	131948

Other Problems Resolved in Security Service Pack 3
(PLAT-rhel5.3-3014.tar)

Problem	Keywords
On System Platform based machines, Security Service Pack PLAT-rhel5.3-3011 introduced an issue that prevented console access to Avaya Aura Communication Manager from System Platform. SSH and System Management Interface connections still worked correctly.	140688

Other Problems Resolved in Security Service Pack 4
(PLAT-rhel5.3-3016.tar)

Problem	Keywords
Logging could fail after installing security service pack PLAT-rhel5.3-3014 due to log rotation failures.	141030
Logging could fail for systems with CMM 6.3 SP2 or later, or AAM 6.3 or later due to localhost mailbox rotation failures.	141057

Other Problems Resolved in Security Service Pack 5
(PLAT-rhel5.3-3018.tar)

Problem	Keywords
Communication Manager now supports the new Russian Time Zone changes from October, 2014.	141383 141600
The bash shellshock fix for ASA-2014-392 could cause issues with the scheduled tasks provided by the 'at' daemon. This could lead to situations that prevent security and kernel service packs from becoming completely activated.	141466
TLSv1 is the only available protocol for accessing the System Management Interface (SMI) web pages. Very old web browsers may not be able to handle TLSv1 - if you experience issues, please update your web browser to a modern version and try again before contacting support.	141470
The postfix mail transport agent has been updated for bug fixes provided by the upstream Red Hat distribution.	141486 141601

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 Security Service Pack PLAT-rhel5.3-3018.tar is required. To obtain the Security Service Pack, refer to the **How do I order this PCN** section below.

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 service pack can be downloaded 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 6.3.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 6.3 Security Service Pack 5, 6.3.x**.
6. Scroll down the page to find the download link for **PLAT-rhel5.3-3018.tar**. This link will take you to the PLDS system with the **Download pub ID** already entered.

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 **CM000000407** in the **Download pub ID:** search field to access the Communication Manager Security service pack download (PLAT-rhel5.3-3018.tar). Click the **Download** link to begin the download.

PLDS Hints:

1. In the PLDS **View Downloads** section under the **Suggested Downloads** tab, select **Communication Manager** in the **Product Line** search field to display frequently downloaded Communication Manager software, including recent service packs and updates.

2. Previous Communication Manager 6.3 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 **6.3** in the **Version** search field to display all available Communication Manager 6.3 software downloads.

The MD5 sums are included in the Support and PLDS descriptions for these downloads.

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

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:

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 6.3.x from the **Choose Release** pull down menu to the right.
5. In the **DOWNLOADS** table find and Click on **Latest TN Circuit Pack, Server, and Media Gateway Firmware and Software Updates, 6.3.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. 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-rhel5.3-3018. 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.

5. If patch PLAT-rhel5.3-3018 fails to activate despite performing these steps, escalate to Avaya Global Support Services.

6. **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-rhel5.3-3018*
     > update_activate *PLAT-rhel5.3-3018*
   - 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 6.3 SP#0 (20553) 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 Communication Manager Virtual Machine.

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-rhel5.3-3018" 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-rhel5.3-3018" as "activated."
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:	Although Security Service Pack PLAT-rhel5.3-3018 can be deactivated, the updates that it installs will still 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-rhel5.3-3018). This current Security Service Pack will include the fixes from all previous Security Service Packs detailed in the next section.

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-rhel5.3-3010.tar)

ASA Number	Communication Manager 6.3 Classification	ASA Number	Communication Manager 6.3 Classification
ASA-2013-163	None	ASA-2013-283	Low
ASA-2013-168	None	ASA-2013-284	Low
ASA-2013-182	Low	ASA-2013-285	Low
ASA-2013-183	Medium	ASA-2013-326	None
ASA-2013-201	Low	ASA-2013-337	Low
ASA-2013-210	Low	ASA-2013-338	None
ASA-2013-277	Low		

Security Vulnerabilities Resolved in Security Service Pack 2
(PLAT-rhel5.3-3011.tar)

ASA Number	Communication Manager 6.3 Classification
ASA-2013-384	Low
ASA-2013-444	Low
ASA-2013-445	Low
ASA-2013-453	None

Security Vulnerabilities Resolved in Security Service Pack 3
(PLAT-rhel5.3-3014.tar)

ASA Number	Communication Manager 6.3 Classification	ASA Number	Communication Manager 6.3 Classification
ASA-2013-470	Low	ASA-2014-064	Low
ASA-2013-471	Low	ASA-2014-084	Low
ASA-2013-499	Low	ASA-2014-121	None
ASA-2013-500	Low	ASA-2014-127	Low
ASA-2013-533	Low	ASA-2014-128	None
ASA-2013-548	Low	ASA-2014-136	Low

ASA-2014-005	Low	ASA-2014-176	Low
ASA-2014-039	None		

Security Vulnerabilities Resolved in Security Service Pack 4
(PLAT-rhel5.3-3016.tar)

ASA Number	Communication Manager 6.3 Classification
ASA-2014-172	Low
ASA-2014-175	Low
ASA-2014-255	Medium
ASA-2014-292	Low

Security Vulnerabilities Resolved in Security Service Pack 5
(PLAT-rhel5.3-3018.tar)

ASA Number	Communication Manager 6.3 Classification	ASA Number	Communication Manager 6.3 Classification
ASA-2014-098	Low	ASA-2014-395	Low
ASA-2014-306	Low	ASA-2014-416	Medium
ASA-2014-339	Low	ASA-2014-417	None
ASA-2014-356	Low	ASA-2014-428	Low
ASA-2014-387	Low	ASA-2014-504	Low
ASA-2014-392	Low		

Mitigation: N/A

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.