Product Correction Notice (PCN)

Issue Date: 05-August-2013
Supplement 8 Date: 13-March-2017
Expiration 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 6.3/6.4 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:

13 March 2017 – Supplement 8 of this PCN introduces Security Service Pack #8 (PLAT-rhel5.3-3021.tar) for Communication Manager 6.3 running on VMware or System Platform 6.3/6.4.

Communication Manager 6.3 Security Service Packs only apply to CM 6.3 software loads R016x.03.0.124.0 (CM6.3.xx.x) and R016x.03.0.141.0 (CM6.3.1xx.x) are not applicable to any other servers, software loads, or releases of Communication Manager.

04 April 2016 – Supplement 7 of this PCN introduced Security Service Pack #7 (PLAT-rhel5.3-3020.tar; PLDS ID CM000000442) for Communication Manager 6.3 running on VMware or System Platform.

12 August 2015 – Supplement 6 of this PCN documented that Security Service Pack #6 (PLAT-rhel5.3-3019.tar) applied to CM 6.3 software load R016x.03.0.141.0 (CM6.3.1xx.x) as well.

09 March 2015 – Supplement 5 of this PCN introduced Security Service Pack #6 (PLAT-rhel5.3-3019.tar) for Communication Manager 6.3 running on VMware or System Platform.

22 December 2014 – Supplement 4 of this PCN introduced Security Service Pack #5 (PLAT-rhel5.3-3018.tar) for Communication Manager 6.3 running on VMware or System Platform.

4 August 2014 – Supplement 3 of this PCN introduced Security Service Pack #4 (PLAT-rhel5.3-3016.tar) for Communication Manager 6.3 running on VMware or System Platform.

2 June 2014 – Supplement 2 of this PCN introduced Security Service Pack #3 (PLAT-rhel5.3-3014.tar) for Communication Manager 6.3 running on VMware or System Platform.

7 October 2013 – Supplement 1 of this PCN introduced Security Service Pack #2 (PLAT-rhel5.3-3011.tar) for Communication Manager 6.3 running on VMware or System Platform.

5 August 2013 – This PCN introduced Security Service Pack #1 (PLAT-rhel5.3-3010.tar) for Communication Manager 6.3 running on VMware or System Platform.

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 recommended for S8300D, S8510, S8800, Common Servers and S8300E Servers running System Platform 6.3 or 6.4 and any of the Communication Manager 6.3 Solution Templates. This PCN is recommended for the Communication Manager 6.3 Simplex VAppliance and Duplex VAppliance running on VMware® vSphere™ ESXi 5.0/5.1/5.5 infrastructures. S8300E Servers must use System Platform 6.3.7 or higher and Communication Manager 6.3.112.0 or 6.3.12.0 and higher SPs/Releases.
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?	Activation of this Communication Manager Security 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 Security Service Pack is customer installable and remotely installable.
Release notes and workarounds are located:	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: 1. Go to http://support.avaya.com 2. Type the ASA number of interest into the **What can we help you with?** search field and when the correct ASA number appears below select it. 3. Scroll down and click on the document link to read the Avaya Security Advisory. You can also access the ASAs 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. Scroll down (if necessary) and click on the link **Security Advisories**
4. Click on the link for the year the security advisory was published, which is part of the ASA number.
5. Page through the advisory numbers to find the link of interest.

Security Service Packs are cumulative and all fixes in previous Security Service Packs for a particular release are included in the latest Security Service Pack for the release. In addition to the Avaya Security Advisories referenced in Section 1B, the following problems are also corrected in this Security Service Pack:

Other Problems Resolved in Security Service Pack 2

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

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

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

Problem	Keywords

Communication Manager now supports the new Russian Time Zone changes from October, 2014.	141383 141600
The bash shellshock fix for ASA-2014-369 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

Other Problems Resolved in Security Service Pack 6

Problem	Keywords
A multithreaded https access could cause httpd to lock up in certain circumstances.	150073
Enhancement: Timezone data was updated to support the next leap second.	150074
Communication Manager did not support SHA-2 LDAP connections, causing "admin" and "cust" LDAP users to no longer log in to Communication Manager.	150075

Other Problems Resolved in Security Service Pack 7

Problem	Keywords
ASG key security update (See PSN020231u).	9218
Customers using RADIUS authentication sometimes had problems authenticating to the RADIUS server.	9779
RHSA-2015-2616 openssl security update.	10251
RHSA-2016-0012 gnutls security update.	10534
RHSA-2016-0073 bind security update.	10552
RHSA-2016-0302 openssl security update.	11267
RHSA-2016-0371 nss security update.	11309

Other Problems Resolved in Security Service Pack 8

No additional problems resolved beyond the Avaya Security Advisories referenced in section 1B.

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

This PCN is being issued as a recommended and customer installable PCN. The specified Security Service Pack tar file is required. To obtain the file refer to the **How do I order this PCN** section of this PCN.

IMPORTANT – Some installation steps are different for Security Service Packs compared to traditional CM Service Packs. These differences are explained in the **Finding the installation instructions** section of this PCN.

installed):

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

The Security Service Pack tar file 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. Mouse over **Support by Product** at the top of the page, click **Downloads** in the menu.
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 if necessary and Click on **Avaya Aura® Communication Manager 6.3 Security Service Pack 7, 6.3.x**.
6. Scroll down the page to find the download link for **PLAT-rhel5.3-3021.tar**. This link will take you to the PLDS system with the **Download pub ID** already entered.

The Security 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 **CM000000454** in the **Download pub ID:** search field to access the Communication Manager Security Service Pack download. 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 Security Service Packs and other software 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 Avaya Support and PLDS descriptions for the download files.

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

This PCN is being issued as a customer installable PCN. The instructions for installing Communication Manager Security Service Packs 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. Mouse over **Support by Product** at the top of the page, click **Documents** in the menu.
3. Begin to type **Communication Manager** in the **Enter Your Product Here** 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. Check the box for **Installation, Upgrades & Config**.
6. Click **ENTER**. Available documents are displayed.

7. Scroll down (if necessary) and click on the document titled **Deploying Avaya Aura® Communication Manager on System Platform** (Chapter 10: Managing Patches) for a System Platform environment or **Deploying Avaya Aura® Communication Manager on VMware® in Virtualized Environment** (Appendix D: Upgrading Communication Manager Open Virtual Application) for a VMware environment.

Important Installation Notes:

1. Security Service Packs are independent of other Communication Manager software updates activated on a server including Communication Manager Service Packs, Kernel Service Packs, over-writable 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 the new Security Service Pack. The system will reboot automatically shortly after activation is successful. Previously removed NTP servers may be re-added to the NTP configuration after the system has rebooted.
5. **Important** - An automatic server reboot will occur after successful activation of a Security Service Pack. The activation steps for a Security Service Pack are:
   a. Run the following bash Command Line Interface (CLI) commands on the server:
      > update_unpack *PLAT-rhel5.3-3021*
      > update_activate *PLAT-rhel5.3-3021*
   b. After successful activation of the Security Service Pack the server will automatically do a full Linux reboot in about 2 minutes.
   c. 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 Security Service Pack is successfully activated using the Communication Manager System Management Interface (SMI) web pages perform the following steps from a web browser:

- Access the Communication Manager SMI web pages by entering the Server name or IP address in the browser Address box.
- Login to the SMI 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:" the Security Service Pack shows "activated."

Or, using the bash Command Line Interface (CLI) run the following command on the server:

> update_show
This should show the status of the new Security Service Pack (Update ID) 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 Packs can be deactivated, the updates installed 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 the Security Service Pack. The Security Service Pack includes fixes from all previous Security Service Packs detailed in the next section as well.

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

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

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

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

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

ASA Number	Communication Manager 6.3 Classification	ASA Number	Communication Manager 6.3 Classification
ASA-2014-098	Low	ASA-2014-417	None
ASA-2014-306	Low	ASA-2014-428	Low
ASA-2014-339	Low	ASA-2014-432	Medium
ASA-2014-356	Low	ASA-2014-504	Low
ASA-2014-387	Low	ASA-2014-523	Low
ASA-2014-369	Low	ASA-2015-002	Low
ASA-2014-395	Low	ASA-2015-012	Low
ASA-2014-416	Medium		

Security Vulnerabilities Resolved in Security Service Pack 6

ASA Number	Communication Manager 6.3 Classification
ASA-2015-011	None
ASA-2015-024	Low

ASA-2015-070	Medium

Security Vulnerabilities Resolved in Security Service Pack 7

ASA Number	Communication Manager 6.3 Classification	ASA Number	Communication Manager 6.3 Classification
ASA-2015-220	None	ASA-2015-409	Low
ASA-2015-239	Low	ASA-2015-438	Low
ASA-2015-320	Low	ASA-2015-442	Low
ASA-2015-366	None	ASA-2015-500	None
ASA-2015-405	Low	ASA-2016-061	None
ASA-2015-407	None		

Security Vulnerabilities Resolved in Security Service Pack 8

ASA Number	Communication Manager 6.3 Classification	ASA Number	Communication Manager 6.3 Classification
ASA-2016-144	None	ASA-2016-428	None
ASA-2016-231	Low	ASA-2016-414	Low
ASA-2016-267	Medium	ASA-2016-323	Low
ASA-2016-386	None	ASA-2016-131	Medium
ASA-2016-412	None		

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	Current Per Incident Rates Apply

Services Labor	

- 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.