**Product Correction Notice (PCN)**

**Issue Date:** 07-October-2013
**Supplement 7 Date:** 27-August-2018
**Archive Date:** NA
**PCN Number:** 1922S

## 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, Common Servers and S8300E servers.

Avaya Aura® Communication Manager 6.3 Simplex vAppliance and Duplex vAppliance running on VMware® vSphere® ESXi 5.0/5.1/5.5 infrastructures. **Note: Before applying this PCN to VMware systems, you must update the VMware tools as described in PCN 1923S.**

**Description:**

**27 August-2018** – Supplement 7 of this PCN introduces Kernel Service Pack #8 for Communication Manager 6.3 (**KERNEL2.6.18-433.AV1.tar; PLDS ID CM000000463**) running on VMware or System Platform 6.3.

This Communication Manager 6.3 Kernel Service Pack only applies to the CM 6.3 software loads R016x.03.0.124.0 (CM 6.3.xx.x) * and R016x.03.0.141.0 (CM 6.3.1xx.x) and is not applicable to any other servers, software loads, or releases of Communication Manager.

***NOTE:** This Kernel Service Pack has only been tested with R016x.03.0.141.0 (CM 6.3.1xx.x) as R016x.03.0.124.0 (CM 6.3.xx.x) is no longer supported per the Avaya Production Software Protection Program and PSN020262u. You may still apply this Kernel Service Pack on an existing R016x.03.0.124.0 system, but if in the event of any issues, the recommendation will be to update to R016x.03.0.141.0.

**NOTE:** Communication Manager 6.3 Kernel Service Pack #4 or later is required for the R016x.03.0.141.0 (CM 6.3.1xx.x) software load.

**13 March-2017** – Supplement 6 of this PCN introduces Kernel Service Pack #7 for Communication Manager 6.3 (KERNEL-2.6.18-417.AV1.tar; PLDS ID CM000000455) running on VMware or System Platform 6.3.

**09 May-2016** – Supplement 5 of this PCN introduced Kernel Service Pack #6 (PLDS ID CM000000443) for Communication Manager 6.3 (KERNEL-2.6.18-409.AV1.tar) running on VMware or System Platform 6.3.

**31 March-2016** – Supplement 4 of this PCN introduces Kernel Service Pack #5 for Communication Manager 6.3 (KERNEL-2.6.18-406.AV1.tar) running on VMware or System Platform 6.3.

| | |
|---|---|
| | **10 August 2015** – Supplement 3 of this PCN introduces Kernel Service Pack #4 for Communication Manager 6.3 (KERNEL-2.6.18-400.AV2.tar) running on VMware or System Platform 6.3.<br><br>**09 March 2015** – Supplement 2 of this PCN introduced Kernel Service Pack #3 for Communication Manager 6.3 (KERNEL-2.6.18-400.AV1.tar) running on VMware or System Platform 6.3. **Note: KSP #3 has been removed from PLDS due to issues activating it on S8300D servers.**<br><br>**11 August 2014** – Supplement 1 of this PCN introduced Kernel Service Pack #2 for Communication Manager 6.3 (KERNEL-2.6.18-371.AV1.tar) running on VMware or System Platform 6.3. **Note: KSP #2 has been removed from PLDS due to issues activating it on S8300D servers.**<br><br>**7 October 2013** – This PCN introduced Kernel Service Pack #1 for Communication Manager 6.3 (KERNEL-2.6.18-348.AV5.tar) running on VMware or System Platform 6.3 equipped S8300D, S8510, S8800 and Common Servers. **Note: KSP #1 has been removed from PLDS due to issues activating it on S8300D servers.** |
| **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. |
| **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 Kernel Service Pack is service disrupting. Activation requires a full Linux reboot. |

| | |
|---|---|
| **Installation of this PCN is required by:** | Customer or Avaya Authorized Service Provider. This Kernel 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 6.3. These vulnerabilities are described by Avaya Security Advisories (ASA), which are referenced in Section 1B – Security Information. The ASA numbers referenced in section 1B can be viewed by performing the following steps from a browser:<br>1. Go to http://support.avaya.com<br>2. Type the ASA number of interest into the **What can we help you with?** search field and when the correct ASA number appears select it.<br>3. Scroll down (if necessary) and click on the document link to read the Avaya Security Advisory.<br><br>You can also access the ASAs by performing the following steps from a browser:<br>1. Go to http://support.avaya.com<br>2. Scroll to the bottom of the page and click **Policies & Legal** under the **HELP & POLICIES** menu.<br>3. Scroll down and click on the link for **Security Advisories**.<br>4. Click on the link for the year the security advisory was published, which is part of the ASA number.<br>5. Page through the advisory numbers to find the link of interest.<br><br>Kernel Service Packs are cumulative and all fixes in previous Kernel Service Packs for a particular release are included in the latest Kernel Service Pack for the release. |
| **What materials are required to implement this PCN (If PCN can be customer installed):** | This PCN is being issued as a recommended and customer installable PCN. The specified Kernel Service Pack tar file is required. To obtain the file refer to the **How do I order this PCN** section of this PCN.<br><br>If unfamiliar with activating Kernel Service Packs, the installation instructions are required. To obtain the installation instructions please refer to the **Finding the installation instructions** section of this PCN. |
| **How do I order this PCN (If PCN can be customer installed):** | **Before applying this PCN to VMware systems, you must update the VMware Tools as described in PCN 1923S**. The Kernel Service Pack tar file can be obtained by performing the following steps from a browser:<br>1. Go to http://support.avaya.com then enter your **Username** and **Password** and click **LOG IN.**<br>2. Mouse over **Support by Product** at the top of the page, click **Downloads** in the menu.<br>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.<br>4. Select 6.3.x from the **Choose Release** pull down menu to the right.<br>5. Scroll down if necessary and click on **Avaya Aura® Communication Manager 6.3 Kernel Service** |

**Pack 8, 6.3.x.**

6. Scroll down the page if necessary and click on the download link **KERNEL-2.6.18-433.AV1.tar**.

The Kernel Service Pack tar file 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 **CM000000463** in the **Download pub ID:** search field to access the Communication Manager Kernel 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 Kernel 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 Kernel 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. Kernel Service Packs are independent of all other Communication Manager software updates activated, including Communication Manager Service Packs, Security Service Packs, over-writable patches or custom patches. None of these other software updates should be deactivated before activating 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. It is not necessary to deactivate an existing Kernel Service Pack before activating a new Kernel Service Pack. Doing so will result in unnecessary additional reboots.
4. If activating a Kernel Service Pack on an S8300D server, PSN020192u should be reviewed and followed.

## 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 Communication Manager Kernel Service Pack installation was successful access the **Server Management** > **Patch Management** > **Manage** page on the System Platform Web Console which should show the status of the Kernel Service Pack as "active."

For VMware® Virtualized Environments you can verify that the Kernel Service Pack is activated using the Communication Manager System Management Interface (SMI) from the **Administration** > **Server (Maintenance)** >**Server Upgrades** > **Manage Updates** page.

For S8300D servers follow the instructions provided in PSN020192u.

**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:**

To remove the Communication Manager Kernel Service Pack:
1) On System Platform click **Server Management** > **Patch Management.**
2) Click **Manage**.
The Patch List page displays the list of patches and the current status of the patches.
3) On the Patch List page, click on the patch that you want to remove.
4) Click **Remove**.

For VMware® Virtualized Environments deactivate the Kernel Service Pack using the Communication Manager System Management Interface from the **Administration** > **Server (Maintenance)** >**Server Upgrades** > **Manage Updates** page.

For S8300D servers follow the instructions provided in PSN020192u

## SECTION 1B – SECURITY INFORMATION

**Are there any security risks involved?**

Issues described by Avaya Security Advisories referenced in this section are corrected by the Communication Manager Kernel Service Pack.

**Avaya Security**

**Note:** A Vulnerability Classification of None in the following tables means either:

**Vulnerability Classification:**

1. The affected components are installed, but the vulnerability is not exploitable.
2. The components are not installed.

**Security vulnerabilities resolved in Kernel Service Pack #8**

| RHSA Number | RHSA Severity | ASA Number | ASA Overall Severity |
|---|---|---|---|
| RHSA-2017-0323 | Important | ASA-2017-096 | Low |
| RHSA-2017-1482 | Important | ASA-2017-145 | Medium |
| RHSA-2017:2412 | Important | ASA-2017-274 | Medium |
| RHSA-2017:2801 | Important | ASA-2017-283 | High |
| RHSA-2018:0292 | Important | ASA-2018-038 | Medium |
| RHSA-2018:1196 | Important | ASA-2018-127 | Medium |
| RHSA-2018:1353 | Moderate | ASA-2018-161 | Medium |
| RHSA-2018:2172 | Important | ASA-2018-231 | Medium |

**Security vulnerabilities resolved in Kernel Service Pack #7**

| RHSA Number | CM 6.3 Vulnerability Classification |
|---|---|
| ASA-2016-396 | Medium |
| ASA-2017-018 | Medium |

**Security vulnerabilities resolved in Kernel Service Pack #6**

| RHSA Number | CM 6.3 Vulnerability Classification |
|---|---|
| RHSA-2016-0450 | Low |

**Security vulnerabilities resolved in Kernel Service Pack #5**

| ASA Number | CM 6.3 Vulnerability Classification |
|---|---|
| ASA-2015-006 | Low |
| ASA-2015-237 | None |
| ASA-2015-289 | Low |

**Security vulnerabilities resolved in Kernel Service Pack #4**

There are no new security vulnerabilities associated with Kernel Service Pack #4.

**Security vulnerabilities resolved in Kernel Service Pack #3**

| ASA Number | CM 6.3 Vulnerability Classification |
|---|---|
| ASA-2014-173 | Low |
| ASA-2014-261 | Low |
| ASA-2014-295 | Low |
| ASA-2014-340 | Low |
| ASA-2014-390 | Low |

**Security vulnerabilities resolved in Kernel Service Pack #2**

| ASA Number | CM 6.3 Vulnerability Classification |
|---|---|
| ASA-2013-446 | Low |

| | |
|---|---|
| ASA-2013-495 | Low |
| ASA-2014-496 | Low |
| ASA-2013-532 | Low |

**Security vulnerabilities resolved in Kernel Service Pack #1**

| ASA Number | CM 6.3 Vulnerability Classification |
|---|---|
| ASA-2013-272 | Low |
| ASA-2013-184 | Low |
| ASA-2014-196 | Low |
| ASA-2014-209 | Low |
| ASA-2014-415 | Low |

**Mitigation:** Activate the Kernel Service Pack. Note: before activating the Kernel Service Pack on VMware systems, VMware Tools should be updated as described in PCN 1923S.

## 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 (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:**<br>-Full Coverage Service Contract*<br>-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.