Product Correction Notice (PCN)

Issue Date: 05-August-2013
Supplement 30 Date: 27-August-2018
Expiration Date: NA
PCN Number: 1798S

SECTION 1 - CUSTOMER NOTICE

Products affected by this PCN:

Avaya Aura® Communication Manager 6.3 Solution Templates running on System Platform equipped S8300D, S8510, S8800 and Common Servers (HP® DL360 G7, Dell® R610 Servers, HP® DL360 G8, and Dell® R620 Servers) plus the newly released S8300E server.

Avaya Aura® Communication Manager 6.3 Solution Templates running on System Platform equipped with the newly released S8300E server must use System Platform Release 6.3.7 or higher.

Avaya Aura® Communication Manager 6.3 Simplex vAppliance and Duplex vAppliance running on VMware® vSphere® ESXi 5.0/5.1/5.5 infrastructures.

Avaya Aura® Communication Manager updated Fault Performance Alarming (FPA) SNMP functionality to Net-SNMP in 6.3.100.0/6.3.111.0 and higher 6.3.1xx Service Packs and releases. There are two separate CM 6.3 releases going forward, with the only difference being new Net-SNMP functionality. 6.3.111.0 (6.3.11.1 CM 6.3 Service Pack 11.1 equivalent) and higher 6.3.1xx SPs include the new Net-SNMP FPA functionality. This new release was introduced with Supplement 18 of this PCN.

Description:

27 August 2018 – Supplement 30 of this PCN introduces verification of **CM 6.3.118.0** with **System Platform 6.4.3.0.01002 (vsp-patch-6.4.3.0.01002.noarch.rpm; PLDS ID CM000000465).** A pre-upgrade patch (**patch-patcher-1.0.bsx; PLDS ID SP00000115**) should be used to speed up the installation of System Platform 6.4.3.0.01002 on an S8300D server running System Platform 6.4.2 only. Installing the System Platform 6.4.3 patch on an S8300D server already running System Platform 6.4.2 can take up to 3 hours. This pre-update patch will reduce that time to 1-1/2 hours. Please see the System Platform 6.4.3 Release Notes for instructions on how to apply this pre-update patch.

NOTE: System Platform 6.4.30.01002 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. If you apply this System Platform Service Pack on an existing R016x.03.0.124.0 system and any issues are encountered, the resolution will be to update to R016x.03.0.141.0.

Important Note: System Platform service packs are cumulative, so System Platform 6.4.3 includes Spectre/Meltdown mitigation originally introduced in April 18 in System Platform 6.4.2

Important Note: If upgrading System Platform to 6.3.8 or higher on a server running a release of Communication Manager lower than 6.3.10.0 or 6.3.111.0, Communication Manager 6.3.10.0 or 6.3.111.0 or higher should be activated prior to upgrading System Platform. Any Communication Manager Service Pack lower than 6.3.10.0 or 6.3.111.0 is incompatible with System Platform 6.3.8 or higher. Communication Manager Service Packs lower than 6.3.10.0 or 6.3.111.0 will undergo an extra

© 2018 Avaya Inc. All Rights Reserved.
Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.
All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya Inc.

reboot roughly 13 minutes after System Platform CDOM and Communication Manager are back in service after the System Platform upgrade to 6.3.8 or higher. Furthermore, subsequent reboots of System Platform CDOM or DOM0 will again cause a CM reboot roughly 13 minutes after System Platform CDOM is back in service.

20 June 2018 – Supplement 29 of this PCN introduces an update to the original CM 6.3 ISO image:

- **Communication Manager 6.3.0.0.2110.iso (PLDS ID CM000000420; md5sum:4EF3C1C923D506FC41C1EA1207FA9B5)** This re-issue of the ISO image has been necessary to remove obsolete Gateway Firmware from the OVAs included in that ISO image. Otherwise, the features are identical to the original release. There is no need for customers to install this new version. The previous 6.3.0.0.2105.iso was removed from PLDS on 06/6/2018 and the new 6.3.0.0.2110.iso was posted to PLDS on 06/6/2018.

17 April 2018 – Supplement 28 of this PCN introduces the following updates:

- **Communication Manager 6.3.118.0 (03.0.141.0-24403.tar; PLDS ID CM000000460)**. This Service Pack only applies to CM 6.3.100.0 load R016x.03.0.141.0 and is not applicable to any other servers, software loads, or releases of Communication Manager. The Service Pack delivers software fixes for Communication Manager 6.3.100.0 and includes all fixes previously provided in earlier 6.3.100.0 Service Packs (see below) plus additional fixes. See the Communication Manager Release Notes for more information.
- **Communication Manager 6.3.18.0 (03.0.124.0-24328.tar; PLDS ID CM000000459)**. This Service Pack only applies to CM 6.3 load R016x.03.0.124.0 and is not applicable to any other servers, software loads, or releases of Communication Manager. The Service Pack delivers software fixes for Communication Manager 6.3.0.0, and includes all fixes previously provided in earlier 6.3.0.0 Service Packs (see below) plus additional fixes. See the Communication Manager Release Notes for more information.
- **System Platform 6.4.2 (vsp-patch-6.4.2.0.01003.noarch.rpm; PLDS ID CM000000461).** The Communication Manager Service Packs were verified with System Platform 6.4.2.

  Important Note: System Platform 6.4.2 includes Spectre/Meltdown mitigation.

  - In order to mitigate the Meltdown and Spectre vulnerabilities, the processor manufacturers and operating system developers will need to provide software patches to their products. These are patches to the processors and operating systems, not to Avaya products.
  - Once these patches are received by Avaya, Avaya will test these patches with the applicable Avaya products to determine what, if any, impact these patches will have on the performance of the Avaya product.
  - Avaya is reliant on our Suppliers to validate the effectiveness of their respective Meltdown and Spectre vulnerability patches.
  - Avaya's test effort is targeted towards reaffirming product/solution functionality and performance associated with the deployment of these patches.
  - The customer is responsible for implementing, and the results obtained from, such patches.

- The customer should be aware that implementing these patches may result in performance degradation.

28 August 2017 – Supplement 27 of this PCN introduced the following updates:

- **Communication Manager 6.3.117.0 (03.0.141.0-23959.tar; PLDS ID CM000000458)**.
- **Communication Manager 6.3.17.0 (03.0.124.0-23947.tar; PLDS ID CM000000457)**.
- **System Platform 6.4.1 (vsp-patch-6.4.1.0.01008.noarch.rpm; PLDS ID CM000000453).**

13 March 2017 – Supplement 26 of this PCN introduced the following updates:

- **Communication Manager 6.3.116.0 (03.0.141.0-23681.tar PLDS ID CM000000452)**.
- **Communication Manager 6.3.16.0 (03.0.124.0-23675.tar PLDS ID CM000000451)**.
- **System Platform 6.4 (vsp-6.4.0.0.17006.iso PLDS ID CM000000450** and **vsp-patch-6.4.1.0.01008.noarch.rpm PLDS ID CM000000453).**

11 November 2016 – Supplement 25 of this PCN introduced verification of CM 6.3.115.1 and 6.3.15.1 with a new version of System Platform 6.4:

- **Communication Manager 6.3.115.1 (03.0.141.0-23383.tar PLDS ID CM000000449)**.
- **Communication Manager 6.3.15.1 (03.0.124.0-23382.tar PLDS ID CM000000448)**.
- **System Platform 6.4 (vsp-6.4.0.0.17006.iso PLDS ID CM000000450).**

10 October 2016 – Supplement 24 of this PCN introduced the following updates:

- **Communication Manager 6.3.115.1 (03.0.141.0-23383.tar PLDS ID CM000000449)**.
- **Communication Manager 6.3.15.1 (03.0.124.0-23382.tar PLDS ID CM000000448)**.
- **System Platform 6.4 (vsp-6.4.0.0.17004.iso PLDS ID CM000000447) and System Platform 6.3.8 (vsp-patch-6.3.8.01002.0.noarch.rpm CM000000439).**

15 September 2016 – Supplement 23 of this PCN introduced verification of CM 6.3.115.0 and 6.3.15.0 with System Platform 6.4:

- **Communication Manager 6.3.115.0 (03.0.141.0-23276.tar PLDS ID CM000000446)**.
- **Communication Manager 6.3.15.0 (03.0.124.0-23263.tar PLDS ID CM000000445)**.
- **System Platform 6.4 (vsp-6.4.0.0.17004.iso) and System Platform 6.3.8 (vsp-patch-6.3.8.01002.0.noarch.rpm).**

29 August 2016 – Supplement 22 of this PCN introduced the following updates:

- **Communication Manager 6.3.115.0 (03.0.141.0-23276.tar)**.
- **Communication Manager 6.3.15.0 (03.0.124.0-23263.tar)**.
- **System Platform 6.3.8 (vsp-patch-6.3.8.01002.0.noarch.rpm)**.

14 March 2016 – Supplement 21 of this PCN introduced the following updates:

- **Communication Manager 6.3.114.0 (03.0.141.0-22901.tar)**.
- **Communication Manager 6.3.14.0 (03.0.124.0-22899.tar)**.
- **System Platform 6.3.8 (vsp-patch-6.3.8.01002.0.noarch.rpm)**.

14 December 2015 – Supplement 20 of this PCN introduced the following updates:

- **Communication Manager 6.3.113.0 (03.0.141.0-22636.tar)**
- **Communication Manager 6.3.13.0 (03.0.124.0-22619.tar)**
- **System Platform 6.3.7 (vsp-6.3.7.0.05001.0.iso)**

31 August 2015 – Supplement 19 of this PCN introduced the following updates:

- **Communication Manager 6.3.112.0 (03.0.141.0-22506.tar)**

© 2018 Avaya Inc. All Rights Reserved.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.
All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya Inc.

- **Communication Manager 6.3.12.0 (03.0.124.0-22505.tar)**
- **System Platform 6.3.7 (vsp-6.3.7.0.05001.0.iso)**

10 August 2015 – Supplement 18 of this PCN introduced the following updates:

- **Communication Manager 6.3.111.0 (03.0.141.0-22460.tar)**. **This Service Pack (or later) is required for CM6.3.100 load R016x.03.0.141.0**
- **System Platform 6.3.7 (vsp-6.3.7.0.05001.0.iso)**

06 August 2015 – Supplement 17 of this PCN introduced the following updates:

Communication Manager 6.3.11.0 (03.0.124.0-22361.tar) is no longer available and is replaced by the following Service Pack.

- **Communication Manager 6.3.11.1 (03.0.124.0-22450.tar)**
- **System Platform 6.3.7 (vsp-6.3.7.0.05001.0.iso)**

08 June 2015 – Supplement 16 of this PCN introduced the following updates:

- **Communication Manager 6.3.11.0 (03.0.124.0-22361.tar)**
- **System Platform 6.3.7 (vsp-6.3.7.0.05001.0.iso)**

18 March 2015 – Supplement 15 of this PCN introduced the following updates:

- **System Platform 6.3.6 (vsp-patch-6.3.6.01005.0.noarch.rpm)**.

09 March 2015 – Supplement 14 of this PCN introduced the following updates:

- **Communication Manager 6.3.10.0 (03.0.124.0-22147.tar)**
- **System Platform 6.3.5 (vsp-patch-6.3.5.01003.0.noarch.rpm)**

05 February 2015 – Supplement 13 of this PCN introduced the following updates:

Communication Manager 6.3.9.0 (03.0.124.0-21971.tar) is no longer available and is replaced by the following Service Pack.

- **Communication Manager 6.3.9.1 (03.0.124.0-22098.tar)**
- **System Platform 6.3.5 (vsp-patch-6.3.5.01003.0.noarch.rpm)**

22 December 2014 – Supplement 12 of this PCN introduced the following updates:

- **Communication Manager 6.3.9.0 (03.0.124.0-21971.tar)**
- **System Platform 6.3.5 (vsp-patch-6.3.5.01003.0.noarch.rpm)**

03 November 2014 – Supplement 11 of this PCN introduced the following updates:

Communication Manager 6.3.7.0 (03.0.124.0-21754.tar) is no longer available and is replaced by the following Service Pack.

- **Communication Manager 6.3.7.1 (03.0.124.0-21895.tar)**
- **System Platform 6.3.4 (vsp-patch-6.3.4.08011.0.noarch.rpm)**

20 October 2014 – Supplement 10 of this PCN introduced the following updates:

- **Communication Manager 6.3.8.0 (03.0.124.0-21588.tar)**
- **System Platform 6.3.5 (vsp-patch-6.3.5.01003.0.noarch.rpm)**

07 October 2014 – Supplement 9 of this PCN introduced the following updates:

- **Communication Manager 6.3.6.1 (03.0.124.0-21894.tar)**
- **System Platform 6.3.4 (vsp-patch-6.3.4.08011.0.noarch.rpm)**
- **Communication Manager 6.3.4.1 (03.0.124.0-21811.tar)**
- **System Platform 6.3.1 (vsp-patch-6.3.1.08002.0.noarch.rpm)**

25 September 2014 – Supplement 8 of this PCN introduced the following updates:

- **System Platform 6.3.4.0 (vsp-patch-6.3.4.08011.0.noarch.rpm)**

11 August 2014 – Supplement 7 of this PCN introduces the following updates:

	• **Communication Manager 6.3.7.0 (03.0.124.0-21754.tar)** • **System Platform 6.3.4 (vsp-patch-6.3.4.08011.0.noarch.rpm)** **2 June 2014** – Supplement 6 of this PCN introduced the following updates: • **Communication Manager 6.3.6.0 (03.0.124.0-21591.tar)** • **System Platform 6.3.4 (vsp-patch-6.3.4.08011.0.noarch.rpm)** **30 April 2014** – Supplement 5 of this PCN introduced the following updates: • **Communication Manager 6.3.5.0 (03.0.124.0-21460.tar)** • **System Platform 6.3.1 (vsp-patch-6.3.1.08002.0.noarch.rpm)** **3 February 2014** – Supplement 4 of this PCN introduced the following updates: • **Communication Manager 6.3.4.0 (03.0.124.0-21291.tar)** • **System Platform 6.3.1 (vsp-patch-6.3.1.08002.0.noarch.rpm)** **2 December 2013** – Supplement 3 of this PCN introduced the following updates: • **Communication Manager 6.3.3.0 (03.0.124.0-21172.tar)** • **System Platform 6.3.1 (vsp-patch-6.3.1.08002.0.noarch.rpm)** **6 November 2013** – Supplement 2 of this PCN introduced the following updates: • **Communication Manager 6.3.2.1 (03.0.124.0-21106.tar)** • **System Platform 6.3.1 (vsp-patch-6.3.1.08002.0.noarch.rpm)** **7 October 2013** – Supplement 1 of this PCN introduced the following updates: • **Communication Manager 6.3.2.0 (03.0.124.0-21053.tar)** • **System Platform 6.3.1 (vsp-patch-6.3.1.08002.0.noarch.rpm)** **5 August 2013** – The original PCN introduced **Communication Manager 6.3.1.0 (Service Pack 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 recommended for S8300D, S8510, S8800, Common Server (HP DL360 G7, Dell R610, HP DL360 G8 and Dell R620) Servers running System Platform and any of the Communication Manager 6.3 Solution Templates. 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. This PCN is recommended for the Communication Manager 6.3 Simplex VAppliance and Duplex VAppliance running on VMware® vSphere^{TM} ESXi 5.0/5.1/5.5 infrastructures.
The risk if this PCN is not installed:	It is possible that Communication Manager service disruptions could occur, as well as some features not working as expected.
Is this PCN for US customers, non-US	This PCN applies to both US and non-US customers.

© 2018 Avaya Inc. All Rights Reserved.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.
All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya Inc.

customers, or both?

Does applying this PCN disrupt my service during installation?

Activation of these Communication Manager Service Packs is service disrupting on simplex (non-duplicated) servers. For duplicated servers, patch activation can be performed in a connection preserving manner. This procedure is described in the installation instructions and in PSN002589u.

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:

The Communication Manager Release Notes contain the specific software updates included in the Service Pack and 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. Scroll down (if necessary) and check the box for **Release & Software Update Notes**.
6. Click **ENTER**. Available documents are displayed.
7. Click on the appropriate Release Notes document.
8. Links to the Release Notes can also be found on the **Avaya Aura® Communication Manager 6.3.x** download page (see section **How do I order this PCN**).

The System Platform Release Notes 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 **System Platform** in the **Enter Your Product Here** box and when Avaya Aura® System Platform appears as a selection below, select it.
4. Select 6.4.x from the **Choose Release** pull down menu to the right.
5. Scroll down (if necessary) and check the box for **Release & Software Update Notes**.
6. Click **ENTER**. Available documents are displayed.
7. Click on the appropriate Release Notes document.

Important Note: System Platform 6.4.2 includes Spectre/Meltdown mitigation.

- In order to mitigate the Meltdown and Spectre vulnerabilities, the processor manufacturers and operating system developers will need to provide software patches to their products. These are patches to the processors and operating systems, not to Avaya products.
- Once these patches are received by Avaya, Avaya will test these patches with the applicable Avaya

products to determine what, if any, impact these patches will have on the performance of the Avaya product.

- Avaya is reliant on our Suppliers to validate the effectiveness of their respective Meltdown and Spectre vulnerability patches.
- Avaya's test effort is targeted towards reaffirming product/solution functionality and performance associated with the deployment of these patches.
- The customer is responsible for implementing, and the results obtained from, such patches.
- The customer should be aware that implementing these patches may result in performance degradation.

Important Note: If upgrading System Platform to 6.3.8 or higher on a server running a release of Communication Manager lower than 6.3.10.0 or 6.3.111.0, Communication Manager 6.3.10.0 or 6.3.111.0 or higher should be activated prior to upgrading to System Platform 6.3.8 or higher. Any Communication Manager Service Pack lower than 6.3.10.0 or 6.3.111.0 is incompatible with System Platform 6.3.8 or higher.

Communication Manager Service Packs lower than 6.3.10.0 or 6.3.111.0 will undergo an extra reboot roughly 13 minutes after System Platform CDOM and Communication Manager are back in service after the System Platform upgrade to 6.3.8 or higher. Furthermore, subsequent reboots of System Platform CDOM or DOM0 will again cause a CM reboot roughly 13 minutes after System Platform CDOM is back in service.

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 specified Communication Manager update file is required. To obtain the update file refer to the **How do I order this PCN** section of this PCN.

If unfamiliar with installing Communication Manager 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):

The software update files 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 and System Platform 6.3 Service Packs, 6.3.x.**
6. For Service Pack 6.3.118.0, scroll down the page to find the download links **03.0.141.0-24403.tar** and **vsp-patch-6.4.2.0.01003.noarch.rpm**. These links will take you to the PLDS system with the **Download pub ID** already entered.
7. For Service Pack 6.3.18.0, scroll down the page to find the download links **03.0.124.0-24328.tar** and **vsp-patch-6.4.2.0.01003.noarch.rpm**. These links will take you to the PLDS system with the **Download pub ID** already entered.

© 2018 Avaya Inc. All Rights Reserved.
All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya Inc.

8. This page also includes links to the Release Notes.

Software updates 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 the appropriate PLDS ID in the **Download pub ID** field to access the desired download (PLDS IDs are included in the Description section of this PCN). 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.

Important Note: If upgrading System Platform to 6.3.8 or higher on a server running a release of Communication Manager lower than 6.3.10.0 or 6.3.111.0, Communication Manager 6.3.10.0 or 6.3.111.0 or higher should be activated prior to upgrading to System Platform 6.3.8 or higher. Any Communication Manager Service Pack lower than 6.3.10.0 or 6.3.111.0 is incompatible with System Platform 6.3.8 or higher.

Communication Manager Service Packs lower than 6.3.10.0 or 6.3.111.0 will undergo an extra reboot roughly 13 minutes after System Platform CDOM and Communication Manager are back in service after the System Platform upgrade to 6.3.8 or higher. Furthermore, subsequent reboots of System Platform CDOM or DOM0 will again cause a CM reboot roughly 13 minutes after System Platform CDOM is back in service.

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):

The instructions for installing Communication Manager software updates 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.

The instructions for patching and upgrading System Platform 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 **System Platform** in the **Enter Your Product Here** box and when Avaya Aura® System Platform 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** and the box for **User Guides**.
6. Click **ENTER**. Available documents are displayed.
7. Click on the document titled **Upgrading Avaya Aura® System Platform Release 6.3.7.** Note that this document includes instructions on installing patches (i.e. 6.3.8) as well.
8. See the following documents: **Installing and Configuring Avaya Aura® System Platform Release 6.3.7** and/or **Upgrading Avaya Aura® System Platform Release 6.3.7**. See the System Platform Release Notes for additional information.

Important Note: System Platform 6.4.2 includes Spectre/Meltdown mitigation.

- In order to mitigate the Meltdown and Spectre vulnerabilities, the processor manufacturers and operating system developers will need to provide software patches to their products. These are patches to the processors and operating systems, not to Avaya products.
- Once these patches are received by Avaya, Avaya will test these patches with the applicable Avaya products to determine what, if any, impact these patches will have on the performance of the Avaya product.
- Avaya is reliant on our Suppliers to validate the effectiveness of their respective Meltdown and Spectre vulnerability patches.
- Avaya's test effort is targeted towards reaffirming product/solution functionality and performance associated with the deployment of these patches.
- The customer is responsible for implementing, and the results obtained from, such patches.
- The customer should be aware that implementing these patches may result in performance degradation.

Important Note: If upgrading System Platform to 6.3.8 or higher on a server running a release of Communication Manager lower than 6.3.10.0 or 6.3.111.0, Communication Manager 6.3.10.0 or 6.3.111.0 or higher should be activated prior to upgrading to System Platform 6.3.8 or higher. Any Communication Manager Service Pack lower than 6.3.10.0 or 6.3.111.0 is incompatible with System Platform 6.3.8 or higher.

Communication Manager Service Packs lower than 6.3.10.0 or 6.3.111.0 will undergo an extra reboot roughly 13 minutes after System Platform CDOM and Communication Manager are back in service after the System Platform upgrade to 6.3.8 or higher. Furthermore, subsequent reboots of System Platform CDOM or DOM0 will again cause a CM reboot roughly 13 minutes after System Platform

CDOM is back in service.

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 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 Service Pack or patch as "active."

For steps to verify that System Platform was successfully upgraded refer to the documentation referenced in the **Finding the installation instructions** section of this PCN.

For VMware® Virtualized Environments verify the Communication Manager Service Pack installation was successful using the Communication Manager System Management Interface (SMI) from the **Administration** > **Server (Maintenance)** >**Server Upgrades** > **Manage Updates** page.

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:

IMPORTANT: To avoid losing service, IP Softphone/soft client users should logoff thereby restoring their base phone to service before removing a Communication Manager Service Pack.

To remove the Communication Manager 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 steps to roll back the System Platform upgrade refer to the documentation referenced in the **Finding the installation instructions** section of this PCN.

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

SECTION 1B – SECURITY INFORMATION

Are there any security risks involved?

No.

Avaya Security Vulnerability Classification:

N/A

© 2018 Avaya Inc. All Rights Reserved.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.
All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya Inc.

Mitigation: N/A

SECTION 1C – ENTITLEMENTS AND CONTACTS

Material Coverage Entitlements:

This Communication Manager 6.3 Service Pack is available free of charge to customers with a valid support contract for Communication Manager 6.x. However, starting with Release 6.2 the Avaya Service Pack and Dot Release Guardian feature controls customer entitlement to these Communication Manager software updates as described below.

Communication Manager 6.2 introduced the Service Pack and Dot Release Guardian feature. This feature determines customer software entitlement by comparing the software Publication Date embedded in the Communication Manager release or Service Pack software to the Support End Date (SED) in the Product Licensing and Delivery System (PLDS) generated license. The SED is set as the later of the warranty expiration date or the support contract expiration date.

> -If the Service Pack/dot release has a ***Publication Date on or before the SED***, the Service Pack/dot release is ***allowed***.
> -If the Service Pack/dot release has a ***Publication Date after the SED***, the Service Pack/dot release is ***not allowed.***

Attempting to install a Service Pack without appropriate entitlements will fail with an error message indicating that the Service Pack Publication Date is after the SED in the license file.

Starting on August 20, 2011 all Communication Manager 6.x (or greater) license files generated in PLDS include the SED. Installing Service Packs on Communication Manager 6.2 (or greater) systems using these licenses will be subject to the Guardian entitlement check.

Communication Manager 6.x license files generated before August 20, 2011 do not have the SED and systems using these licenses can upgrade to Communication Manager 6.2 (or greater) without the Guardian entitlement check. Installing Service Packs on Communication Manager 6.2 (or greater) systems using these licenses will not be subject to the Guardian entitlement check.

Avaya recommends generating and installing a license file with SED before upgrading Communication Manager 6.3 Service Packs. This ensures the license file includes the most up to date SED.

For more information on Service Pack and Dot Release Guardian refer to the document titled **Service Pack & Dot Release Guardian FAQs.** Go to http://support.avaya.com then enter the document title in the “What can we help you with?” search box. Scroll down and click on the document link.

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.