Product Correction Notice (PCN)

Issue Date:	**02-October-2017**
Supplement Date:	**11-January-2021**
Expiration Date:	**NA**
PCN Number:	**2075S**

SECTION 1 - CUSTOMER NOTICE

Products affected by this PCN:

Avaya Aura® Communication Manager 7.1 Simplex vAppliance and Duplex vAppliance running on Avaya Aura® Appliance Virtualization Platform (AVP) on Avaya provided servers, VMware® vSphere® ESXi infrastructures on VMware® certified hardware, Simplex and Duplex vAppliance running on Amazon Web Services (AWS), and Simplex and Duplex running on Kernel-based Virtual Machines (KVM).

Description:

11 January 2021 – Supplement 9 of this PCN introduces **Security Service Pack #10 (**PLAT-rhel7.2-0100.tar**; PLDS ID CM000000936)** and **Kernel Service Pack #10 (**KERNEL-3.10.0-1160.6.1.el7.AV1.tar**; PLDS ID CM000000937)** for Avaya Aura® Communication Manager 7.1.x software load R017x.01.0.532.0. These are the final Security and Kernel Service Packs for Aura 7.x. Customers should actively plan to upgrade to a supported load.

- **Overwritable patch 25925** is **required** prior to applying SSP 10. **(**01.0.532.0-25925.tar**; PLDS ID CM000000928)**
- Order of application is **critical** – see the *Finding the installation instructions* section of this PCN.
- If System Manager (SMGR) SDM was used to upgrade from CM 7.0 to 7.1.x, reference PSN020355u – *Avaya Aura® Communication Manager 7.x, 8.x Kernel and Security Service Pack Installation Failures* if System Manager (SMGR). The pre-activation patch listed in that PSN is required when applying **any** 7.1 SSP or KSP if SMGR SDM was used in the upgrade process.

09 November 2020 – Supplement 8 of this PCN introduces **Security Service Pack #9 (**PLAT-rhel7.2-0090.tar**; PLDS ID CM000000933)** and **Kernel Service Pack #9 (**KERNEL-3.10.0-1127.19.1.el7.AV1.tar**; PLDS ID CM000000934)** for Avaya Aura® Communication Manager 7.1.x software load R017x.01.0.532.0.

- **Overwritable patch 25925** is **required** prior to applying SSP 9. **(**01.0.532.0-25925.tar**; PLDS ID CM000000928)**
- Order of application is **critical** – see the *Finding the installation instructions* section of this PCN.
- If System Manager (SMGR) SDM was used to upgrade from CM 7.0 to 7.1.x, reference PSN020355u – *Avaya Aura® Communication Manager 7.x, 8.x Kernel and Security Service Pack Installation Failures* if System Manager (SMGR). The pre-activation patch listed in that PSN is required when applying **any** 7.1 SSP or KSP if SMGR SDM was used in the upgrade process.

13 April 2020 – Supplement 7 of this PCN introduces **Security Service Pack #8 (**PLAT-rhel7.2-0080.tar**; PLDS ID CM000000930)** and **Kernel Service Pack #8 (**KERNEL-3.10.0-1062.12.1.el7.AV1.tar**; PLDS ID CM000000931)** for Avaya Aura® Communication Manager 7.1.x software load R017x.01.0.532.0.

- **Overwritable patch 25925** is **required** prior to applying SSP 8. **(**01.0.532.0-25925.tar**; PLDS ID CM000000928)**
- Order of application is **critical** – see the *Finding the installation instructions* section of this PCN.
- If System Manager (SMGR) SDM was used to upgrade from CM 7.0 to 7.1.x, reference PSN020355u – *Avaya Aura® Communication Manager 7.x, 8.x Kernel and Security Service Pack Installation Failures* if System Manager (SMGR). The pre-activation patch listed in that PSN is required when applying **any** 7.1 SSP or KSP if SMGR SDM was used in the upgrade process.

16 January 2020 – Supplement 6 of this PCN introduces **Security Service Pack #7 (**PLAT-rhel7.2-0070.tar**; PLDS ID CM000000926)** and **Kernel Service Pack #7 (**KERNEL-3.10.0-1062.1.2.el7.AV1.tar**; PLDS ID CM000000927)** for Avaya Aura® Communication Manager 7.1.x software load R017x.01.0.532.0.

- **Overwritable patch 25925** is **required** prior to applying SSP 7. **(**01.0.532.0-25925.tar**; PLDS ID CM000000928)**
- Order of application is **critical** – see the *Finding the installation instructions* section of this PCN.
- If System Manager (SMGR) SDM was used to upgrade from CM 7.0 to 7.1.x, reference PSN020355u – *Avaya Aura® Communication Manager 7.x, 8.x Kernel and Security Service Pack Installation Failures* if System Manager (SMGR). The pre-activation patch listed in that PSN is required when applying **any** 7.1 SSP or KSP if SMGR SDM was used in the upgrade process.

08 July 2019 – Supplement 5 of this PCN introduces **Security Service Pack #6 (**PLAT-rhel7.2-0060.tar**; PLDS ID CM000000923)** and **Kernel Service Pack #6 (**KERNEL-3.10.0-957.12.2.el7.AV1.tar**; PLDS ID CM000000924)** for Avaya Aura® Communication Manager 7.1.x software load R017x.01.0.532.0.

11 February 2019 – Supplement 4 of this PCN introduces **Security Service Pack #5 (**PLAT-rhel7.2-0050.tar**; PLDS ID CM000000920)** and **Kernel Service Pack #5 (**KERNEL-3.10.0-957.1.3.el7.AV1.tar**; PLDS ID CM000000921)** for Avaya Aura® Communication Manager 7.1.x software load R017x.01.0.532.0.

22 October 2018 – Supplement 3 of this PCN introduces **Security Service Pack #4 (PLAT-rhel7.2-0040.tar; PLDS ID CM000000917)** and **Kernel Service Pack #4 (KERNEL-3.10.0-862.11.6.el7.AV2.tar; PLDS ID CM000000918)** for Avaya Aura® Communication Manager 7.1.x software load R017x.01.0.532.0.

NOTE: Kernel Service Pack #4 includes L1TF mitigation for Communication Manager and it is enabled by default. Refer to PSN020369u/PSN020372u for important information on L1TF mitigation.

- In order to help mitigate the L1TF Vulnerabilities, the processor manufacturers and operating system developers provide software patches to their products. These are patches to the processors, hypervisors, and operating systems that the Avaya solutions utilize (they are not patches applied to the Avaya developed components of the solutions).
- Once these patches are received by Avaya, they are tested with the applicable Avaya solutions to characterize any impact on the performance of the Avaya solutions. The objective of the testing is to reaffirm product/solution functionality and to observe the

performance of the Avaya solutions in conjunction with the patches using typical operating parameters.

- Avaya is reliant on our suppliers to validate the effectiveness of their respective Speculative Execution Vulnerability patches.
- The customer should be aware that implementing these patches may result in performance degradation and that results may vary to some degree for each deployment. The customer is responsible for implementing the patches, and for the results obtained from such patches.

06 August 2018 – Supplement 2 of this PCN introduces **Security Service Pack #3 (PLAT-rhel7.2-0030.tar; PLDS ID CM000000914)** and ~~**Kernel Service Pack #3 (KERNEL-3.10.0-862.3.2.el7.AV1.tar; PLDS ID CM000000915)**~~ for Avaya Aura® Communication Manager 7.1.x software load R017x.01.0.532.0.

Kernel Service Pack #3 was removed from support.avaya.com on Sept 11, 2018. Reference "PSN020366u – Avaya Aura® Communication Manager 7.1 Kernel Service Pack #3 (KSP #3) Removed."

13 August 2018 – Supplement 2.1 Updated RHSAs for SSP #3.

NOTE: If Avaya Aura® System Manager Solution Deployment Manager (SDM) is/was used to upgrade Communication Manager from CM 7.0.x to CM 7.1.x then an upgrade patch must be applied before the Kernel Service Pack and/or Security Service Pack are activated, otherwise activation will fail. Refer to PSN020355u for more information.

07 May 2018 – Supplement 1 of this PCN introduces **Security Service Pack #2 (PLAT-rhel7.2-0020.tar; PLDS ID CM000000909)** and **Kernel Service Pack #2 (KERNEL-3.10.0-693.21.1.el7.AV1.tar; PLDS ID CM000000910)** for Avaya Aura® Communication Manager 7.1.x software load R017x.01.0.532.0.

NOTE: Kernel Service Pack #2 includes Spectre/Meltdown mitigation for Communication Manager and it is enabled by default. Refer to PSN020346u/PSN020347u for important information on performance impact.

- 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.

	NOTE: If Avaya Aura® System Manager Solution Deployment Manager (SDM) is/was used to upgrade Communication Manager from CM 7.0.x to CM 7.1.x then an upgrade patch must be applied before the Kernel Service Pack and/or Security Service Pack are activated, otherwise activation will fail. Refer to PSN020355u for more information. **02 October 2017** – This PCN introduced **Security Service Pack #1 (PLAT-rhel7.2-0010.tar; PLDS ID CM000000831)** and **Kernel Service Pack #1 (KERNEL-3.10.0-693.el7.AV1.tar; PLDS ID CM000000832)** for Avaya Aura® Communication Manager 7.1.x software load R017x.01.0.532.0.
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 recommended for Communication Manager 7.1 running on the Appliance Virtualization Platform (AVP), Vmware® vSphere™ ESXi, AWS, or KVM platforms/infrastructures.
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 the Security Service Pack and/or Kernel Service Pack will disrupt service since they both require a full Linux reboot of the Communication Manager Virtual Machine (VM) to take effect. Refer to the **Description** section of this PCN for important notes.
Installation of this PCN is required by:	Customer or Avaya Authorized Service Provider. This upgrade is customer installable and remotely installable.
Release notes and workarounds are located:	The Security Service Pack and Kernel Service Pack resolve vulnerabilities described by Avaya Security Advisories (ASA) referenced in section 1B – Security information. The ASAs referenced in section 1B can be viewed by performing the following steps in 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 select it. 3. Scroll down (if necessary) 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
2. Scroll to the bottom of the page and click **Policies & Legal** under the **HELP & POLICIES** menu.
3. Scroll down and click on the link for **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 (SSP) and Kernel Service Packs (KSP) are cumulative. This means that all fixes in previous 7.1.x KSPs and SSPs are included in the most recent KSP and SSP. Vmware Tools updates are included in KSPs.

Refer to the **Description** section of this PCN for important notes.

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 files are required. To obtain the update files refer to the **How do I order this PCN** section of this PCN.

If unfamiliar with installing Communication Manager software updates, 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 Security Service Pack and Kernel 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. 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 7.1.x from the **Choose Release** pull down menu to the right.
5. Scroll down if necessary and click on **Avaya Aura® Communication Manager 7.1 Kernel Service Pack 3, 7.1.x** and/or **Avaya Aura® Communication Manager 7.1 Security Service Pack 3, 7.1.x.**
6. Click on the download link for the tar file and download it.

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. Select **View Downloads.**
3. In the **Search by Download** tab enter the correct PLDS ID (corresponding PLDS IDs included in the Description section of this document) in the **Download pub ID** search field to access the download. Select 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 other software updates.

2. All Communication Manager 7.1 software downloads are available on PLDS. In the PLDS **View Downloads** section under the **Search by Download** tab, select **Communication Manager** in the **Application** search field and **7.1** in the **Version** search field to display all available Communication Manager 7.1 software downloads.

The MD5 sums are included in the Avaya Support and PLDS descriptions for the download files.

Refer to the **Description** section of this PCN for important notes that might require additional materials.

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

The instructions for installing or upgrading Communication Manager software 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 **7.1.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) Click on the appropriate document (e.g., click on **Deploying Avaya Aura® Communication Manager** for new installations or **Upgrading to Avaya Aura® Communication Manager** for upgrades). These documents include patching instructions.

Important Security Service Pack Installation Notes:

➔If SMGR SDM was used to upgrade from CM 7.0 to 7.1.x, a pre-activation patch (24598**, PLDS ID**: CM000000911) is required for the SSP and/or KSP.
Reference PSN020355u – *Avaya Aura® Communication Manager 7.x, 8.x Kernel and Security Service Pack Installation Failures* for instructions.

➔ Critical steps for SSP 7 and HIGHER installation

If upgrading the CM Service Pack, SSP and KSP, use the following order:

Use these steps to upgrade any CM 7.1.x.x Feature Pack, Service Pack or custom patch to 7.1.3.5 or higher AND to SSP 7/KSP 7 or higher.
These steps would also be followed if updating any CM 7.1.x.x Service Pack to a later 7.1.x.x Service Pack prior to 7.1.3.5 AND applying SSP7/KSP 7 or higher.
For example, CM 7.1.3.0 to 7.1.3.4, then applying KSP 7/SSP 7 or higher.

a. Copy all patches to CM.
b. Unpack all patches.
c. Apply KSP/SSP pre-activation patch 24598 **if SMGR SDM** was used to update CM 7.0.x to 7.1.x. This REQUIRES DEACTIVATION of any Service Pack, Kernel Service Pack and Security Service Pack before activation of 24598.
d. Activate 25925 BEFORE any further steps.

e. Activate KSP 7 or higher.
    i. Reboot occurs.
    ii. Commit KSP 7 or higher.
f. Deactivate existing SSP (if not already deactivated).
g. Activate SSP 7 or higher.
h. Deactivate 7.1.x.x (if not already deactivated).
i. Activate 7.1.3.5 or higher (whatever 7.1.x.x Service Pack is applicable).

If upgrading only the SSP and KSP, use the following order:

CM 7.1.x through 7.1.3.4, updating to SSP 7/KSP 7 or higher.

a. Copy all patches to CM.
b. Unpack all patches.
c. Activate 25925 BEFORE any further steps.
d. Apply KSP/SSP pre-activation patch 24598 **if SMGR SDM** was used to update CM 7.0.x to 7.1.x. This REQUIRES DEACTIVATION of any Service Pack, Kernel Service Pack and Security Service Pack before activation of 24598 EXCEPT for 25925. Do NOT deactivate 25925.
e. Activate KSP 7 or higher.
    iii. Reboot occurs.
    iv. Commit KSP 7 or higher.
f. Deactivate existing SSP (if not already deactivated).
g. Activate SSP 7 or higher.
h. Activate CM Service Pack (if it was previously deactivated).

NOTE: In rare cases, a scenario may be encountered where activation of a CM Service Pack or custom patch results in a string of errors similar to the following:

```
SERVER_SETUP: server_setup completed successfully
sudo: PAM account management error: Permission denied
ERROR: runcmd:CMDCheck – invalid usage of commandCheck
sudo: PAM account management error: Permission denied
ERROR: runcmd:CMDCheck – invalid usage of commandCheck
sudo: PAM account management error: Permission denied
ERROR: runcmd:CMDCheck – invalid usage of commandCheck
```

If this occurs, the steps to remediate the issue are as follows:

Deactivate 25925.
Activate 25925.
Deactivate the CM Service Pack.
Activate the CM Service Pack.

NOTE: If using SDM to activate the patches, the steps are similar.

Additional Security Service Pack Installation Notes:

1) Security Service Packs are independent of other Communication Manager software updates activated on a server including CM 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 Security Service Pack. 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. Note that system time changes and NTP server changes can cause service disruptions.

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:
      i. update_unpack *PLAT-rhel7.2-0050.tar*
      ii. update_activate *PLAT-rhel7.2-0050*

   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.

Important Kernel Service Pack Installation Notes:

➔If SMGR SDM was used to upgrade from CM 7.0 to 7.1.x, a pre-activation patch (24598**, PLDS ID**: CM000000911) is required for the SSP and/or KSP.
Reference PSN020355u – *Avaya Aura® Communication Manager 7.x, 8.x Kernel and Security Service Pack Installation Failures* for instructions.

➔Reference critical steps above for SSP 7.

1) Kernel Service Packs are independent of 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 Service Packs/Feature Packs.

How to verify the installation

Using the bash Command Line Interface (CLI) run the following command on the server:

- update_show

of the Service Pack has been successful:	This should show the status of the Security Service Pack and/or Kernel Service Pack (Update ID) as "activated". You can also use 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 (deactivate) the Kernel Service Pack use 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 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 previous versions. ➢ NOTE: With Security Service Packs, deactivating the Security Service Pack and attempting to activate an older/lower numbered Security Service Pack will fail and include errors similar to the following: Install of rpms in PLAT-rhel7.2-00x0 failed! Failed to activate PLAT-rhel7.2-00x0!

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 or Kernel Service Pack as noted. Security Service Packs (SSP) and Kernel Service Packs (KSP) include the fixes from all previous SSPs and KSPs respectively for a given CM release.
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. **Security vulnerabilities resolved in Security Service Pack #1**

SA Number	Classification	SA Number	Classification
RHSA-2016-2590	Moderate	RHSA-2017-1095	Important
ASA-2017-010	Low	RHSA-2017-1852	Moderate
ASA-2017-107	Low	RHSA-2017:1860	Moderate
ASA-2017-108	Low	RHSA-2017:1865	Moderate
ASA-2017-112	Low	RHSA_2017:1868	Moderate
ASA-2017-117	Low	RHSA-2017:1916	Moderate
ASA-2017-142	Low	RHSA-2017:1931	Moderate
ASA-2017-149	Low	RHSA-2017:2016	Moderate

ASA-2017-190	Low	RHSA-2017:2029	Moderate
ASA-2017-192	None	RHSA-2017:2192	Moderate
ASA-2017-233	Low	RHSA-2017:2285	Moderate
RHSA-2017-0906	Moderate	RHSA-2017:2292	Moderate
RHSA-2017-0907	Moderate	RHSA-2017:2299	Moderate

Security vulnerabilities resolved in Kernel Service Pack #1

SA Number	Classification	SA Number	Classification
ASA-2017-070	Medium	ASA-2017-215	Medium
ASA-2017-151	Medium	RHSA-2017:1842	Important
ASA-2017-155	Medium		

Security vulnerabilities resolved in Security Service Pack #2

SA Number	Classification	SA Number	Classification
ASA-2017-216	Low	ASA-2017-322	Medium
ASA-2017-271	High	ASA-2017-331	Medium
ASA-2017-275	Medium	ASA-2017-336	High
ASA-2017-286	High	ASA-2018-004	Medium
ASA-2017-289	Critical	ASA-2018-002	Medium
ASA-2017-298	High	ASA-2018-017	High
ASA-2017-318	High	ASA-2018-020	Medium
ASA-2017-275	Medium	ASA-2018-029	Medium

Security vulnerabilities resolved in Kernel Service Pack #2

SA Number	Classification	SA Number	Classification
ASA-2018-023 (Meltdown/Spectre)	Medium	ASA-2018-056	Medium

Note Change in format starting with SSP and KSP #3 to show RHSA as well.

Security vulnerabilities resolved in Security Service Pack #3

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2018:0406	Moderate	ASA-2018-058	Medium
RHSA-2018:0483	Important	ASA-2018-055	High
RHSA-2018:0998	Moderate	ASA-2018-100	Medium
RHSA-2018:0805	Moderate	ASA-2018-103	High
RHSA-2018:0980	Low	ASA-2018-095	Medium
RHSA-2018:0855	Moderate	ASA-2018-101	Medium
RHSA-2018:0913	Low	ASA-2018-093	Low
RHSA-2018:0666	Moderate	ASA-2018-096	Medium
RHSA-2018:0849	Low	ASA-2018-099	Medium

RHSA-2018:1200	Important	ASA-2018-115	High
RHSA-2018:1453	Critical	ASA-2018-159	High
RHSA-2018:1700	Important	ASA-2018-173	High
RHSA-2018:0094	Important	ASA-2018-006	Medium

Security vulnerabilities resolved in Kernel Service Pack #3

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2018:1062	Important	ASA-2018-097	High
RHSA-2018:1318	Important	ASA-2018-141	High
RHSA-2018:1629	Important	ASA-2018-177	Medium

Security vulnerabilities resolved in Security Service Pack #4

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2018:2123	Moderate	ASA-2018-279	Low
RHSA-2018:2181	Important	ASA-2018-232	High

CM 7.1 SSP #4 also contains an updated tzdata: tzdata-2018e

Security vulnerabilities resolved in Kernel Service Pack #4

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2018:1852	Moderate	ASA-2018-229	Medium
RHSA-2018:1965	Important	ASA-2018-227	Medium
RHSA-2018:2384	Important	ASA-2018-270	Medium

CM 7.1 KSP #4 also contains a fix for this issue:

- CM-23336 Running “list measurements occupancy” with any option gives a blank table.

Security vulnerabilities resolved in Security Service Pack #5

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2018:2570	Important	ASA-2018-260	High
RHSA-2018:2768	Moderate	ASA-2018-293	Medium
RHSA-2018-3249	Low	ASA-2018-348	Medium
RHSA-2018-3092	Moderate	ASA-2018-375	High
RHSA-2018:3032	Low	ASA-2018-339	Low
RHSA-2018:3157	Moderate	ASA-2018-346	Medium
RHSA-2018:3052	Moderate	ASA-2018-340	High
RHSA-2018:3221	Moderate	ASA-2018-350	Medium
RHSA-2018:3050	Moderate	ASA-2018-341	Medium
RHSA-2018:3327	Low	ASA-2018-352	Medium
RHSA-2018:3071	Low	ASA-2018-351	Medium
RHSA-2018:3140	Moderate	N/A	
RHSA-2018:3324	Moderate	ASA-2018-357	Medium
RHSA-2018:3059	Low	ASA-2018-354	Medium

RHSA-2018:3041	Moderate	ASA-2018-342	Medium
RHSA-2018:3107	Moderate	ASA-2018-347	High
RHSA-2018:2439	Moderate	ASA-2018-254	High
RHSA-2018:3665	Important	ASA-2019-011	High
RHSA-2018:2942	Critical	ASA-2018-331	High
RHSA-2018:1058	Important	ASA-2018-088	High

Security vulnerabilities resolved in Kernel Service Pack #5

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2018:2748	Important	ASA-2018-284	High
RHSA-2018:3083	Important	ASA-2018-359	Low
RHSA-2018:3651	Moderate	ASA-2018-381	High

Security vulnerabilities resolved in Security Service Pack #6

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2019:0049	Important	ASA-2019-009	High
RHSA-2019:0109	Important	ASA-2019-018	High
RHSA-2019:0194	Important	ASA-2019-020	High
RHSA-2019:0201	Low	ASA-2019-021	Low
RHSA-2019:0230	Low	ASA-2019-029	Low
RHSA-2019:0368	Important	ASA-2019-054	High
RHSA-2019:0679-01	Important	ASA-2019-075	High
RHSA-2019:0710-01	Important	ASA-2019-080	High
RHSA-2019:1228	Important	ASA-2019-106	High

CM 7.1 SSP #6 also includes an update to tzdata-2019a and updates to audispd-plugin, rsyslog, rsyslog-gnutls and libfastjson rpms.

Security vulnerabilities resolved in Kernel Service Pack #6

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2019:0163	Important	ASA-2019-019	High
RHSA-2019:0512	Important	ASA-2019-055	High
RHSA-2019:0818	Important	ASA-2019-084	High
RHSA-2019:1168	Important	ASA-2019-095	Medium

Security vulnerabilities resolved in Security Service Pack #7

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2018:3140	Moderate	N/A	N/A
RHSA-2019:0109	Important	ASA-2019-018	High
RHSA-2019:0447	Low	N/A	N/A

RHSA-2019:1587	Important	ASA-2019-120	Critical
RHSA-2019:1619	Important	ASA-2019-121	Medium
RHSA-2019:1880	Low	ASA-2019-178	High
RHSA-2019:1884	Moderate	ASA-2019-136	High
RHSA-2019:1898	Low	ASA-2019-135	Medium
RHSA-2019:1942	Important	N/A	N/A
RHSA-2019:1947	Important	N/A	N/A
RHSA-2019:2030	Moderate	ASA-2019-191	High
RHSA-2019:2033	Low	ASA-2019-196	Low
RHSA-2019:2046	Moderate	ASA-2019-152	High
RHSA-2019:2047	Moderate	ASA-2019-147	Medium
RHSA-2019:2049	Moderate	ASA-2019-169	Medium
RHSA-2019:2057	Moderate	ASA-2019-202	Medium
RHSA-2019:2060	Moderate	ASA-2019-194	Medium
RHSA-2019:2075	Moderate	ASA-2019-188	High
RHSA-2019:2077	Low	ASA-2019-189	High
RHSA-2019:2091	Moderate	ASA-2019-203	Medium
RHSA-2019:2110	Moderate	ASA-2019-211	Medium
RHSA-2019:2118	Moderate	ASA-2019-192	Medium
RHSA-2019:2136	Moderate	ASA-2019-185	Medium
RHSA-2019:2143	Low	ASA-2019-204	Medium
RHSA-2019:2181	Low	ASA-2019-183	Low
RHSA-2019:2189	Moderate	ASA-2019-158	Medium
RHSA-2019:2197	Low	ASA-2019-154	Medium
RHSA-2019:2237	Moderate	ASA-2019-205	Medium
RHSA-2019:2304	Moderate	ASA-2019-193	Medium
RHSA-2019:2327	Moderate	ASA-2019-155	Medium
RHSA-2019:2343	Moderate	ASA-2019-197	High
RHSA-2019:2896	Low	N/A	N/A
RHSA-2019:2964	Important	ASA-2019-227	High
RHSA-2019:3197	Important	ASA-2019-233	High
RHSA-2019:3286	Critical	ASA-2019-240	High

Security vulnerabilities resolved in Kernel Service Pack #7

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2019:1481	Important	ASA-2019-109	High
RHSA-2019:1873	Important	ASA-2019-207	High
RHSA-2019:2029	Important	ASA-2019-208	High
RHSA-2019:2600	Important	ASA-2019-220	Medium
RHSA-2019:2829	Important	ASA-2019-226	High

Security vulnerabilities resolved in Security Service Pack #8

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2019:0447	Low	N/A	N/A
RHSA-2019:2079	Moderate	N/A	N/a

RHSA-2019:2110	Moderate	ASA-2019-211	Medium
RHSA-2019:2159	Low	N/A	N/A
RHSA-2019:2169	Important	ASA-2019-144	High
RHSA-2019:2283	Low	N/A	N/A
RHSA-2019:2571	Important	ASA-2019-218	Critical
RHSA-2019:2896	Low	N/A	N/A
RHSA-2019:4190	Important	ASA-2019-247	High
RHSA-2019:4326	Important	ASA-2019-251	High
RHSA-2020:0196	Important	N/A	N/A
RHSA-2020:0227	Important	ASA-2020-008	High
RHSA-2020:0540	Important	ASA-2020-006	High

Security vulnerabilities resolved in Kernel Service Pack #8

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2019:3055	Important	ASA-2019-228	High
RHSA-2019:3834	Important	ASA-2019-237	Medium
RHSA-2019:3872	Important	ASA-2019-241	High
RHSA-2019:3979	Important	ASA-2019-245	High
RHBA-2019:4106	Bug Fix Advisory	N/A	N/A
RHSA-2020:0374	Important	ASA-2020-010	High

Security vulnerabilities resolved in Security Service Pack #9

In addition to the RHSA related issues below, fixes/updates were delivered for the following:

ID 31119: HostName in CM SMI disappears when we deactivate old and activate new SSP

ID 33870: tzdata-2020a-1.el7.noarch.rpm delivered

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2020:2432	Important	ASA-2020-083	Medium
RHSA-2020:2344	Important	ASA-2020-079	High
RHSA-2020:2894	Important	ASA-2020-092	Medium
RHSA-2020:3217	Moderate	ASA-2020-102	High
RHSA-2020:2663	Moderate	ASA-2020-090	High
RHSA-2020:0897	Important	ASA-2020-031	High
RHSA-2020:0630	Important	ASA-2020-017	Critical
RHSA-2020:1047	Moderate	ASA-2020-044	Medium
RHSA-2020:1020	Low	ASA-2020-040	Medium
RHSA-2020:1121	Moderate	ASA-2020-062	Medium
RHSA-2020:1022	Low	ASA-2020-043	Medium
RHSA-2020:1061	Moderate	ASA-2020-059	High
RHSA-2020:1011	Moderate	ASA-2020-037	Medium
RHSA-2020:1081	Moderate	ASA-2020-056	High

RHSA-2020:1113	Moderate	ASA-2020-061	Medium
RHSA-2020:1131	Moderate	ASA-2020-038	High
RHSA-2020:1000	Moderate	ASA-2020-041	High
RHSA-2020:1138	Low	ASA-2020-057	Medium
RHSA-2020:1021	Moderate	ASA-2020-033	Medium
RHSA-2020:1180	Moderate	ASA-2020-035	High
RHSA-2020:1112	Moderate	ASA-2020-046	Medium
RHSA-2020:0540	Important	ASA-2020-006	High
RHSA-2020:3952	Moderate	ASA-2020-116	Medium
RHSA-2020:1181	Low	ASA-2020-055	Low
RHSA-2020:1334	Important	ASA-2020-064	Critical
RHSA-2020:1185	Moderate	ASA-2020-047	High
RHSA-2020:1050	Moderate	ASA-2020-042	High
RHSA-2020:1176	Low	ASA-2020-049	Medium
RHSA-2020:1080	Moderate	ASA-2020-034	High
RHSA-2020:2968	Important	ASA-2020-098	High
RHSA-2020:1135	Low	ASA-2020-051	Medium
RHSA-2020:1100	Moderate	ASA-2020-032	Medium
RHSA-2020:4026	Moderate	ASA-2020-112	Medium
RHSA-2020:3878	Low	ASA-2020-114	Low
RHSA-2020:3902	Moderate	ASA-2020-139	High
RHSA-2020:3922	Low	ASA-2020-126	Low

Security vulnerabilities resolved in Kernel Service Pack #9

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2020:0834	Important	ASA-2020-026	High
RHSA-2020:1016	Moderate	ASA-2020-036	High
RHSA-2020:2082	Important	ASA-2020-075	High
RHBA-2020:2355	Bug Fix Advisory	N/A	N/A
RHSA-2020:2664	Important	ASA-2020-089	Medium
RHSA-2020:3220	Important	ASA-2020-103	High
RHBA-2020:3528	Bug Fix Advisory	N/A	N/A

Note Change in format starting with SSP and KSP #3 to show RHSA as well.

Security vulnerabilities resolved in Security Service Pack #3

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2018:0406	Moderate	ASA-2018-058	Medium
RHSA-2018:0483	Important	ASA-2018-055	High
RHSA-2018:0998	Moderate	ASA-2018-100	Medium
RHSA-2018:0805	Moderate	ASA-2018-103	High
RHSA-2018:0980	Low	ASA-2018-095	Medium
RHSA-2018:0855	Moderate	ASA-2018-101	Medium
RHSA-2018:0913	Low	ASA-2018-093	Low
RHSA-2018:0666	Moderate	ASA-2018-096	Medium

RHSA-2018:0849	Low	ASA-2018-099	Medium
RHSA-2018:1200	Important	ASA-2018-115	High
RHSA-2018:1453	Critical	ASA-2018-159	High
RHSA-2018:1700	Important	ASA-2018-173	High
RHSA-2018:0094	Important	ASA-2018-006	Medium

Security vulnerabilities resolved in Kernel Service Pack #3

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2018:1062	Important	ASA-2018-097	High
RHSA-2018:1318	Important	ASA-2018-141	High
RHSA-2018:1629	Important	ASA-2018-177	Medium

Security vulnerabilities resolved in Security Service Pack #4

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2018:2123	Moderate	ASA-2018-279	Low
RHSA-2018:2181	Important	ASA-2018-232	High

CM 7.1 SSP #4 also contains an updated tzdata: tzdata-2018e

Security vulnerabilities resolved in Kernel Service Pack #4

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2018:1852	Moderate	ASA-2018-229	Medium
RHSA-2018:1965	Important	ASA-2018-227	Medium
RHSA-2018:2384	Important	ASA-2018-270	Medium

CM 7.1 KSP #4 also contains a fix for this issue:

- CM-23336 Running “list measurements occupancy” with any option gives a blank table.

Security vulnerabilities resolved in Security Service Pack #5

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2018:2570	Important	ASA-2018-260	High
RHSA-2018:2768	Moderate	ASA-2018-293	Medium
RHSA-2018-3249	Low	ASA-2018-348	Medium
RHSA-2018-3092	Moderate	ASA-2018-375	High
RHSA-2018:3032	Low	ASA-2018-339	Low
RHSA-2018:3157	Moderate	ASA-2018-346	Medium
RHSA-2018:3052	Moderate	ASA-2018-340	High
RHSA-2018:3221	Moderate	ASA-2018-350	Medium
RHSA-2018:3050	Moderate	ASA-2018-341	Medium
RHSA-2018:3327	Low	ASA-2018-352	Medium
RHSA-2018:3071	Low	ASA-2018-351	Medium
RHSA-2018:3140	Moderate	N/A	
RHSA-2018:3324	Moderate	ASA-2018-357	Medium

RHSA-2018:3059	Low	ASA-2018-354	Medium
RHSA-2018:3041	Moderate	ASA-2018-342	Medium
RHSA-2018:3107	Moderate	ASA-2018-347	High
RHSA-2018:2439	Moderate	ASA-2018-254	High
RHSA-2018:3665	Important	ASA-2019-011	High
RHSA-2018:2942	Critical	ASA-2018-331	High
RHSA-2018:1058	Important	ASA-2018-088	High

Security vulnerabilities resolved in Kernel Service Pack #5

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2018:2748	Important	ASA-2018-284	High
RHSA-2018:3083	Important	ASA-2018-359	Low
RHSA-2018:3651	Moderate	ASA-2018-381	High

Security vulnerabilities resolved in Security Service Pack #6

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2019:0049	Important	ASA-2019-009	High
RHSA-2019:0109	Important	ASA-2019-018	High
RHSA-2019:0194	Important	ASA-2019-020	High
RHSA-2019:0201	Low	ASA-2019-021	Low
RHSA-2019:0230	Low	ASA-2019-029	Low
RHSA-2019:0368	Important	ASA-2019-054	High
RHSA-2019:0679-01	Important	ASA-2019-075	High
RHSA-2019:0710-01	Important	ASA-2019-080	High
RHSA-2019:1228	Important	ASA-2019-106	High

CM 7.1 SSP #6 also includes an update to tzdata-2019a and updates to audispd-plugin, rsyslog, rsyslog-gnutls and libfastjson rpms.

Security vulnerabilities resolved in Kernel Service Pack #6

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2019:0163	Important	ASA-2019-019	High
RHSA-2019:0512	Important	ASA-2019-055	High
RHSA-2019:0818	Important	ASA-2019-084	High
RHSA-2019:1168	Important	ASA-2019-095	Medium

Security vulnerabilities resolved in Security Service Pack #7

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2018:3140	Moderate	N/A	N/A
RHSA-2019:0109	Important	ASA-2019-018	High

RHSA-2019:0447	Low	N/A	N/A
RHSA-2019:1587	Important	ASA-2019-120	Critical
RHSA-2019:1619	Important	ASA-2019-121	Medium
RHSA-2019:1880	Low	ASA-2019-178	High
RHSA-2019:1884	Moderate	ASA-2019-136	High
RHSA-2019:1898	Low	ASA-2019-135	Medium
RHSA-2019:1942	Important	N/A	N/A
RHSA-2019:1947	Important	N/A	N/A
RHSA-2019:2030	Moderate	ASA-2019-191	High
RHSA-2019:2033	Low	ASA-2019-196	Low
RHSA-2019:2046	Moderate	ASA-2019-152	High
RHSA-2019:2047	Moderate	ASA-2019-147	Medium
RHSA-2019:2049	Moderate	ASA-2019-169	Medium
RHSA-2019:2057	Moderate	ASA-2019-202	Medium
RHSA-2019:2060	Moderate	ASA-2019-194	Medium
RHSA-2019:2075	Moderate	ASA-2019-188	High
RHSA-2019:2077	Low	ASA-2019-189	High
RHSA-2019:2091	Moderate	ASA-2019-203	Medium
RHSA-2019:2110	Moderate	ASA-2019-211	Medium
RHSA-2019:2118	Moderate	ASA-2019-192	Medium
RHSA-2019:2136	Moderate	ASA-2019-185	Medium
RHSA-2019:2143	Low	ASA-2019-204	Medium
RHSA-2019:2181	Low	ASA-2019-183	Low
RHSA-2019:2189	Moderate	ASA-2019-158	Medium
RHSA-2019:2197	Low	ASA-2019-154	Medium
RHSA-2019:2237	Moderate	ASA-2019-205	Medium
RHSA-2019:2304	Moderate	ASA-2019-193	Medium
RHSA-2019:2327	Moderate	ASA-2019-155	Medium
RHSA-2019:2343	Moderate	ASA-2019-197	High
RHSA-2019:2896	Low	N/A	N/A
RHSA-2019:2964	Important	ASA-2019-227	High
RHSA-2019:3197	Important	ASA-2019-233	High
RHSA-2019:3286	Critical	ASA-2019-240	High

Security vulnerabilities resolved in Kernel Service Pack #7

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2019:1481	Important	ASA-2019-109	High
RHSA-2019:1873	Important	ASA-2019-207	High
RHSA-2019:2029	Important	ASA-2019-208	High
RHSA-2019:2600	Important	ASA-2019-220	Medium
RHSA-2019:2829	Important	ASA-2019-226	High

Security vulnerabilities resolved in Security Service Pack #8

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2019:0447	Low	N/A	N/A

RHSA-2019:2079	Moderate	N/A	N/a
RHSA-2019:2110	Moderate	ASA-2019-211	Medium
RHSA-2019:2159	Low	N/A	N/A
RHSA-2019:2169	Important	ASA-2019-144	High
RHSA-2019:2283	Low	N/A	N/A
RHSA-2019:2571	Important	ASA-2019-218	Critical
RHSA-2019:2896	Low	N/A	N/A
RHSA-2019:4190	Important	ASA-2019-247	High
RHSA-2019:4326	Important	ASA-2019-251	High
RHSA-2020:0196	Important	N/A	N/A
RHSA-2020:0227	Important	ASA-2020-008	High
RHSA-2020:0540	Important	ASA-2020-006	High

Security vulnerabilities resolved in Kernel Service Pack #8

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2019:3055	Important	ASA-2019-228	High
RHSA-2019:3834	Important	ASA-2019-237	Medium
RHSA-2019:3872	Important	ASA-2019-241	High
RHSA-2019:3979	Important	ASA-2019-245	High
RHBA-2019:4106	Bug Fix Advisory	N/A	N/A
RHSA-2020:0374	Important	ASA-2020-010	High

Security vulnerabilities resolved in Security Service Pack #10

In addition to the RHSA related issues below, fixes/updates were delivered for the following:
ID 37068: tzdata-2020d-2.el7.noarch.rpm delivered

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2020:3848	Low	ASA-2020-137	Low
RHSA-2020:3861	Low	ASA-2020-124	Low
RHSA-2020:3864	Moderate	ASA-2020-129	Medium
RHSA-2020:3901	Low	ASA-2020-130	Low
RHSA-2020:3908	Moderate	ASA-2020-120	Medium
RHSA-2020:3911	Moderate	ASA-2020-134	Medium
RHSA-2020:3915	Moderate	ASA-2020-135	Medium
RHSA-2020:3958	Moderate	ASA-2020-142	Medium
RHSA-2020:3978	Moderate	ASA-2020-125	Medium
RHSA-2020:3996	Moderate	ASA-2020-122	High
RHSA-2020:4003	Moderate	ASA-2020-127	Medium
RHSA-2020:4005	Moderate	ASA-2020-138	High
RHSA-2020:4007	Low	ASA-2020-128	Low
RHSA-2020:4011	Moderate	ASA-2020-133	High

RHSA-2020:4032	Moderate	ASA-2020-136	High
RHSA-2020:4041	Moderate	ASA-2020-121	High
RHSA-2020:4072	Moderate	ASA-2020-131	High
RHSA-2020:4076	Moderate	ASA-2020-119	High
RHSA-2020:4350	Moderate	ASA-2020-148	Medium
RHSA-2020:4907	Important	ASA-2020-187	High
RHSA-2020:4908	Important	ASA-2020-182	High
RHSA-2020:5002	Moderate	ASA-2020-192	Medium
RHSA-2020:5009	Moderate	ASA-2020-201	High
RHSA-2020:5011	Moderate	ASA-2020-203	High
RHSA-2020:5083	Moderate	ASA-2020-193	Medium

Security vulnerabilities resolved in Kernel Service Pack #10

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2020:4060	Important	ASA-2020-140	High
RHBA-2020:4180	Bug Fix Advisory	N/A	N/A
RHSA-2020:4276	Important	ASA-2020-146	High
RHSA-2020:5023	Moderate	ASA-2020-186	Medium

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.