Product Correction Notice (PCN)

Issue Date: 08-June-2020
Supplement Date: 15-May-2023
Expiration Date: NA
PCN Number: 2122S

SECTION 1 - CUSTOMER NOTICE

Products affected by this PCN:

Avaya Aura® Appliance Virtualization Platform 8.1 running on Avaya S8300E, Common Servers R2 and R3 (Dell® PowerEdge R620, Dell® PowerEdge R630, HP® ProLiant DL 360p G8, HP® ProLiant DL 360 G9) and Avaya Converged Platform 120 (ACP 120 - Dell® PowerEdge R640).

Description:

NOTE: Beginning December 2020, PLAT Security Service Packs (SSPs) will be released on a more frequent cadence. This means that SSPs may also be available between application Service Packs/Feature Packs. These SSPs will also be available on PLDS and documented in this PCN. SSP required artifacts and fix IDs will no longer be tracked in the Avaya Aura 8.1.x Release Notes but will be included in this PCN.

15 May 2023 – Supplement 10 of this PCN **is informational only** to summarize that Avaya Aura® 8.x went End of Manufacturer Support (EOMS) on March 6, 2023 as noted in the *Product Lifecycle Notice*. ESXi 6.x went End of Life in October 2022. The final ESXi build 20502893 from VMware was provided in the final AVP SSP #15 from December 2022.

13-December-2022 – Supplement 9 of this PCN introduces **Security Service Pack #15** (PLAT-avaya-avp-e65-015.tar; **PLDS ID** AVP00000088) for Avaya Aura® Virtualization Platform 8.1.x.

- Since there was not an AVP Security Service Pack coincident with the June 2022 Aura 8.1.3.5 release, the AVP SSP numbering jumps from 13 to 15 to align with the AVP Utilities Security Service Pack numbering. AVP SSP#14 was never built. The current AVP release is 8.1.3.3.
- Security Service Pack #15 is applicable to any AVP 8.1.x.
- Reference PCN2097S for details on AVP version releases.
- AVP SSP #15 updates the ESXi Build to Releasebuild-20502893 Update: 3 Patch: 195

08-August-2022 – Supplement 8 of this PCN introduces **Security Service Pack #13** (PLAT-avaya-avp-e65-013.tar; **PLDS ID** AVP00000087) for Avaya Aura® Virtualization Platform 8.1.x.

- Since there was not an AVP Security Service Pack coincident with the June 2022 Aura 8.1.3.5 release, the AVP SSP numbering jumps from 11 to 13 to align with the AVP Utilities Security Service Pack numbering. AVP SSP#12 was never built. The current AVP release is 8.1.3.3.
- Security Service Pack #13 is applicable to any AVP 8.1.x.
- Reference PCN2097S for details on AVP version releases.
- AVP SSP #13 updates the ESXi Build to Releasebuild-19997716 Update: 3 Patch: 187

11 April 2022 – Supplement 7 of this PCN introduces **Security Service Pack #11** (PLAT-avaya-avp-e65-011.tar; **PLDS ID** AVP00000086) for Avaya Aura® Virtualization Platform 8.1.x.

- Since there was not an AVP Security Service Pack coincident with the February 2022 Aura

8.1.3.4 release, the AVP SSP numbering jumps from 9 to 11 to align with the AVP Utilities Security Service Pack numbering. AVP SSP#10 was never built. The current AVP release is 8.1.3.3.
- Security Service Pack #13 is applicable to any AVP 8.1.x.
- Security Service Pack #11 is applicable to any AVP 8.1.x.
- Reference PCN2097S for details on AVP version releases.
- AVP SSP #11 updates the ESXi Build to Releasebuild-19092475 Update: 3 Patch: 173

21 February 2022 – Supplement 6-1 of this PCN provides an update in **Section 1B – Security Information** to the list of **Security vulnerabilities resolved in Security Service Pack #9.** VMSA-2022-0001 has been added as resolved in **Security Service Pack #9**

20 December 2021 – Supplement 6 of this PCN introduces **Security Service Pack #9** (PLAT-avaya-avp-e65-009.tar; **PLDS ID** AVP00000085) for Avaya Aura® Virtualization Platform 8.1.x.
- Since there was not an AVP Security Service Pack coincident with the October 2021 AVP 8.1.3.3 release, the AVP SSP numbering jumps from 7 to 9 to align with the AVP Utilities Security Service Pack numbering. AVP SSP#8 was never built.
- Security Service Pack #9 is applicable to any AVP 8.1.x.
- Reference PCN2097S for details on AVP version releases.
- AVP SSP #9 updates the ESXi Build to Releasebuild-18678235 Update: 3 Patch: 170

Please note that this SSP does not have any VMSAs targeted in particular to ESXi 6.5 but only has the latest security bundle provided by VMware in order to stay updated.

9 August 2021 – Supplement 5 of this PCN introduces **Security Service Pack #7** (PLAT-avaya-avp-e65-007.tar; **PLDS ID** AVP00000082) for Avaya Aura® Virtualization Platform 8.1.x.
- Since there was not an AVP Security Service Pack coincident with the June 2021 AVP 8.1.3.2 release, the AVP SSP numbering jumps from 5 to 7 to align with the AVP Utilities Security Service Pack numbering. AVP SSP#6 was never built.
- Security Service Pack #7 is applicable to any AVP 8.1.x.
- Reference PCN2097S for details on AVP version releases.
- AVP SSP #7 updates the ESXi Build to Releasebuild-18071574 Update: 3 Patch: 161

5 April 2021 – Supplement 4 of this PCN introduces **Security Service Pack #5** (PLAT-avaya-avp-e65-005.tar; **PLDS ID** AVP00000079) for Avaya Aura® Virtualization Platform 8.1.x.
- Security Service Pack #7 is applicable to any AVP 8.1.x.
- Reference PCN2097S for details on AVP version releases.

17 February 2021 – Supplement 3-1 of this PCN provides an update in **Section 1B – Security Information** to the list of **Security vulnerabilities resolved in Security Service Pack #4.** VMSA-2020-0026 has been added as resolved in **Security Service Pack #4**

8 February 2021 – Supplement 3 of this PCN introduces **Security Service Pack #4** (PLAT-avaya-avp-e65-004.tar; **PLDS ID** AVP00000078) for Avaya Aura® Virtualization Platform 8.1.x.
- Security Service Pack #4 is applicable to any AVP 8.1.x.
- All fixes in AVP SSP#4 are already included in AVP 8.1.3.1, thus SSP#4 does not need to be applied on AVP 8.1.3.1.
- Reference PCN2097S for details on AVP version releases.

14 December 2020 – Supplement 2 of this PCN introduces **Security Service Pack #3**
(PLAT-avaya-avp-e65-003.tar; **PLDS ID** AVP00000073) for Avaya Aura® Virtualization Platform 8.1.x.

- Security Service Pack #3 is applicable to any AVP 8.1.x.
- Reference PCN2097S for details on AVP version releases.

12 October 2020 – **Supplement 1** of this PCN introduces **Security Service Pack #2**
(PLAT-avaya-avp-e65-002.tar; **PLDS ID** AVP00000068) for Avaya Aura® Virtualization Platform 8.1.x.

- Security Service Pack #2 is applicable to any AVP 8.1.x where the AVP version is <8.1.3.
- All fixes in AVP SSP#2 are already included in AVP 8.1.3, thus SSP#2 does not need to be applied on AVP 8.1.3.
- Reference PCN2097S for details on AVP version releases.

08 June 2020 – This PCN introduces **Security Service Pack #1**
(PLAT-avaya-avp-e65-001.tar; **PLDS ID** AVP00000065) for Avaya Aura® Virtualization Platform 8.1.x.
Please note that the security content already exists in the AVP 8.1.2 and 8.1.2.1 Service Pack. Hence this Security Service Pack should not be installed on the new 8.1.2.1 Service Pack.

- Security Service Pack #1 is applicable to any AVP 8.1.x where the AVP version is <8.1.2.
- Reference PCN2097S for details on AVP version releases.

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 required for Appliance Virtualization Platform 8.1.x.
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 will disrupt service since it will result in a full system reboot of the Appliance Virtualization Platform to take effect.

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 resolves 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. Mouse over **Search** at the top of the page 3. Type the ASA number of interest into the search field and Enter. 4. Click on the Security Advisory document link to read Scroll 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 **Community->Avaya Security.** 3. Click on the link for the year the security advisory was published, which is part of the ASA number. 4. Page through the advisory numbers to find the link of interest. Security Service Packs (SSP) are cumulative. This means that all fixes in previous 8.1.x SSPs are included in the most recent SSP.
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 Appliance Virtualization Platform 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 Appliance Virtualization Platform 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 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 select **LOG IN.** 2. Mouse over **Search Product** at the top of the page. 3. Begin to type **Appliance Virtualization Platform** and when Avaya Aura® Appliance Virtualization Platform appears as a selection below, select it. 4. Select 8.1.x from the **Choose Release** pull down menu to the right. 5. Select **Downloads** on the new page that is displayed. Scroll down (if necessary) and select **View All Downloads**. 6. Scroll down the page to find the download link for the required Security Service Pack. Click on the download link for the appropriate Security Service Pack. This will take you to the download page that also includes a link to this PCN and the Release Notes. 7. Select the file name link on this page to take you to the PLDS system with the **Download pub ID** already entered.

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 appropriate PLDS Download ID and select the **Download** link to begin the download:

PLDS Hints:

1. In the PLDS **View Downloads** section under the **Suggested Downloads** tab, select **Appliance Virtualization Platform** in the **Product Line** search field to display frequently downloaded Appliance Virtualization Platform software, including recent Service Packs and updates.
2. All Appliance Virtualization 8.1.x OVAs, Platform Security Service Packs, Platform Service Packs and Feature Packs are available on PLDS.

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):

Important Security Service Pack Installation Notes:

A service impacting reboot of AVP will occur after installation of the Security Service Pack.

1. AVP Security Service Packs are independent of the AVP Feature Pack or Service Pack. The Security Service Pack mentioned in this document can only be installed on 8.1.x AVP installation
2. If an AVP Feature Pack or Service Pack is being installed, the Security Service Pack of the same or the lower release should not be installed on the system. As new AVP 8.1 SSPs are released, they will be applicable to any 8.1.x AVP installation except for the corresponding Feature Pack or Service Pack released coincident with the SSP. For example, SSP #1 was released coincident with AVP 8.1.2.1. It is not necessary to apply SSP #1 on AVP 8.1.2.1 or 8.1.2 as all security updates in SSP #1 are included in both AVP 8.1.2 and AVP 8.1.2.1. It is also possible that an SSP will be released without a corresponding Feature Pack or Service Pack. In that case, it is applicable to all AVP versions. Always refer to this PCN to determine what AVP versions require a specific Security Service Pack.
3. The AVP Security Service Pack includes a pre-upgrade component/patch which is packaged inside the Security Service Pack bundle. It will be activated along with the Security Service Pack. The AVP pre-upgrade component/patch is NOT installed as a separate patch.
4. To activate the AVP Security Service Pack, perform the following steps:
    a. Activate SSH on AVP from the Solution Deployment Manager or execute “AVP_SSH enable” from AVP Utilities (AVPU).
    b. Login to AVP shell.
    c. Transfer the appropriate SSP, in this example we are using SSP #13, ***PLAT-avaya-avp-e65-013.tar***. Transfer the SSP to the following directory on AVP: /vmfs/volumes/server-local-disk/.

This can be done using the Secure Copy Protocol (SCP) utility on Linux or AVP, or a tool like WinSCP which is an SCP client for Windows.

d. Execute the following to unpack the SSP, replacing the SSP name in the command with the appropriate SSP to be installed:

```
[admin@Avp-17:~] tar -xf /vmfs/volumes/server-local-disk/PLAT-avaya-avp-e65-013.tar -C /vmfs/volumes/server-local-disk/
```

e. Execute the following to install the SSP, replacing the SSP name in the command with the appropriate SSP to be installed:

```
[admin@Avp-17:~] /vmfs/volumes/server-local-disk/PLAT-avaya-avp-e65-013/apply_ssp.sh
```

f. You will be required to accept the EULA:

g. You will be required to Confirm installation of the SSP which will require a reboot:

h. You will see progress status displayed. It will check for installation of the pre-upgrade patch. If not present, it will be installed. Then it will install the SSP.

i. The AVP system will go for a reboot after successful installation of the SSP.

j. Once AVP reboots, activate SSH on AVP from the Solution Deployment Manager or execute “AVP_SSH enable” from AVP Utilities (AVPU).

k. Login to AVP shell and execute:

```
admin@avp236:~] /opt/avaya/bin/swversion
# Maj.Min.FP.SP.PATCH.BUILD
Release: 8.1.3.3.0.02
Sprint: 34
Build: 2
git: 69f2dfe
Security Service Patch: PLAT-e65-013
Hotfix ID: None
VersionGet:
   Product: VMware ESXi
   Version: 6.5.0
   Build: Releasebuild-19997716
   Update: 3
   Patch: 187
```

5. The Security Service Pack is now installed and active on AVP.

6. **NOTE**: If an older Feature Pack or a Service Pack is applied on the latest Security Service Pack, then the latest Security Service Pack will have to be applied again.
For example, server is on AVP 8.1.3.0 and SSP #7 is applied. If AVP is then updated to 8.1.3.2, SSP #7 will need to be applied again.

SECTION 1A – SOFTWARE SERVICE PACK INFORMATION

Note: Customers are required to backup their application data before applying Plat Security Service Packs/Feature Packs.

How to verify the installation of the Service Pack has been successful:

Once AVP reboots, activate SSH on AVP from the Solution Deployment Manager or execute "AVP_SSH enable" from AVP Utilities (AVPU).

Login to AVP shell and execute the full path

```
[admin@Avp-17:~] /opt/avaya/bin/swversion
```

The output of the command should include the SSP and the Pre-upgrade patch. This example is from an AVP 8.1.3.3.0.02 after installing AVP 8.1 SSP #13:

```
# Maj.Min.FP.SP.PATCH.BUILD
Release: 8.1.3.3.0.02
Sprint: 34
Build: 2
git: 69f2dfe
Security Service Patch: PLAT-e65-013
Hotfix ID: None
VersionGet:
   Product: VMware ESXi
   Version: 6.5.0
   Build: Releasebuild-19997716
   Update: 3
   Patch: 187
```

```
[admin@Avp-17:~] /opt/avaya/bin/swversion | grep Security

Security Service Patch : PLAT-e65-013
```

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:

The AVP Security Service Pack cannot be removed.

SECTION 1B – SECURITY INFORMATION

Are there any security risks involved?

VMware Security Advisories (VMSAs) document remediation for security vulnerabilities reported in VMware products. Fixes for these vulnerabilities are included in the Security Service Pack. Security Service Packs (SSP) include the fixes from all previous SSPs for a given AVP 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 AVP 8.1 Security Service Pack #15

ID	VMSA Number	Common Vulnerability and Exposure (CVE) ID	CVE Severity	ASA Number	ASA Overall Severity
AVP-2087	VMSA-2022-0025	CVE-2022-31681	Low	NA	NA

Security vulnerabilities resolved in AVP 8.1 Security Service Pack #13

ID	VMSA Number	Common Vulnerability and Exposure (CVE) ID	CVE Severity	ASA Number	ASA Overall Severity
AVP-2083	VMSA-2022-0020	CVE-2022-29901 CVE-2022-28693 CVE-2022-23816 CVE-2022-23825	Moderate	NA	NA

Security vulnerabilities resolved in AVP 8.1 Security Service Pack #11

ID	VMSA Number	Common Vulnerability and Exposure (CVE) ID	CVE Severity	ASA Number	ASA Overall Severity
AVP-1966	VMSA-2022-0004	CVE-2021-22040 CVE-2021-22041 CVE-2021-22042 CVE-2021-22043 CVE-2021-22050	Important	NA	NA

Security vulnerabilities resolved in AVP 8.1 Security Service Pack #9

ID	VMSA Number	Common Vulnerability and Exposure (CVE) ID	CVE Severity	ASA Number	ASA Overall Severity
AVP-1747	VMSA-2022-0001	CVE-2021-22045	Important	NA	NA

Security vulnerabilities resolved in AVP 8.1 Security Service Pack #7

ID	VMSA Number	Common Vulnerability and Exposure (CVE) ID	CVE Severity	ASA Number	ASA Overall Severity
AVP-1582	VMSA-2021-0014	CVE-2021-21994 CVE-2021-21995	Important Moderate	NA	NA

Security vulnerabilities resolved in AVP 8.1 Security Service Pack #5

ID	VMSA Number	VMSA Severity	ASA Number	ASA Overall Severity

AVP-1338	VMSA-2021-0002	Critical	NA	NA

Security vulnerabilities resolved in AVP 8.1 Security Service Pack #4

ID	VMSA Number	VMSA Severity	ASA Number	ASA Overall Severity
AVP-1285	VMSA-2020-0026	Critical	NA	NA

Security vulnerabilities resolved in AVP 8.1 Security Service Pack #3

ID	VMSA Number	VMSA Severity	ASA Number	ASA Overall Severity
AVP-1251	VMSA-2020-0023	Critical	NA	NA

Security vulnerabilities resolved in AVP 8.1 Security Service Pack #2

VMSA Number	VMSA Severity	ASA Number	ASA Overall Severity
VMSA-2020-0018	Moderate	NA	NA
VMSA-2020-0015	Critical	NA	NA
VMSA-2020-0012	Important	NA	NA
VMSA-2020-0011	Moderate	ASA-2020-078	Medium

Security vulnerabilities resolved in AVP 8.1 Security Service Pack #1

VMSA Number	VMSA Severity	ASA Number	ASA Overall Severity
VMSA-2020-0008	Important	ASA-2020-072	High
VMSA-2019-0019	Moderate	NA	NA
VMSA-2019-0022	Critical	ASA-2020-001	Critical
VMSA-2019-0020	Moderate	NA	NA
VMSA-2019-0014	Important	NA	NA
VMSA-2019-0013	Important	NA	NA
VMSA-2019-0012	Important	NA	NA
VMSA-2019-0011	Moderate	NA	NA
VMSA-2019-0008	Moderate	NA	NA
VMSA-2019-0006	Important	NA	NA
VMSA-2019-0005	Critical	ASA-2019-079	Medium
VMSA-2018-0027	Critical	ASA-2019-067	High

Mitigation: Apply the latest AVP Security Service Pack.

SECTION 1C – ENTITLEMENTS AND CONTACTS

Material Coverage Entitlements: Appliance Virtualization Platform 8.1.x ISO image (for a new install of AVP) and a ZIP upgrade bundle (for upgrades from a previous AVP installation to AVP 8.1.x) are available free of charge to customers with a valid support contract for Appliance Virtualization Platform 8.1.x.

Avaya Customer Service Coverage 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

Entitlements:

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.