Product Correction Notice (PCN)

Issue Date:	**28-October-2019**
Supplement Date:	**08-May-2023**
Archive Date:	**Not Applicable**
PCN Number:	**2112S**

SECTION 1 - CUSTOMER NOTICE

Products affected by this PCN:

Session Manager servers running a release 8.1 software base load.
This is applicable for the following Session Manager offer types: Kernel-based Virtual Machine (KVM), Avaya Aura® Appliance Virtualization Platform (AVP), vAppliance running on Amazon Web Services (AWS) and Virtualized Environment

Description:

Beginning December 2020, SSPs will also 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 Release Notes but will be included in this PCN.

Avaya Aura® went End of Manufacturer Support (EOMS) on March 6, 2023 as noted in the Product Lifecycle Notice. Avaya is providing a final Security Service Pack on 8.1.x to cover vulnerabilities that were not able to be included in the February SSPs.

08-May-2023- Supplement 29 of this PCN introduces **Avaya Aura Session Manager 8.1 Security Service Pack #30 (Session_Manager_8.1-SSP-30001.bin PLDS ID: SM000000267)**

- Session Manager 8.1 SSP #30 is applicable to Session Manager 8.1.0 through 8.1.3.8
- Session Manager Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager service pack 8.1.3.4 onwards do NOT contain any Red Hat security updates. Therefore, it is NOT cumulative with respect to Red Hat security updates that were present in earlier 8.1.3.x Service Packs. SSP #30 must be installed after** applying the 8.1.3.4 or 8.1.3.5 or 8.1.3.6 or 8.1.3.7 or 8.1.3.8 Service Pack to ensure robust security protection.
  Reference PCN2099S for additional details on the Session Manager 8.1.3.x Service Packs.
- If SSP #21 is installed, SSP #30 **must** be applied as soon as possible to address the issues noted in **PSN020574u** and before applying any additional Service Packs.

21-February-2023- Supplement 28 of this PCN introduces **Avaya Aura Session Manager 8.1 Security Service Pack #29 (Session_Manager_8.1-SSP-29001.bin PLDS ID: SM000000259)**

- Session Manager 8.1 SSP #29 is applicable to Session Manager 8.1.0 through 8.1.3.7
- Session Manager Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager service pack 8.1.3.4 onwards do NOT contain any Red Hat security updates. Therefore, it is NOT cumulative with respect to Red Hat security updates that were present in earlier 8.1.3.x Service Packs. SSP #29 must be installed after** applying the 8.1.3.4 or 8.1.3.5 or 8.1.3.6 or 8.1.3.7 Service Pack to ensure robust security protection.
  Reference PCN2099S for additional details on the Session Manager 8.1.3.x Service Packs.
- If SSP #21 is installed, SSP #29 **must** be applied as soon as possible to address the issues noted in **PSN020574u** and before applying any additional Service Packs.

9-January-2023- Supplement 27 of this PCN introduces **Avaya Aura Session Manager 8.1 Security Service Pack #28 (Session_Manager_8.1-SSP-28001.bin PLDS ID: SM000000252)**

- Session Manager 8.1 SSP #28 is applicable to Session Manager 8.1.0 through 8.1.3.6
- Session Manager Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager service pack 8.1.3.4 onwards do NOT contain any Red Hat security updates. Therefore, it is NOT cumulative with respect to Red Hat security updates that were present in earlier 8.1.3.x Service Packs. SSP #28 must be installed after** applying the 8.1.3.4 or 8.1.3.5 or 8.1.3.6 Service Pack to ensure robust security protection.
  Reference PCN2099S for additional details on the Session Manager 8.1.3.x Service Packs.
- If SSP #21 is installed, SSP #28 **must** be applied as soon as possible to address the issues noted in **PSN020574u** and before applying any additional Service Packs.

13-December-2022- Supplement 26 of this PCN introduces **Avaya Aura Session Manager 8.1 Security Service Pack #27 (Session_Manager_8.1-SSP-27001.bin PLDS ID: SM000000250)**

- Session Manager 8.1 SSP #27 is applicable to Session Manager 8.1.0 through 8.1.3.6
- Session Manager Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager service pack 8.1.3.4 onwards do NOT contain any Red Hat security updates. Therefore, it is NOT cumulative with respect to Red Hat security updates that were present in earlier 8.1.3.x Service Packs. SSP #27 must be installed after** applying the 8.1.3.4 or 8.1.3.5 or 8.1.3.6 Service Pack to ensure robust security protection.
  Reference PCN2099S for additional details on the Session Manager 8.1.3.x Service Packs.
- If SSP #21 is installed, SSP #27 **must** be applied as soon as possible to address the issues noted in **PSN020574u** and before applying any additional Service Packs.

14-November-2022- Supplement 25 of this PCN introduces **Avaya Aura Session Manager 8.1 Security Service Pack #26 (Session_Manager_8.1-SSP-26001.bin PLDS ID: SM000000247)**

- Session Manager 8.1 SSP #26 is applicable to Session Manager 8.1.0 through 8.1.3.6
- Session Manager Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager service pack 8.1.3.4 onwards do NOT contain any Red Hat security updates. Therefore, it is NOT cumulative with respect to Red Hat security updates that were present in earlier 8.1.3.x Service Packs. SSP #26 must be installed after** applying the 8.1.3.4 or 8.1.3.5 or 8.1.3.6 Service Pack to ensure robust security protection.
  Reference PCN2099S for additional details on the Session Manager 8.1.3.x Service Packs.
- If SSP #21 is installed, SSP #26 **must** be applied as soon as possible to address the issues noted in **PSN020574u** and before applying any additional Service Packs.

24-October-2022- Supplement 24 of this PCN introduces **Avaya Aura Session Manager 8.1 Security Service Pack #25 (Session_Manager_8.1-SSP-25001.bin PLDS ID: SM000000244)**

- Session Manager 8.1 SSP #25 is applicable to Session Manager 8.1.0 through 8.1.3.6
- Session Manager Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager service pack 8.1.3.4 onwards do NOT contain any Red Hat security updates. Therefore, it is NOT cumulative with respect to Red Hat security updates that were present in earlier 8.1.3.x Service Packs. SSP #25 must be installed after** applying the 8.1.3.4 or 8.1.3.5 or 8.1.3.6 Service Pack to ensure robust security protection.

Reference PCN2099S for additional details on the Session Manager 8.1.3.x Service Packs.

- If SSP #21 is installed and SSP #22/#23/#24 were not installed, SSP #25 **must** be applied as soon as possible to address the issues noted in **PSN020574u** and before applying any additional Service Packs.

12-September-2022- Supplement 23 of this PCN introduces **Avaya Aura Session Manager 8.1 Security Service Pack #24 (Session_Manager_8.1-SSP-24001.bin PLDS ID: SM000000241)**

- Session Manager 8.1 SSP #24 is applicable to Session Manager 8.1.0 through 8.1.3.5
- Session Manager Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 8.1.3.4 and 8.1.3.5 Service Packs do NOT contain any Red Hat security updates. Therefore, it is NOT cumulative with respect to Red Hat security updates that were present in earlier 8.1.3.x Service Packs. SSP #24 must be installed** after applying the 8.1.3.4 or 8.1.3.5 Service Pack to ensure robust security protection. Reference PCN2099S for additional details on the Session Manager 8.1.3.x Service Packs.
- If SSP #21 is installed and SSP #22 or #23 were not installed, SSP #24 **must** be applied as soon as possible to address the issues noted in **PSN020574u** and before applying any additional Service Packs.

8-August-2022- Supplement 22 of this PCN introduces **Avaya Aura Session Manager 8.1 Security Service Pack #23 (Session_Manager_8.1-SSP-23001.bin PLDS ID: SM000000238)**

- Session Manager 8.1 SSP #23 is applicable to Session Manager 8.1.0 through 8.1.3.5
- Session Manager Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 8.1.3.4 and 8.1.3.5 Service Packs do NOT contain any Red Hat security updates. Therefore, it is NOT cumulative with respect to Red Hat security updates that were present in earlier 8.1.3.x Service Packs. SSP #23 must be installed** after applying the 8.1.3.4 or 8.1.3.5 Service Pack to ensure robust security protection. Reference PCN2099S for additional details on the Session Manager 8.1.3.x Service Packs.
- If SSP #21 is installed and SSP #22 was not installed, SSP #23 **must** be applied as soon as possible to address the issues noted in **PSN020574u** and before applying any additional Service Packs.

18-July-2022- Supplement 21 of this PCN introduces **Avaya Aura Session Manager 8.1 Security Service Pack #22 (Session_Manager_8.1-SSP-22002.bin PLDS ID: SM000000236)**

- Session Manager 8.1 SSP #22 is applicable to Session Manager 8.1.0 through 8.1.3.5
- Session Manager Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 8.1.3.4 and 8.1.3.5 Service Packs do NOT contain any Red Hat security updates. Therefore, it is NOT cumulative with respect to Red Hat security updates that were present in earlier 8.1.3.x Service Packs. SSP #22 must be installed** after applying the 8.1.3.4 or 8.1.3.5 Service Pack to ensure robust security protection. Reference PCN2099S for additional details on the Session Manager 8.1.3.x Service Packs.
- If SSP #21 is already installed, SSP #22 **must** be applied as soon as possible to address the issues noted in **PSN020574u** and before applying any additional Service Packs.

06-July-2022- Supplement 20-1

- **ALERT!! : SSP #21, which includes OpenJDK updates, results in Cassandra/User Data Storage issues. For now, this SSP is disabled from the support site. Reference PSN020574u for additional details.**

13-June-2022- Supplement 20 of this PCN introduces **Avaya Aura Session Manager 8.1 Security Service Pack #21 (~~Session_Manager_8.1-SSP-21001.bin; PLDS ID: SM000000233~~)**

- Session Manager 8.1 SSP #21 is applicable to Session Manager 8.1.0 through 8.1.3.5 (8.1.3.5 target GA June 21, 2022).
- Session Manager Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 8.1.3.4 and 8.1.3.5 Service Packs do NOT contain any Red Hat security updates. Therefore, it is NOT cumulative with respect to Red Hat security updates that were present in earlier 8.1.3.x Service Packs. SSP #21 must be installed** after applying the 8.1.3.4 or 8.1.3.5 Service Pack to ensure robust security protection. Reference PCN2099S for additional details on the Session Manager 8.1.3.x Service Packs.

Disabled – see Supplement 20-1 above.

09-May-2022- Supplement 19 of this PCN introduces **Avaya Aura Session Manager 8.1 Security Service Pack #20 (Session_Manager_8.1-SSP-20001.bin; PLDS ID: SM000000231)**

- Session Manager 8.1 SSP #20 is applicable to Session Manager 8.1.0 through 8.1.3.4
- Session Manager Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 8.1.3.4 Service Pack does NOT contain any Red Hat security updates. Therefore, it is NOT cumulative with respect to Red Hat security updates that were present in earlier 8.1.3.x Service Packs. SSP #20 must be installed** after applying the 8.1.3.4 Service Pack to ensure robust security protection. Reference PCN2099S for additional details on the Session Manager 8.1.3.4 Service Pack.

11-April-2022- Supplement 18 of this PCN introduces **Avaya Aura Session Manager 8.1 Security Service Pack #19 (Session_Manager_8.1-SSP-19002.bin; PLDS ID: SM000000230)**

- Session Manager 8.1 SSP #19 is applicable to Session Manager 8.1.0 through 8.1.3.4
- Session Manager Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 8.1.3.4 Service Pack does NOT contain any Red Hat security updates. Therefore, it is NOT cumulative with respect to Red Hat security updates that were present in earlier 8.1.3.x Service Packs. SSP #19 must be installed** after applying the 8.1.3.4 Service Pack to ensure robust security protection. Reference PCN2099S for additional details on the Session Manager 8.1.3.4 Service Pack.

14-March-2022- Supplement 17 of this PCN introduces **Avaya Aura Session Manager 8.1 Security Service Pack #18 (Session_Manager_8.1-SSP-18002.bin; PLDS ID: SM000000227)**

- Session Manager 8.1 SSP #18 is applicable to Session Manager 8.1.0 through 8.1.3.4
- Session Manager Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 8.1.3.4 Service Pack does NOT contain any Red Hat security updates. Therefore, it is NOT cumulative with respect to Red Hat security updates that were present in earlier 8.1.3.x Service Packs. SSP #18 must be installed** after applying the 8.1.3.4 Service Pack to ensure robust security protection. Reference PCN2099S for additional details on the Session Manager 8.1.3.4 Service Pack.

22-February-2022- Supplement 16 of this PCN introduces **Avaya Aura Session Manager 8.1 Security Service Pack #17 (Session_Manager_8.1-SSP-17001.bin; PLDS ID: SM000000224)**

- Session Manager 8.1 SSP #17 is applicable to Session Manager 8.1.0 through 8.1.3.4
- Session Manager Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 8.1.3.4 Service Pack does NOT contain any Red Hat security updates. Therefore, it is NOT cumulative with respect to Red Hat security updates that were present in earlier 8.1.3.x Service Packs. ~~SSP #17 must be installed after applying the 8.1.3.4 Service Pack to ensure robust security protection. Reference PCN2099S for additional details on the Session Manager 8.1.3.4 Service Pack.~~**
  Updated: *see **Supplement 17** above.*

10-January-2022- Supplement 15 of this PCN introduces **Avaya Aura Session Manager 8.1 Security Service Pack #16 (Session_Manager_8.1-SSP-16001.bin; PLDS ID: SM000000221)**

- Session Manager 8.1 SSP #16 is applicable to Session Manager 8.1.0 through 8.1.3.3
- Session Manager Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 8.1.3.3 Service Pack does NOT contain any security updates. Therefore, it is NOT cumulative with respect to Red Hat security updates that were present in earlier 8.1.3.x Service Packs. SSP #16 must be installed** after applying the 8.1.3.3 Service Pack to ensure robust security protection. Reference PCN2099S for additional details on the Session Manager 8.1.3.3 Service Pack.

20-December-2021- Supplement 14 of this PCN introduces **Avaya Aura Session Manager 8.1 Security Service Pack #15 (Session_Manager_8.1-SSP-15001.bin; PLDS ID: SM000000216)**

- Session Manager 8.1 SSP #15 is applicable to Session Manager 8.1.0 through 8.1.3.3
- Session Manager Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 8.1.3.3 Service Pack does NOT contain any security updates. Therefore, it is NOT cumulative with respect to Red Hat security updates that were present in earlier 8.1.3.x Service Packs. SSP #15 must be installed** after applying the 8.1.3.3 Service Pack to ensure robust security protection. Reference PCN2099S for additional details on the Session Manager 8.1.3.3 Service Pack.

15-November-2021- Supplement 13 of this PCN introduces **Avaya Aura Session Manager 8.1 Security Service Pack #14 (Session_Manager_8.1-SSP-14003.bin; PLDS ID: SM000000209)**

- Session Manager 8.1 SSP #14 is applicable to Session Manager 8.1.0 through 8.1.3.3
- Session Manager Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 8.1.3.3 Service Pack does NOT contain any security updates. Therefore, it is NOT cumulative with respect to Red Hat security updates that were present in earlier 8.1.3.x Service Packs. ~~SSP #14 must be installed after applying the 8.1.3.3 Service Pack to ensure robust security protection. Reference PCN2099S for additional details on the Session Manager 8.1.3.3 Service Pack~~.**
  ~~Updated:~~ *~~see **Supplement 14** above.~~*
  ~~Updated:~~ *~~see **Supplement 15** above.~~*
  Updated: *see **Supplement 17** above.*

11-October-2021- Supplement 12 of this PCN introduces **Avaya Aura Session Manager 8.1 Security Service Pack #13 (Session_Manager_8.1-SSP-13001.bin; PLDS ID: SM000000207)**

- Session Manager 8.1 SSP #13 is applicable to Session Manager 8.1.0 through 8.1.3.3
- Session Manager Security Service Packs should NOT be applied on the Software Only Offer.

- **Critical Note: Session Manager 8.1.3.3 Service Pack does NOT contain any security updates. Therefore, it is NOT cumulative with respect to Red Hat security updates that were present in earlier 8.1.3.x Service Packs. ~~SSP #13 must be installed after applying the 8.1.3.3 Service Pack to ensure robust security protection. Reference PCN2099S for additional details on the Session Manager 8.1.3.3 Service Pack.~~**
  Updated: *see **Supplement 13** above.*

06-September-2021- Supplement 11 of this PCN introduces **Avaya Aura Session Manager 8.1 Security Service Pack #12 (Session_Manager_8.1-SSP-12001.bin; PLDS ID: SM000000205)**

- Session Manager 8.1 SSP #12 is applicable to Session Manager 8.1.0 through 8.1.3.2
- Session Manager Security Service Packs should NOT be applied on the Software Only Offer.

09-August-2021- Supplement 10 of this PCN introduces **Avaya Aura Session Manager 8.1 Security Service Pack #11 (Session_Manager_8.1-SSP-11001.bin; PLDS ID: SM000000204)**

- Session Manager 8.1 SSP #11 is applicable to Session Manager 8.1.0 through 8.1.3.2
- Session Manager Security Service Packs should NOT be applied on the Software Only Offer.

12-July-2021- Supplement 9 of this PCN introduces **Avaya Aura Session Manager 8.1 Security Service Pack #10 (Session_Manager_8.1-SSP-10002.bin; PLDS ID: SM000000203)**

- Session Manager 8.1 SSP #10 is applicable to Session Manager 8.1.0 through 8.1.3.2
- Session Manager Security Service Packs should NOT be applied on the Software Only Offer.

14-June-2021- Supplement 8 of this PCN introduces **Avaya Aura Session Manager 8.1 Security Service Pack #9 (Session_Manager_8.1-SSP-09002.bin; PLDS ID: SM000000201)**

- Session Manager 8.1 SSP #9 is applicable to Session Manager 8.1.0 through 8.1.3.2
  - Session Manager 8.1.3.2 has a tentative GA date of June 21, 2021.
  - Session Manager 8.1.3.2 will only contain the security updates in SSP#8.
  - Therefore, SSP #9 should be applied to Session Manager 8.1.3.2 when it launches to ensure robust security protection.
- Session Manager Security Service Packs should NOT be applied on the Software Only Offer.

10-May-2021- Supplement 7 of this PCN introduces **Avaya Aura Session Manager 8.1 Security Service Pack #8 (Session_Manager_8.1-SSP-08001.bin; PLDS ID: SM000000200)**

- This Security Service Pack is only applicable to SM 8.1.0 through 8.1.3.1.
- SM Security Service Packs should NOT be applied on the Software Only Offer.

05-April-2021- Supplement 6 of this PCN introduces **Avaya Aura Session Manager 8.1 Security Service Pack #7 (Session_Manager_8.1-SSP-07002.bin; PLDS ID: SM000000198)**

- This Security Service Pack is only applicable to SM 8.1.0 through 8.1.3.1.
- SM Security Service Packs should NOT be applied on the Software Only Offer.

08-February-2021- Supplement 5 of this PCN introduces **Avaya Aura Session Manager 8.1 Security Service Pack #6 (Session_Manager_8.1-SSP-06002.bin; PLDS ID: SM000000195)**

- This Security Service Pack is only applicable to SM 8.1.0 through 8.1.3.0.
- All fixes in SM SSP#6 are already included in SM 8.1.3.1, thus SSP#6 should NOT be applied on SM 8.1.3.1 or later SM.

- SM Security Service Packs should NOT be applied on the Software Only Offer.

14-December-2020- Supplement 4 of this PCN introduces **Avaya Aura Session Manager 8.1 Security Service Pack #5 (Session_Manager_8.1-SSP-05003.bin; PLDS ID: SM000000191)**

- This Security Service Pack is only applicable to SM 8.1.0 through 8.1.3.0.
- SM Security Service Packs should NOT be applied on the Software Only Offer.

12-October-2020 – Supplement 3 of this PCN introduces **Avaya Aura Session Manager 8.1 Security Service Pack #4 (Session_Manager_8.1-SSP-04004.bin; PLDS ID SM000000188).**

- This Security Service Pack is only applicable to SM 8.1.0 through 8.1.2.1.
- All fixes in SM SSP#4 are already included in SM 8.1.3.0, thus SSP#4 should NOT be applied on SM 8.1.3.0 or later SM.
- SM Security Service Packs should NOT be applied on the Software Only Offer.

08-June-2020 – Supplement 2 of this PCN introduces **Avaya Aura Session Manager 8.1 Security Service Pack #3 (Session_Manager_8.1-SSP-03002.bin; PLDS ID SM000000183).**

- This Security Service Pack is only applicable to SM 8.1.0 through 8.1.2.0.
- All fixes in SM SSP#3 are already included in SM 8.1.2.1, thus SSP#3 should NOT be applied on SM 8.1.2.1 or later SM.
- SM Security Service Packs should NOT be applied on the Software Only Offer.

02-March-2020 – Supplement 1 of this PCN introduces **Avaya Aura Session Manager 8.1 Security Service Pack #2 (Session_Manager_8.1-SSP-008.bin; PLDS ID SM000000174).**

- This Security Service Pack is only applicable to SM 8.1.0 through 8.1.1.0.
- All fixes in SM SSP#2 are already included in SM 8.1.2.0, thus SSP#2 should NOT be applied on SM 8.1.2.0 or later SM.
- SM Security Service Packs should NOT be applied on the Software Only Offer.

28-October-2019 – This PCN introduces **Avaya Aura Session Manager 8.1 Security Service Pack #1 (Session_Manager_8.1-SSP-005.bin; PLDS ID SM000000168).**

- This Security Service Pack is only applicable to SM 8.1.0 .
- All fixes in SM SSP#1 are already included in SM 8.1.1.0, thus SSP#1 should NOT be applied on SM 8.1.1.0 or later SM.
- SM Security Service Packs should NOT be applied on the Software Only Offer.

*

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?	**Note: SSP# 30 can be applied to SM 8.1.0 through 8.1.3.8 Session Manager.**

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 applies to both US and non-US customers.
Does applying this PCN disrupt my service during installation?	This security service Pack will disrupt service in that it requires a system reboot to take effect. Since Session Manager runs in an active-active environment, when multiple Session Manager instances are in a network, the servers should be updated one at a time to minimize any service impact. If only one Session Manager server is in the configuration, service will be impacted during the upgrade time, and should be planned for accordingly.
Installation of this PCN is required by:	Customer and/or (Avaya Remote or On-Site Services) and/or Avaya Authorized Business Partner.
Release notes and workarounds are located:	The **Avaya Aura® Session Manager Release 8.1 Release Notes** can be obtained by performing the following steps from a browser: 1. Go to http://support.avaya.com 2. Search for the document titled "**Avaya Aura® Session Manager Release 8.1 Release 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 Session 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 Session 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):	Software can be downloaded directly from support.avaya.com. No order is required. 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 click **LOG IN.** 2. Mouse over **Search Product** at the top of the page. 3. Begin to type **Session Manager** and when Avaya Aura® Session Manager 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. Select **Avaya Aura® Session Manager 8.1 Security Service Pack.** 7. Click on the download link for the bin 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 **Session Manager** in the **Product Line** search field to display frequently downloaded Communication Manager software, including recent Service Packs and other software updates.
2. All Session Manager 8.1.x software downloads are available on PLDS. In the PLDS **View Downloads** section under the **Search by Download** tab, select **Session Manager** in the **Application** search field and **8.1** in the **Version** search field to display all available Communication Manager 8.1 software downloads.

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

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

Important Security Service Pack Installation Notes:

Installation using CLI

1. Download the Security Service Pack binary and place it in the customer account home directory. (e.g. /home/cust)
2. Take a VM snapshot prior to making changes.
3. Place the SM in **Deny New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
    c. Click **Service State**.
    d. From the drop-down list box, select **Deny New Service**.
    e. Before updating on the confirmation page, click **Confirm**.
4. On the **Session Manager Dashboard** page, wait until **Active Call Count** is zero. Refresh the screen to update the count.
5. Using the customer account, install the patch using **patchSM.**

For example,

 # patchSM /home/cust/Session_Manager_8.1-SSP-30001.bin

Confirm the installation by selecting "y" when prompted.

6. The system will reboot after the patch install completes.
7. Verify the patch.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. For the Session Manager, verify that all tests are passing, entity links are up, data replication, and user data storage (core SMs only).

8. Remove the VM snapshot.
9. Place the SM in **Accept New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
    c. Click **Service State**.
    d. From the drop-down list box, select **Accept New Service**.
    e. Before updating on the confirmation page, click **Confirm**.

Installation using SDM

1. Download the Security Service Pack binary and place on System Manager under /swlibrary/staging/sync/.
2. Place the SM in **Deny New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
    c. Click **Service State**.
    d. From the drop-down list box, select **Deny New Service**.
    e. Before updating on the confirmation page, click **Confirm**.
3. On the **Session Manager Dashboard** page, wait until **Active Call Count** is zero. Refresh the screen to update the count.
4. Add patch to SDM Software Library.
    a. On the home page of System Manager Web Console, Under **Services**, click **Solution Deployment Manager**.
    b. Select **Software Library Management.**
    c. Select **Manage Files.**
    d. In the **Sync Files from directory** section select the SSP.
        i. Enter SHA256 Checksum. The command **sha256sum** from the command line can be used to calculate it.
        ii. Select the desired software library.
        iii. The product family should be **Session Manager** or **Branch Session Manager** depending on the type of Session Manager being patched.
        iv. Device Type should set to **Custom Patch.**
    e. Click **Sync.**
5. Select **Upgrade Management** link on the left-hand menu.
6. Select the Session Manager or Branch Session Manager to update.
7. Under the **Upgrade Actions** button select **Custom Patching.**
8. On the **Upgrade Configuration** page click the **Edit** button**.**
    a. For **Upgrade Source** select the software library containing the patch.
    b. Select the SSP from the file list.
    c. Read and accept the **End User License Agreement.**
    d. Click **Save.**
9. On the **Upgrade Configuration** page click the **Upgrade** button**.**
    a. (Optional)Enter a **Job Name**
    b. (Optional) Select a date in the future for applying the patch.
    c. Click the **Schedule** button.
10. After the patch finishes install, verify the patch.

a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
b. For the Session Manager, verify that all tests are passing, entity links are up, data replication, and user data storage (core SMs only).

11. Commit the patch.
    a. On the **Upgrade Management** page click the **Upgrade Actions** button select **Installed Patches.**
    b. Under **Patch Operation** select **Commit.**
    c. Select the patch and click **Schedule.**
12. Place the SM in **Accept New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
    c. Click **Service State**.
    d. From the drop-down list box, select **Accept New Service**.
    e. Before updating on the confirmation page, click **Confirm**

Note: If you try to install this SSP#8 on top of SM 8.1.3.2 using ASM CLI, it will give you following message as it contains all the fixes which are incorporated in SSP#8.

```
"Security Service Pack 8.1-SSP-08001 is already installed."
```

** If you try to install this SSP#8 using SDM on top of SM 8.1.3.2 SDM installation will remain in stuck state. To recover and remove stuck SDM job, please engage product house.

Note: SSP #30 can be applied to SM 8.1.0 through 8.1.3.8 Session Manager.

SECTION 1A – SOFTWARE FEATURE PACK INFORMATION

Note: Customers are required to backup their systems before applying the Service Pack.

How to verify the installation of the Software has been successful:

The **Upgrading Avaya Aura Session Manager** and **Installing Service Packs for Avaya Aura Session Manager** documents contain details on how to ensure the update(s) installed correctly. You can also confirm the software was installed correctly by confirming the software version displayed for the Session Manager in the System Manger web interface.

To determine the release of Session Manager software that is being run on a server you can:

- Via a browser, log into the System Manager used to manage the targeted Session Manager server/instance.
- Navigate to **Session Manager -> Dashboard.**
- The current Session Manager version can be viewed in the "**Version**" column

```
ID                   Version        Status    Summary
-------------------- -------------- --------- --------------------------------
8.1-SSP-30001        30001          installed Security Service Pack #30
```

What you

Escalate to Avaya **Global Support Services (GSS)** or an Avaya authorized Business Partner.

should do if the Software installation fails?	
How to remove the Software if malfunction of your system occurs:	The **Upgrading Avaya Aura® Session Manager** document and **Upgrading and Migrating Avaya Aura® Applications to 8.1** contains instructions on how to upgrade Session Manager release 8.1.X and later systems to release 8.1.3.6, 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 select **LOG IN** 2. Mouse over **Product Support** at the top of the page and select **Documents** in the drop down menu. 3. Mouse over **Search Product**. 4. Begin to type **Session Manager** and when Avaya Aura® Session Manager appears as a selection below, select it. 5. Select release **8.1.x** from the **Choose Release** pull down menu to the right. 6. Select **Installation, Upgrades & Config** from the **Select Content Type** box on the right**.** 7. Search for the document titled "**Upgrading Avaya Aura® Session Manager"** & **"Upgrading and Migrating Avaya Aura® Applications to 8.1".** **Contact Avaya Services for assistance if the system is not operating properly after the upgrade to this release. Alternatively, a rollback can be performed by re-installing all software on the Session Manager server per the server replacement procedures in the Maintenance and Troubleshooting guide.**

SECTION 1B – SECURITY INFORMATION

Security Notes	In keeping with NIST guidelines and industry best practices, Avaya is rotating the security keys associated with remote maintenance access through the Access Security Gateway.
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 as noted.
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. **As noted in the Description section of this PCN, SSP and KSP 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.** **Beginning with SM SSP#8, the format of the information in this section is expanded.**

SM 8.1 Security Service Pack #30 includes the following rpm updates:

bind-32:9.11.4-26.P2.el7_9.13.x86_64.rpm	nss-3.79.0-5.el7_9.x86_64.rpm
bind-libs-32:9.11.4-26.P2.el7_9.13.x86_64.rpm	nss-sysinit-3.79.0-5.el7_9.x86_64.rpm
bind-libs-lite-32:9.11.4-26.P2.el7_9.13.x86_64.rpm	nss-tools-3.79.0-5.el7_9.x86_64.rpm
bind-license-32:9.11.4-26.P2.el7_9.13.noarch.rpm	openssl-1:1.0.2k-26.el7_9.x86_64.rpm
bind-utils-32:9.11.4-26.P2.el7_9.13.x86_64.rpm	openssl-libs-1:1.0.2k-26.el7_9.x86_64.rpm
kernel-3.10.0-1160.88.1.el7.x86_64.rpm	perf-3.10.0-1160.88.1.el7.x86_64.rpm
kernel-tools-3.10.0-1160.88.1.el7.x86_64.rpm	python-perf-3.10.0-1160.88.1.el7.x86_64.rpm

kernel-tools-libs-3.10.0-1160.88.1.el7.x86_64.rpm	zlib-1.2.7-21.el7_9.x86_64.rpm

Security vulnerabilities resolved in SM 8.1 Security Service Pack #30

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-90725	openssl openssl-libs	RHSA-2023:1335	CVE-2023-0286	Important	ASA-2021-189	High
ASM-90801	nss nss-sysinit nss-tools	RHSA-2023:1332	CVE-2023-0767	Important	None	None
ASM-90800	zlib	RHSA-2023:1095	CVE-2022-37434	Moderate	None	None
ASM-90723	kernel kernel-tools kernel-tools-libs perf python-perf	RHSA-2023:1091	CVE-2022-4378 CVE-2022-42703	Important	ASA-2021-189	High
ASM-90414	bind bind-libs bind-libs-lite bind-license bind-utils	RHSA-2023:0402	CVE-2021-25220 CVE-2022-2795	Moderate	ASA-2022-018	Medium
ASM-90661	kernel kernel-tools kernel-tools-libs perf python-perf	RHSA-2023:0399	CVE-2021-26401 CVE-2022-2964	Important	None	None

SM 8.1 Security Service Pack #29 includes the following rpm updates:

java-1.8.0-openjdk-devel-1:1.8.0.362.b08-1.el7_9.x86_64.rpm
java-1.8.0-openjdk-headless-1:1.8.0.362.b08-1.el7_9.x86_64.rpm
sudo-1.8.23-10.el7_9.3.x86_64.rpm

Security vulnerabilities resolved in SM 8.1 Security Service Pack #29

Fix id	Updated Package	RHSA Number	Common Vulnerability and	RHSA Severity	ASA Number	ASA Overall

			Exposure (CVE) ID			Severity
ASM-90413	sudo	RHSA-2023:0291	CVE-2023-22809	Important	None	None
ASM-90412	java-1.8.0-openjdk-devel java-1.8.0-openjdk-headless	RHSA-2023:0203	CVE-2023-21830 CVE-2023-21843	Moderate	ASA-2023-015	Medium

SM 8.1 Security Service Pack #28 includes the following rpm updates:

grub2-1:2.02-0.87.el7_9.11.x86_64.rpm	grub2-tools-1:2.02-0.87.el7_9.11.x86_64.rpm
grub2-common-1:2.02-0.87.el7_9.11.noarch.rpm	grub2-tools-extra-1:2.02-0.87.el7_9.11.x86_64.rpm
grub2-pc-1:2.02-0.87.el7_9.11.x86_64.rpm	grub2-tools-minimal-1:2.02-0.87.el7_9.11.x86_64.rpm
grub2-pc-modules-1:2.02-0.87.el7_9.11.noarch.rpm	krb5-libs-1.15.1-55.el7_9.x86_64.rpm

Security vulnerabilities resolved in SM 8.1 Security Service Pack #28

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-90240	grub2 grub2-common grub2-pc grub2-pc-modules grub2-tools grub2-tools-extra grub2-tools-minimal	RHSA-2022:8900	CVE-2022-28733	Important	ASA-2022-162	High
ASM-90152	krb5-libs	RHSA-2022:8640	CVE-2022-42898	Important	ASA-2022-161	Medium

SM 8.1 Security Service Pack #27 includes the following rpm updates:

java-1.8.0-openjdk-devel-1:1.8.0.352.b08-2.el7_9.x86_64.rpm	kernel-tools-libs-3.10.0-1160.80.1.el7.x86_64.rpm
java-1.8.0-openjdk-headless-1:1.8.0.352.b08-2.el7_9.x86_64.rpm	kpartx-0.4.9-136.el7_9.x86_64.rpm
kernel-3.10.0-1160.80.1.el7.x86_64.rpm	perf-3.10.0-1160.80.1.el7.x86_64.rpm
kernel-tools-3.10.0-1160.80.1.el7.x86_64.rpm	python-perf-3.10.0-1160.80.1.el7.x86_64.rpm

Security vulnerabilities resolved in SM 8.1 Security Service Pack #27

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-90111	kernel kernel-tools kernel-tools-libs perf python-perf	RHSA-2022:7337	CVE-2022-2588 CVE-2022-23816 CVE-2022-23825 CVE-2022-26373 CVE-2022-29900 CVE-2022-29901	Important	ASA-2022-152	High
ASM-90110	kpartx	RHSA-2022:7186	CVE-2022-41974	Important	None	None
ASM-89956	java-1.8.0-openjdk-devel java-1.8.0-openjdk-headless	RHSA-2022:7002	CVE-2022-21619 CVE-2022-21624	Moderate	ASA-2022-127	Medium

			CVE-2022-21626 CVE-2022-21628			

SM 8.1 Security Service Pack #26 includes the following rpm updates:

bind-32:9.11.4-26.P2.el7_9.10.x86_64.rpm	bind-license-32:9.11.4-26.P2.el7_9.10.noarch.rpm
bind-libs-32:9.11.4-26.P2.el7_9.10.x86_64.rpm	bind-utils-32:9.11.4-26.P2.el7_9.10.x86_64.rpm
bind-libs-lite-32:9.11.4-26.P2.el7_9.10.x86_64.rpm	expat-2.1.0-15.el7_9.x86_64.rpm

Security vulnerabilities resolved in SM 8.1 Security Service Pack #26

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-89928	expat	RHSA-2022:6834	CVE-2022-40674	Important	ASA-2022-125	Critical
ASM-89889	Bind bind-libs bind-libs-lite bind-license bind-utils	RHSA-2022:6765	CVE-2022-38177 CVE-2022-38178	Important	ASA-2022-124	High

SM 8.1 Security Service Pack #25 includes the following rpm updates:

open-vm-tools-11.0.5-3.el7_9.4.x86_64.rpm	systemd-libs-219-78.el7_9.7.x86_64.rpm
systemd-219-78.el7_9.7.x86_64.rpm	systemd-sysv-219-78.el7_9.7.x86_64.rpm

Security vulnerabilities resolved in SM 8.1 Security Service Pack #25

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-89823	open-vm-tools	RHSA-2022:6381	CVE-2022-31676	Important	ASA-2022-119	High
ASM-89738	systemd systemd-libs systemd-sys	RHSA-2022:6160	CVE-2022-2526	Important	ASA-2022-115	High

SM 8.1 Security Service Pack #24 includes the following rpm updates:

java-1.8.0-openjdk-devel-1:1.8.0.342.b07-1.el7_9.x86_64.rpm	kernel-tools-libs-3.10.0-1160.76.1.el7.x86_64.rpm
java-1.8.0-openjdk-headless-1:1.8.0.342.b07-1.el7_9.x86_64.rpm	perf-3.10.0-1160.76.1.el7.x86_64.rpm
kernel-3.10.0-1160.76.1.el7.x86_64.rpm	python-perf-3.10.0-1160.76.1.el7.x86_64.rpm
kernel-tools-3.10.0-1160.76.1.el7.x86_64.rpm	

Security vulnerabilities resolved in SM 8.1 Security Service Pack #24

Fix id	Updated Package	RHSA Number	Common Vulnerability and	RHSA Severity	ASA Number	ASA Overall

			Exposure (CVE) ID			Severity
ASM-89646	kernel kernel-tools kernel-tools-libs perf python-perf	RHSA-2022:5937	CVE-2022-21123 CVE-2022-21125 CVE-2022-21166	Moderate	ASA-2022-113	Medium
ASM-89571	java-1.8.0-openjdk-devel java-1.8.0-openjdk-headless	RHSA-2022:5698	CVE-2022-21540 CVE-2022-21541 CVE-2022-34169	Important	ASA-2022-106	High

SM 8.1 Security Service Pack #23 includes the following rpm updates:

kernel-3.10.0-1160.71.1.el7.x86_64.rpm	postgresql-libs-9.2.24-8.el7_9.x86_64.rpm
kernel-tools-3.10.0-1160.71.1.el7.x86_64.rpm	python-2.7.5-92.el7_9.x86_64.rpm
kernel-tools-libs-3.10.0-1160.71.1.el7.x86_64.rpm	python-libs-2.7.5-92.el7_9.x86_64.rpm
perf-3.10.0-1160.71.1.el7.x86_64.rpm	python-perf-3.10.0-1160.71.1.el7.x86_64.rpm

Security vulnerabilities resolved in SM 8.1 Security Service Pack #23

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-89482	python python-libs	RHSA-2022:5235	CVE-2020-26116 CVE-2020-26137 CVE-2021-3177	Moderate	None	None
ASM-89368	kernel kernel-tools kernel-tools-libs perf python-perf	RHSA-2022:5232	CVE-2022-1729 CVE-2022-1966	Important	ASA-2022-097	High
ASM-89483	postgresql-libs	RHSA-2022:5162	CVE-2022-1552	Important	None	None

SM 8.1 Security Service Pack #22 includes the following rpm updates:

kernel-3.10.0-1160.66.1.el7.x86_64.rpm	rsyslog-8.24.0-57.el7_9.3.x86_64.rpm
kernel-tools-3.10.0-1160.66.1.el7.x86_64.rpm	rsyslog-gnutls-8.24.0-57.el7_9.3.x86_64.rpm
kernel-tools-libs-3.10.0-1160.66.1.el7.x86_64.rpm	xz-5.2.2-2.el7_9.x86_64.rpm
perf-3.10.0-1160.66.1.el7.x86_64.rpm	xz-libs-5.2.2-2.el7_9.x86_64.rpm
python-perf-3.10.0-1160.66.1.el7.x86_64.rpm	

Security vulnerabilities resolved in SM 8.1 Security Service Pack #22

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-89285	xz xz-libs	RHSA-2022:5052	CVE-2022-1271	Important	ASA-2022-081	High
ASM-89178	rsyslog rsyslog-gnutls	RHSA-2022:4803	CVE-2022-24903	Important	ASA-2022-076	High
ASM-89286	kernel kernel-tools kernel-tools-libs perf python-perf	RHSA-2022:4642	CVE-2022-0492	Important	ASA-2022-087	High

SM 8.1 Security Service Pack #21 includes the following rpm updates:

gzip-1.5-11.el7_9.x86_64.rpm
java-1.8.0-openjdk-devel-1:1.8.0.332.b09-1.el7_9.x86_64.rpm
java-1.8.0-openjdk-headless-1:1.8.0.332.b09-1.el7_9.x86_64.rpm
zlib-1.2.7-20.el7_9.x86_64.rpm

Security vulnerabilities resolved in SM 8.1 Security Service Pack #21

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-89043	zlib	RHSA-2022:2213	CVE-2018-25032	Important	ASA-2022-064	High
ASM-89057	gzip	RHSA-2022:2191	CVE-2022-1271	Important	None	Important
ASM-88835	java-1.8.0-openjdk-devel java-1.8.0-openjdk-headless	RHSA-2022:1487	CVE-2022-21426 CVE-2022-21434 CVE-2022-21443 CVE-2022-21476 CVE-2022-21496	Important	ASA-2022-039	High

SM 8.1 Security Service Pack #20 includes the following rpm updates:

expat-2.1.0-14.el7_9.x86_64.rpm	openssl-1:1.0.2k-25.el7_9.x86_64.rpm
kernel-3.10.0-1160.62.1.el7.x86_64.rpm	openssl-libs-1:1.0.2k-25.el7_9.x86_64.rpm
kernel-tools-3.10.0-1160.62.1.el7.x86_64.rpm	perf-3.10.0-1160.62.1.el7.x86_64.rpm
kernel-tools-libs-3.10.0-1160.62.1.el7.x86_64.rpm	python-perf-3.10.0-1160.62.1.el7.x86_64.rpm

Security vulnerabilities resolved in SM 8.1 Security Service Pack #20

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-88636	kernel kernel-tools kernel-tools-libs perf python-perf	RHSA-2022:1198	CVE-2021-4028 CVE-2021-4083	Important	ASA-2022-037	High
ASM-88797	expat	RHSA-2022:1069	CVE-2021-45960 CVE-2021-46143 CVE-2022-22822 CVE-2022-22823 CVE-2022-22824 CVE-2022-22825 CVE-2022-22826 CVE-2022-22827 CVE-2022-23852 CVE-2022-25235 CVE-2022-25236 CVE-2022-25315	Important	ASA-2022-067	Critical
ASM-88796	openssl openssl-libs	RHSA-2022:1066	CVE-2022-0778	Important	NA	NA

SM 8.1 Security Service Pack #19 includes the following rpm updates:

cyrus-sasl-lib-2.1.26-24.el7_9.x86_64.rpm

Security vulnerabilities resolved in SM 8.1 Security Service Pack #19

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-88276	cyrus-sasl-lib	RHSA-2022:0666	CVE-2022-24407	Important	ASA-2022-027	Critical

SM 8.1 Security Service Pack #18 includes the following rpm updates:

aide-0.15.1-13.el7_9.1.x86_64.rpm	kernel-tools-libs-3.10.0-1160.59.1.el7.x86_64.rpm
java-1.8.0-openjdk-devel-1:1.8.0.322.b06-1.el7_9.x86_64.rpm	openldap-2.4.44-25.el7_9.x86_64.rpm

java-1.8.0-openjdk-headless-1:1.8.0.322.b06-1.el7_9.x86_64.rpm	perf-3.10.0-1160.59.1.el7.x86_64.rpm
kernel-3.10.0-1160.59.1.el7.x86_64.rpm	polkit-0.112-26.el7_9.1.x86_64.rpm
kernel-tools-3.10.0-1160.59.1.el7.x86_64.rpm	python-perf-3.10.0-1160.59.1.el7.x86_64.rpm

Security vulnerabilities resolved in SM 8.1 Security Service Pack #18

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-88254	openldap	RHSA-2022:0621	CVE-2020-25709 CVE-2020-25710	Moderate	ASA-2022-025	Low
ASM-88255	kernel kernel-tools kernel-tools-libs perf python-perf	RHSA-2022:0620	CVE-2020-0465 CVE-2020-0466 CVE-2021-0920 CVE-2021-3564 CVE-2021-3573 CVE-2021-3752 CVE-2021-4155 CVE-2022-0330 CVE-2022-22942	Important	ASA-2022-026	High
ASM-88218	aide	RHSA-2022:0473	CVE-2021-45417	Important	NA	NA
ASM-88074	java-1.8.0-openjdk-devel java-1.8.0-openjdk-headless	RHSA-2022:0306	CVE-2022-21248 CVE-2022-21282 CVE-2022-21283 CVE-2022-21293 CVE-2022-21294 CVE-2022-21296 CVE-2022-21299 CVE-2022-21305 CVE-2022-21340 CVE-2022-21341 CVE-2022-21360 CVE-2022-21365	Moderate	ASA-2022-018	Low
ASM-88064	polkit	RHSA-2022:0274	CVE-2021-4034	Important	ASA-2022-010	High

SM 8.1 Security Service Pack #17 includes the following rpm updates:

kernel-3.10.0-1160.53.1.el7.x86_64.rpm	openssl-libs-1:1.0.2k-23.el7_9.x86_64.rpm
kernel-tools-3.10.0-1160.53.1.el7.x86_64.rpm	perf-3.10.0-1160.53.1.el7.x86_64.rpm
kernel-tools-libs-3.10.0-1160.53.1.el7.x86_64.rpm	python-perf-3.10.0-1160.53.1.el7.x86_64.rpm
openssl-1:1.0.2k-23.el7_9.x86_64.rpm	

Security vulnerabilities resolved in SM 8.1 Security Service Pack #17

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity

ASM-87891	openssl openssl-libs	RHSA-2022:0064	CVE-2021-3712	Moderate	ASA-2022-004	High
ASM-87892	kernel kernel-tools kernel-tools-libs perf python-perf	RHSA-2022:0063	CVE-2020-25704 CVE-2020-36322 CVE-2021-42739	Moderate	ASA-2022-011	Medium

SM 8.1 Security Service Pack #16 includes the following rpm updates:

kernel-3.10.0-1160.49.1.el7.x86_64.rpm	perf-3.10.0-1160.49.1.el7.x86_64.rpm
kernel-tools-3.10.0-1160.49.1.el7.x86_64.rpm	python-perf-3.10.0-1160.49.1.el7.x86_64.rpm
kernel-tools-libs-3.10.0-1160.49.1.el7.x86_64.rpm	rpm-4.11.3-48.el7_9.x86_64.rpm
krb5-libs-1.15.1-51.el7_9.x86_64.rpm	rpm-build-libs-4.11.3-48.el7_9.x86_64.rpm
nss-3.67.0-4.el7_9.x86_64.rpm	rpm-libs-4.11.3-48.el7_9.x86_64.rpm
nss-sysinit-3.67.0-4.el7_9.x86_64.rpm	rpm-python-4.11.3-48.el7_9.x86_64.rpm
nss-tools-3.67.0-4.el7_9.x86_64.rpm	
openssh-7.4p1-22.el7_9.x86_64.rpm	
openssh-clients-7.4p1-22.el7_9.x86_64.rpm	
openssh-server-7.4p1-22.el7_9.x86_64.rpm	

Security vulnerabilities resolved in SM 8.1 Security Service Pack #16

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-87641	nss nss-sysinit nss-tools	RHSA-2021:4904	CVE-2021-43527	Critical	ASA-2021-184	Critical
ASM-87623	krb5-libs	RHSA-2021:4788	CVE-2021-37750	Moderate	ASA-2021-179	Medium
ASM-87621	rpm rpm-build-libs rpm-libs rpm-python	RHSA-2021:4785	CVE-2021-20271	Moderate	ASA-2021-180	Medium
ASM-87631	openssh openssh-clients openssh-server	RHSA-2021:4782	CVE-2021-41617	Moderate	ASA-2021-183	High
ASM-87630	kernel kernel-tools kernel-tools-libs perf python-perf	RHSA-2021:4777	CVE-2020-36385	Important	ASA-2021-182	High

SM 8.1 Security Service Pack #15 includes the following rpm updates:

java-1.8.0-openjdk-headless-1:1.8.0.312.b07-1.el7_9.x86_64.rpm	binutils-2.27-44.base.el7_9.1.x86_64.rpm
java-1.8.0-openjdk-devel-1:1.8.0.312.b07-1.el7_9.x86_64.rpm	

Security vulnerabilities resolved in SM 8.1 Security Service Pack #15

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-87448	binutils	RHSA-2021:4033	CVE-2021-42574	Moderate	ASA-2021-128	High
ASM-87313	java-1.8.0-openjdk-devel java-1.8.0-openjdk-headless	RHSA-2021:3889	CVE-2021-35550 CVE-2021-35556 CVE-2021-35559 CVE-2021-35561 CVE-2021-35564 CVE-2021-35565 CVE-2021-35567 CVE-2021-35578 CVE-2021-35586 CVE-2021-35588 CVE-2021-35603	Important	ASA-2021-124	Low

SM 8.1 Security Service Pack #14 includes the following rpm updates:

kernel-3.10.0-1160.45.1.el7.x86_64.rpm	openssl-1:1.0.2k-22.el7_9.x86_64.rpm
kernel-tools-3.10.0-1160.45.1.el7.x86_64.rpm	openssl-libs-1:1.0.2k-22.el7_9.x86_64.rpm
kernel-tools-libs-3.10.0-1160.45.1.el7.x86_64.rpm	perf-3.10.0-1160.45.1.el7.x86_64.rpm
libxml2-2.9.1-6.el7_9.6.x86_64.rpm	python-perf-3.10.0-1160.45.1.el7.x86_64.rpm
libxml2-python-2.9.1-6.el7_9.6.x86_64.rpm	

Security vulnerabilities resolved in SM 8.1 Security Service Pack #14

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-87225	libxml2 libxml2-python	RHSA-2021:3810	CVE-2016-4658	Moderate	ASA-2021-129	Medium
ASM-87224	kernel kernel-tools kernel-tools-libs perf python-perf	RHSA-2021:3801	CVE-2021-3653 CVE-2021-3656 CVE-2021-22543 CVE-2021-37576	Important	ASA-2021-118	High
ASM-87226	openssl openssl-libs	RHSA-2021:3798	CVE-2021-23840 CVE-2021-23841	Moderate	ASA-2021-120	High

SM 8.1 Security Service Pack #13 includes the following rpm updates:

bind-32:9.11.4-26.P2.el7_9.7.x86_64.rpm	kernel-3.10.0-1160.42.2.el7.x86_64.rpm
bind-libs-32:9.11.4-26.P2.el7_9.7.x86_64.rpm	kernel-tools-3.10.0-1160.42.2.el7.x86_64.rpm
bind-libs-lite-32:9.11.4-26.P2.el7_9.7.x86_64.rpm	kernel-tools-libs-3.10.0-1160.42.2.el7.x86_64.rpm
bind-license-32:9.11.4-26.P2.el7_9.7.noarch.rpm	perf-3.10.0-1160.42.2.el7.x86_64.rpm

bind-utils-32:9.11.4-26.P2.el7_9.7.x86_64.rpm	python-perf-3.10.0-1160.42.2.el7.x86_64.rpm

Security vulnerabilities resolved in SM 8.1 Security Service Pack #13

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-86769	kernel kernel-tools kernel-tools-libs perf python-perf	RHSA-2021:3438	CVE-2021-3715	Moderate	ASA-2021-113	High
ASM-86768	kernel kernel-tools kernel-tools-libs perf python-perf	RHSA-2021:3327	CVE-2020-27777 CVE-2021-22555 CVE-2021-29154 CVE-2021-29650 CVE-2021-32399	Important	ASA-2021-110	High
ASM-86789	bind bind-libs bind-libs-lite bind-license bind-utils	RHSA-2021:3325	CVE-2021-25214	Moderate	ASA-2021-122	Medium

SM 8.1 Security Service Pack #12 includes the following rpm updates:

java-1.8.0-openjdk-devel-1:1.8.0.302.b08-0.el7_9.x86_64.rpm java-1.8.0-openjdk-headless-1:1.8.0.302.b08-0.el7_9.x86_64.rpm kernel-3.10.0-1160.36.2.el7.x86_64.rpm kernel-tools-3.10.0-1160.36.2.el7.x86_64.rpm	kernel-tools-libs-3.10.0-1160.36.2.el7.x86_64.rpm microcode_ctl-2:2.1-73.11.el7_9.x86_64.rpm perf-3.10.0-1160.36.2.el7.x86_64.rpm python-perf-3.10.0-1160.36.2.el7.x86_64.rpm

Security vulnerabilities resolved in SM 8.1 Security Service Pack #12

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-86410	microcode_ctl	RHSA-2021:3028	CVE-2020-0543 CVE-2020-0548 CVE-2020-0549	Important	ASA-2021-105	Important

			CVE-2020-8695 CVE-2020-8696 CVE-2020-8698 CVE-2020-24489 CVE-2020-24511 CVE-2020-24512			
ASM-86091	java-1.8.0-openjdk-devel java-1.8.0-openjdk-headless	RHSA-2021:2845	CVE-2021-2341 CVE-2021-2369 CVE-2021-2388	Important	ASA-2021-095	High
ASM-86335	kernel kernel-tools kernel-tools-libs perf python-perf	RHSA-2021:2725	CVE-2019-20934 CVE-2020-11668 CVE-2021-33033 CVE-2021-33034 CVE-2021-33909	Important	ASA-2021-103	High

SM 8.1 Security Service Pack #11 includes the following rpm updates:

dhclient-12:4.2.5-83.el7_9.1.x86_64.rpm dhcp-common-12:4.2.5-83.el7_9.1.x86_64.rpm dhcp-libs-12:4.2.5-83.el7_9.1.x86_64.rpm	postgresql-libs-9.2.24-7.el7_9.x86_64.rpm

Security vulnerabilities resolved in SM 8.1 Security Service Pack #11

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-85952	postgresql-libs	RHSA-2021:2397	CVE-2021-32027	Important	ASA-2021-080	High
ASM-85711	dhclient dhcp-common dhcp-libs	RHSA-2021:2357	CVE-2021-25217	Important	ASA-2021-085	High

SM 8.1 Security Service Pack #10 includes the following rpm updates:

glib2-2.56.1-9.el7_9.x86_64.rpm kernel-3.10.0-1160.31.1.el7.x86_64.rpm kernel-tools-3.10.0-1160.31.1.el7.x86_64.rpm kernel-tools-libs-3.10.0-1160.31.1.el7.x86_64.rpm	microcode_ctl-2:2.1-73.9.el7_9.x86_64.rpm perf-3.10.0-1160.31.1.el7.x86_64.rpm python-perf-3.10.0-1160.31.1.el7.x86_64.rpm

Security vulnerabilities resolved in SM 8.1 Security Service Pack #10

Fix id	Updated Package	RHSA	Common Vulnerability and	RHSA	ASA Number	ASA Overall

		Number	Exposure (CVE) ID	Severity		Severity
ASM-85692	kernel kernel-tools kernel-tools-libs perf python-perf	RHSA-2021:2314	CVE-2020-8648 CVE-2020-12362 CVE-2020-12363 CVE-2020-12364 CVE-2020-27170 CVE-2021-3347	Important	ASA-2021-083	High
ASM-85691	microcode_ctl	RHSA-2021:2305	CVE-2020-24489 CVE-2020-24511 CVE-2020-24512 CVE-2020-24513	Important	ASA-2021-079	High
ASM-85624	glib2	RHSA-2021:2147	CVE-2021-27219	Important	ASA-2021-072	Critical

SM 8.1 Security Service Pack #9 includes the following rpm updates:

bind-32:9.11.4-26.P2.el7_9.5.x86_64.rpm bind-libs-32:9.11.4-26.P2.el7_9.5.x86_64.rpm bind-libs-lite-32:9.11.4-26.P2.el7_9.5.x86_64.rpm bind-license-32:9.11.4-26.P2.el7_9.5.noarch.rpm bind-utils-32:9.11.4-26.P2.el7_9.5.x86_64.rpm java-1.8.0-openjdk-devel-1:1.8.0.292.b10-1.el7_9.x86_64.rpm	java-1.8.0-openjdk-headless-1:1.8.0.292.b10-1.el7_9.x86_64.rpm nss-3.53.1-7.el7_9.x86_64.rpm nss-sysinit-3.53.1-7.el7_9.x86_64.rpm nss-tools-3.53.1-7.el7_9.x86_64.rpm openldap-2.4.44-23.el7_9.x86_64.rpm postgresql-libs-9.2.24-6.el7_9.x86_64.rpm

Security vulnerabilities resolved in SM 8.1 Security Service Pack #9

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-85312	postgresql-libs	RHSA-2021:1512	CVE-2019-10208 CVE-2020-25694 CVE-2020-25695	Important	ASA-2021-043	High
ASM-85210	bind bind-libs bind-libs-lite bind-license bind-utils	RHSA-2021:1469	CVE-2021-25215	Important	ASA-2021-037	High
ASM-85283	openldap	RHSA-2021:1389	CVE-2020-25692	Moderate	ASA-2021-042	High
ASM-85159	nss nss-sysinit nss-tools	RHSA-2021:1384	CVE-2020-25648	Moderate	ASA-2021-035	High

ASM-85142	java-1.8.0-openjdk-devel java-1.8.0-openjdk-headless	RHSA-2021:1298	CVE-2021-2163	Moderate	ASA-2021-034	Medium

SM 8.1 Security Service Pack #8 includes the following rpm updates:

kernel-3.10.0-1160.24.1.el7.x86_64.rpm kernel-tools-3.10.0-1160.24.1.el7.x86_64.rpm kernel-tools-libs-3.10.0-1160.24.1.el7.x86_64.rpm nettle-2.7.1-9.el7_9.x86_64.rpm	perf-3.10.0-1160.24.1.el7.x86_64.rpm python-perf-3.10.0-1160.24.1.el7.x86_64.rpm screen-4.1.0-0.27.20120314git3c2946.el7_9.x86_64.rpm

Security vulnerabilities resolved in SM 8.1 Security Service Pack #8

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-85014	nettle	RHSA-2021:1145	CVE-2021-20305	Important	ASA-2021-028	High
ASM-85013	Kernel kernel-tools kernel-tools-libs perf python-perf	RHSA-2021:1071	CVE-2021-27363 CVE-2021-27364 CVE-2021-27365	Important	ASA-2021-027	High
ASM-84848	kernel kernel-tools kernel-tools-libs perf python-perf	RHSA-2021:0856	CVE-2019-19532 CVE-2020-0427 CVE-2020-7053 CVE-2020-14351 CVE-2020-25211 CVE-2020-25645 CVE-2020-25656 CVE-2020-25705 CVE-2020-28374 CVE-2020-29661 CVE-2021-20265	Important	ASA-2021-021	High
ASM-84871	screen	RHSA-2021:0742	CVE-2021-26937	Important	ASA-2021-024	Critical

Security vulnerabilities resolved in SM 8.1 Security Service Pack #7

Fix id	RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity

ASM-84655	RHSA-2021:0699	Moderate	ASA-2021-019	Low
ASM-84631	RHSA-2021:0671	Important	ASA-2021-018	High
ASM-84332	RHSA-2021:0348	Moderate	ASA-2021-014	High
ASM-84331	RHSA-2021:0343	Moderate	ASA-2021-013	High
ASM-84311	RHSA-2021:0339	Important	ASA-2021-011	High
ASM-84246	RHSA-2021:0336	Moderate	ASA-2021-010	Medium
ASM-84073	RHSA-2021:0221	Important	ASA-2021-009	High

Security vulnerabilities resolved in SM 8.1 Security Service Pack #6

Fix id	RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
ASM-83655	RHSA-2020:5566	Important	ASA-2021-001	Important
ASM-83652	RHSA-2020:5437	Important	ASA-2020-208	High

Security vulnerabilities resolved in SM 8.1 Security Service Pack #5

Fix id	RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
ASM-83196	RHSA-2020:5083	Moderate	ASA-2020-193	Medium
ASM-83189	RHSA-2020:5023	Moderate	ASA-2020-186	Medium
ASM-83195	RHSA-2020:5011	Moderate	ASA-2020-203	High
ASM-83194	RHSA-2020:5009	Moderate	ASA-2020-201	High
ASM-83193	RHSA-2020:5002	Moderate	ASA-2020-192	Medium
ASM-83190	RHSA-2020:4907	Important	ASA-2020-187	High
ASM-82951	RHSA-2020:4350	Moderate	ASA-2020-148	Medium
ASM-82919	RHSA-2020:4276	Important	ASA-2020-146	High
ASM-82600	RHSA-2020:4076	Moderate	ASA-2020-119	High
ASM-82604	RHSA-2020:4072	Moderate	ASA-2020-131	High
ASM-82615	RHSA-2020:4060	Important	ASA-2020-140	High
ASM-82598	RHSA-2020:4041	Moderate	ASA-2020-121	High
ASM-82612	RHSA-2020:4032	Moderate	ASA-2020-136	High
ASM-82585	RHSA-2020:4026	Moderate	ASA-2020-112	Medium
ASM-82603	RHSA-2020:4011	Moderate	ASA-2020-133	Low
ASM-82607	RHSA-2020:4007	Low	ASA-2020-128	Low
ASM-82614	RHSA-2020:4005	Moderate	ASA-2020-138	High
ASM-82597	RHSA-2020:3996	Moderate	ASA-2020-122	High
ASM-82606	RHSA-2020:3978	Moderate	ASA-2020-125	Medium
ASM-82584	RHSA-2020:3952	Moderate	ASA-2020-116	Medium
ASM-82602	RHSA-2020:3916	Moderate	ASA-2020-132	Medium
ASM-82611	RHSA-2020:3915	Moderate	ASA-2020-135	Medium
ASM-82610	RHSA-2020:3911	Moderate	ASA-2020-134	Medium
ASM-82599	RHSA-2020:3908	Moderate	ASA-2020-120	Medium
ASM-82609	RHSA-2020:3901	Low	ASA-2020-130	Low
ASM-82608	RHSA-2020:3864	Moderate	ASA-2020-129	Medium
ASM-82605	RHSA-2020:3861	Low	ASA-2020-124	Low
ASM-82613	RHSA-2020:3848	Low	ASA-2020-137	Low

Security vulnerabilities resolved in SM 8.1 Security Service Pack #4

Fix id	RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
ASM-81868	RHSA-2020:3220	Important	ASA-2020-103	High

ASM-81862	RHSA-2020:3217	Moderate	ASA-2020-102	High
ASM-81557	RHSA-2020:2968	Important	ASA-2020-098	High
ASM-81503	RHSA-2020:2894	Important	ASA-2020-092	Medium
ASM-81318	RHSA-2020:2664	Important	ASA-2020-089	Medium
ASM-81317	RHSA-2020:2663	Moderate	ASA-2020-090	High
ASM-81087	RHSA-2020:2432	Moderate	ASA-2020-083	Medium
ASM-80975	RHSA-2020:2344	Important	ASA-2020-079	High
ASM-80641	RHSA-2020:2082	Important	ASA-2020-075	High

Security vulnerabilities resolved in SM 8.1 Security Service Pack #3

Fix id	RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
ASM-80500	RHSA-2020:1512	Important	ASA-2020-071	High
ASM-80100	RHSA-2020:1190	Moderate	ASA-2020-050	Low
ASM-80098	RHSA-2020:1181	Low	ASA-2020-055	Low
ASM-80107	RHSA-2020:1176	Low	ASA-2020-049	Medium
ASM-80101	RHSA-2020:1138	Low	ASA-2020-057	Critical
ASM-80099	RHSA-2020:1135	Low	ASA-2020-051	Low
ASM-80088	RHSA-2020:1131	Moderate	ASA-2020-038	High
ASM-80106	RHSA-2020:1113	Moderate	ASA-2020-061	Medium
ASM-80085	RHSA-2020:1100	Moderate	ASA-2020-032	Medium
ASM-80105	RHSA-2020:1061	Moderate	ASA-2020-059	Medium
ASM-80097	RHSA-2020:1047	Moderate	ASA-2020-044	Medium
ASM-80102	RHSA-2020:1022	Low	ASA-2020-043	Medium
ASM-80084	RHSA-2020:1021	Moderate	ASA-2020-033	Medium
ASM-80087	RHSA-2020:1020	Low	ASA-2020-040	Medium
ASM-80090	RHSA-2020:1016	Moderate	ASA-2020-036	High
ASM-80089	RHSA-2020:1011	Moderate	ASA-2020-037	Medium
ASM-80096	RHSA-2020:1000	Moderate	ASA-2020-041	High
ASM-80051	RHSA-2020:0897	Important	ASA-2020-031	High
ASM-80056	RHSA-2020:0834	Important	ASA-2020-026	Important
ASM-79605	RHSA-2020:0540	Important	ASA-2020-006	High

Security vulnerabilities resolved in SM 8.1 Security Service Pack #2

Fix id	RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
ASM-79376	RHSA-2020:0374	Important	ASA-2020-010	Critical
ASM-79379	RHSA-2020:0227	Important	ASA-2020-008	High
ASM-79378	RHSA-2020:0196	Important	ASA-2020-014	High
ASM-78322	RHSA-2019:4190	Important	ASA-2019-247	High
ASM-78323	RHSA-2019:3979	Important	ASA-2019-245	High
ASM-77872	RHSA-2019:3872	Important	ASA-2019-241	High
ASM-77861	RHSA-2019:3834	Important	ASA-2019-237	Medium
ASM-77688	RHSA-2019:3197	Important	ASA-2019-233	High
ASM-77693	RHSA-2019:3128	Important	ASA-2019-230	Medium
ASM-77593	RHSA-2019:3055	Important	ASA-2019-228	High
ASM-77396	RHSA-2019:2964	Important	ASA-2019-227	High

Security vulnerabilities resolved in SM 8.1 Security Service Pack #1

Fix id	RHSA Number	RHSA Severity	ASA Number	ASA Overall

				Severity
ASM-77352	RHSA-2019:2829	Important	ASA-2019-226	High
ASM-77124	RHSA-2019:2600	Important	ASA-2019-220	Medium
ASM-76738	RHSA-2019:2327	Moderate	ASA-2019-155	Medium
ASM-76933	RHSA-2019:2304	Moderate	ASA-2019-193	Medium
ASM-76932	RHSA-2019:2237	Moderate	ASA-2019-205	Medium
ASM-76739	RHSA-2019:2197	Low	ASA-2019-154	Medium
ASM-76737	RHSA-2019:2189	Moderate	ASA-2019-158	Medium
ASM-76741	RHSA-2019:2169	Important	ASA-2019-144	High
ASM-76931	RHSA-2019:2159	Low	ASA-2019-198	Low
ASM-76930	RHSA-2019:2143	Low	ASA-2019-204	Medium
ASM-76929	RHSA-2019:2118	Moderate	ASA-2019-192	Medium
ASM-76928	RHSA-2019:2110	Moderate	ASA-2019-211	Medium
ASM-76927	RHSA-2019:2091	Moderate	ASA-2019-203	Medium
ASM-76926	RHSA-2019:2060	Moderate	ASA-2019-194	Medium
ASM-76925	RHSA-2019:2057	Moderate	ASA-2019-202	Medium
ASM-76924	RHSA-2019:2052	Moderate	ASA-2019-216	Medium
ASM-76735	RHSA-2019:2049	Moderate	ASA-2019-169	Medium
ASM-76923	RHSA-2019:2047	Moderate	ASA-2019-147	Medium
ASM-76740	RHSA-2019:2046	Moderate	ASA-2019-152	High
ASM-76922	RHSA-2019:2033	Low	ASA-2019-196	Low
ASM-76934	RHSA-2019:2030	Moderate	ASA-2019-191	High
ASM-76921	RHSA-2019:2029	Important	ASA-2019-208	High
ASM-76795	RHSA-2019:1880	Low	ASA-2019-178	High
ASM-76920	RHSA-2019:1873	Important	ASA-2019-207	High
ASM-76581	RHSA-2019:1815	Moderate	ASA-2019-130	Medium
ASM-76337	RHSA-2019:1619	Important	ASA-2019-121	Medium
ASM-76225	RHSA-2019:1587	Important	ASA-2019-120	Critical
ASM-76150	RHSA-2019:1481	Important	ASA-2019-109	High
ASM-76126	RHSA-2019:1294	Important	ASA-2019-100	High
ASM-75817	RHSA-2019:1228	Important	ASA-2019-106	High
ASM-75818	RHSA-2019:1168	Important	ASA-2019-095	Medium
ASM-76886	RHSA-2019-2181	Low	ASA-2019-183	Low
ASM-76885	RHSA-2019-2136	Moderate	ASA-2019-185	Medium
ASM-76598	RHSA-2019-1884	Moderate	ASA-2019-136	High

Mitigation: Not Applicable

SECTION 1C – ENTITLEMENTS AND CONTACTS

Material Coverage Entitlements: There is no charge for material related to this PCN.

PLDS can be reached by performing the following steps from a browser:
1. Go to http://support.avaya.com
2. Click on **Downloads** in the top menu bar
3. In the Enter Your Product Here box, enter "**Session Manager**", select release "**8.1.x"** in the pull-down list.
4. Select the Session Manager **8.1** Virtual Appliance OVA file (**SM-8.1.0.0.810007-e70-2E.ova**).

For BSM (**BSM-8.1.0.0.810007-e70-2E.ova)**

The **Upgrading Avaya Aura® Session Manager** document and **Upgrading and Migrating Avaya Aura® Applications to 8.1** contains instructions on how to upgrade Session Manager release to 8.1.3.4 and can be obtained by performing the following steps from a browser:
1. Go to http://support.avaya.com
2. Click on **Documents** in the top menu bar
3. In the Enter Your Product Here box, enter "**Session Manager**", select release "**8.1.x"** in the pull-down list, and select the **"Installation, Upgrades & Config"** checkbox in the Content Type box on the left. Then click the "**ENTER**" button to display a list of documents.
4. Search for the document titled "**Upgrading Avaya Aura® Session Manager"** & **"Upgrading and Migrating Avaya Aura® Applications to 8.1"**

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.