

Product Correction Notice (PCN)

Issue Date: July 15, 2019
 Supplement Date: May 8, 2023
 Expiration Date: NA
 PCN Number: 2105S

SECTION 1 - CUSTOMER NOTICE


Products affected by this PCN: Avaya Aura® System Manager, Release 8.1.x (All offer types). This is applicable for all System Manager Services offer types: Kernel-based Virtual Machine (KVM), Amazon Web Service (AWS), Avaya Aura® Appliance Virtualization Platform (AVP) and Virtualized Environment.

Description: **Beginning December 2020, 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.**

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.

8-May-2023 – Supplement 29 – Supplement 29 of this PCN introduces **Avaya Aura System Manager 8.1 Security Service Pack SSP #30** (System_Manager_SSP_R8.1.0.0_Patch30_810015698.bin; PLDS ID SMGR81SSP30)

To determine that System Manager software that is being run on your server you can:

- Log on to the System Manager Web Interface.
- On the top-right corner click on the  icon and then select the “About” link. Verify version details present on About page.


IMPORTANT NOTE:

- System Manager 8.1 SSP #30 is applicable to System Manager 8.1.0 through 8.1.3.7.
Note - No need to install Security Service Pack(SSP) #30 on the 8.1.3.8 Service Pack as 8.1.3.8 already contains all security updates included in SSP #30.
 This patch is not applicable for System Manager 8.1.x Software Only deployments. This patch should **NOT** be installed on System Manager 8.1.x Software Only deployments.

21-February-2023 – Supplement 28 – Supplement 28 of this PCN introduces **Avaya Aura System Manager 8.1 Security Service Pack SSP #29** (System_Manager_SSP_R8.1.0.0_Patch29_810015565.bin; PLDS ID SMGR81SSP29)

To determine that System Manager software that is being run on your server you can:

- Log on to the System Manager Web Interface.


- On the top-right corner click on the  icon and then select the “About” link. Verify version details present on About page.

IMPORTANT NOTE:

- System Manager 8.1 SSP #29 is applicable to System Manager 8.1.0 through 8.1.3.6.
Note - No need to install Security Service Pack(SSP) #29 on the 8.1.3.7 Service Pack as 8.1.3.7 already contains all security updates included in SSP #29.
- This patch is not applicable for System Manager 8.1.x Software Only deployments. This patch should **NOT** be installed on System Manager 8.1.x Software Only deployments.

**9-January-2023 – Supplement 27 – Supplement 27 of this PCN introduces Avaya Aura System Manager 8.1 Security Service Pack SSP #28
(System_Manager_SSP_R8.1.0.0_Patch28_810015486.bin; PLDS ID SMGR81SSP28)**

To determine that System Manager software that is being run on your server you can:


- Log on to the System Manager Web Interface.
- On the top-right corner click on the  icon and then select the “About” link. Verify version details present on About page.

IMPORTANT NOTE:

- System Manager 8.1 SSP #28 is applicable to System Manager 8.1.0 through 8.1.3.6.
- This patch is not applicable for System Manager 8.1.x Software Only deployments. This patch should **NOT** be installed on System Manager 8.1.x Software Only deployments.

**13-December-2022 – Supplement 26 – Supplement 26 of this PCN introduces Avaya Aura System Manager 8.1 Security Service Pack SSP #27
(System_Manager_SSP_R8.1.0.0_Patch27_810015404.bin; PLDS ID SMGR81SSP27)**

To determine that System Manager software that is being run on your server you can:


- Log on to the System Manager Web Interface.
- On the top-right corner click on the  icon and then select the “About” link. Verify version details present on About page.

IMPORTANT NOTE:

- System Manager 8.1 SSP #27 is applicable to System Manager 8.1.0 through 8.1.3.6.
- This patch is not applicable for System Manager 8.1.x Software Only deployments. This patch should **NOT** be installed on System Manager 8.1.x Software Only deployments.

**14-November-2022 – Supplement 25 – Supplement 25 of this PCN introduces Avaya Aura System Manager 8.1 Security Service Pack SSP #26
(System_Manager_SSP_R8.1.0.0_Patch26_810015327.bin; PLDS ID SMGR81SSP26)**

To determine that System Manager software that is being run on your server you can:


- Log on to the System Manager Web Interface.
- On the top-right corner click on the  icon and then select the “About” link. Verify version details present on About page.

IMPORTANT NOTE:

- System Manager 8.1 SSP #26 is applicable to System Manager 8.1.0 through 8.1.3.6.
- This patch is not applicable for System Manager 8.1.x Software Only deployments. This patch should **NOT** be installed on System Manager 8.1.x Software Only deployments.

24-October-2022 – Supplement 24 – Supplement 24 of this PCN introduces **Avaya Aura System Manager 8.1 Security Service Pack SSP #25**
(System_Manager_SSP_R8.1.0.0_Patch25_810015188.bin; PLDS ID SMGR81SSP25)

To determine that System Manager software that is being run on your server you can:


- Log on to the System Manager Web Interface.
- On the top-right corner click on the  icon and then select the “About” link. Verify version details present on About page.

IMPORTANT NOTE:

- System Manager 8.1 SSP #25 is applicable to System Manager 8.1.0 through 8.1.3.5.
Note - No need to install Security Service Pack(SSP) #25 on the 8.1.3.6 Service Pack (tentative GA date is October 24, 2022) as 8.1.3.6 already contains all security updates included in SSP #25.
- This patch is not applicable for System Manager 8.1.x Software Only deployments. This patch should **NOT** be installed on System Manager 8.1.x Software Only deployments.

12-September-2022 – Supplement 23 – Supplement 23 of this PCN introduces **Avaya Aura System Manager 8.1 Security Service Pack SSP #24**
(System_Manager_SSP_R8.1.0.0_Patch24_810015019.bin; PLDS ID SMGR81SSP24)

To determine that System Manager software that is being run on your server you can:


- Log on to the System Manager Web Interface.
- On the top-right corner click on the  icon and then select the “About” link. Verify version details present on About page.

IMPORTANT NOTE:

- System Manager 8.1 SSP #24 is applicable to System Manager 8.1.0 through 8.1.3.5.
- This patch is not applicable for System Manager 8.1.x Software Only deployments. This patch should **NOT** be installed on System Manager 8.1.x Software Only deployments.

8-August-2022 – Supplement 22 – Supplement 22 of this PCN introduces **Avaya Aura System Manager 8.1 Security Service Pack SSP #23**
(System_Manager_SSP_R8.1.0.0_Patch23_810014926.bin; PLDS ID SMGR81SSP23)

To determine that System Manager software that is being run on your server you can:

- Log on to the System Manager Web Interface.
- On the top-right corner click on the  icon and then select the “About” link. Verify version details present on About page.


IMPORTANT NOTE:

- System Manager 8.1 SSP #23 is applicable to System Manager 8.1.0 through 8.1.3.5.
- This patch is not applicable for System Manager 8.1.x Software Only deployments. This patch

should **NOT** be installed on System Manager 8.1.x Software Only deployments.

18-July-2022 – Supplement 21 – Supplement 21 of this PCN introduces **Avaya Aura System Manager 8.1 Security Service Pack SSP #22 (System_Manager_SSP_R8.1.0.0_Patch22_810014775.bin; PLDS ID SMGR81SSP22)**

To determine that System Manager software that is being run on your server you can:


- Log on to the System Manager Web Interface.
- On the top-right corner click on the  icon and then select the “About” link. Verify version details present on About page.

IMPORTANT NOTE:

- System Manager 8.1 SSP #22 is applicable to System Manager 8.1.0 through 8.1.3.5.
- This patch is not applicable for System Manager 8.1.x Software Only deployments. This patch should **NOT** be installed on System Manager 8.1.x Software Only deployments.

13-June-2022 – Supplement 20 – Supplement 20 of this PCN introduces **Avaya Aura System Manager 8.1 Security Service Pack SSP #21 (System_Manager_SSP_R8.1.0.0_Patch21_810014593.bin; PLDS ID SMGR81SSP21)**

To determine that System Manager software that is being run on your server you can:


- Log on to the System Manager Web Interface.
- On the top-right corner click on the  icon and then select the “About” link. Verify version details present on About page.

IMPORTANT NOTE:

- System Manager 8.1 SSP #21 is applicable to System Manager 8.1.0 through 8.1.3.4.
Note - No need to install Security Service Pack(SSP) #21 on the 8.1.3.5 Service Pack as 8.1.3.5 already contains all security updates included in SSP #21.
- This patch is not applicable for System Manager 8.1.x Software Only deployments. This patch should **NOT** be installed on System Manager 8.1.x Software Only deployments.

9-May-2022 – Supplement 19 – Supplement 19 of this PCN introduces **Avaya Aura System Manager 8.1 Security Service Pack SSP #20(System_Manager_SSP_R8.1.0.0_Patch20_810014469.bin; PLDS ID SMGR81SSP20)**

To determine that System Manager software that is being run on your server you can:

- Log on to the System Manager Web Interface.
- On the top-right corner click on the  icon and then select the “About” link. Verify version details present on About page.


IMPORTANT NOTE:

- System Manager 8.1 SSP #20 is applicable to System Manager 8.1.0 through 8.1.3.4.
- This patch is not applicable for System Manager 8.1.x Software Only deployments. This patch should **NOT** be installed on System Manager 8.1.x Software Only deployments.

11-April-2022 – Supplement 18 – Supplement 18 of this PCN introduces **Avaya Aura System Manager 8.1 Security Service Pack SSP #19 (System_Manager_SSP_R8.1.0.0_Patch19_810014363.bin; PLDS**

ID SMGR81SSP19)

To determine that System Manager software that is being run on your server you can:


- Log on to the System Manager Web Interface.
- On the top-right corner click on the  icon and then select the “About” link. Verify version details present on About page.

IMPORTANT NOTE:

- System Manager 8.1 SSP #19 is applicable to System Manager 8.1.0 through 8.1.3.4.
- This patch is not applicable for System Manager 8.1.x Software Only deployments. This patch should **NOT** be installed on System Manager 8.1.x Software Only deployments.

14-March-2022 – Supplement 17 – Supplement 17 of this PCN introduces **Avaya Aura System Manager 8.1 Security Service Pack SSP #18**
(System_Manager_SSP_R8.1.0.0_Patch18_810014282.bin; PLDS ID SMGR81SSP18)

To determine that System Manager software that is being run on your server you can:


- Log on to the System Manager Web Interface.
- On the top-right corner click on the  icon and then select the “About” link. Verify version details present on About page.

IMPORTANT NOTE:

- System Manager 8.1 SSP #18 is applicable to System Manager 8.1.0 through 8.1.3.4.
- This patch is not applicable for System Manager 8.1.x Software Only deployments. This patch should **NOT** be installed on System Manager 8.1.x Software Only deployments.

22-February-2022 – Supplement 16 – Supplement 16 of this PCN introduces **Avaya Aura System Manager 8.1 Security Service Pack SSP #17**
(System_Manager_SSP_R8.1.0.0_Patch17_810014187.bin; PLDS ID SMGR81SSP17)

To determine that System Manager software that is being run on your server you can:


- Log on to the System Manager Web Interface.
- On the top-right corner click on the  icon and then select the “About” link. Verify version details present on About page.

IMPORTANT NOTE:

- System Manager 8.1 SSP #17 is applicable to System Manager 8.1.0 through 8.1.3.4.
- This patch is not applicable for System Manager 8.1.x Software Only deployments. This patch should **NOT** be installed on System Manager 8.1.x Software Only deployments.

20-December-2021 – Supplement 14 – Supplement 14 of this PCN introduces **Avaya Aura System Manager 8.1 Security Service Pack SSP #15**
(System_Manager_SSP_R8.1.0.0_Patch15_810013886.bin; PLDS ID SMGR81SSP15)

To determine that System Manager software that is being run on your server you can:

- Log on to the System Manager Web Interface.
- On the top-right corner click on the  icon and then select the “About” link. Verify version


details present on About page.

IMPORTANT NOTE:

- System Manager 8.1 SSP #15 is applicable to System Manager 8.1.0 through 8.1.3.3
- This patch is not applicable for System Manager 8.1.x Software Only deployments. This patch should **NOT** be installed on System Manager 8.1.x Software Only deployments.

10-January-2022 – Supplement 15 – Supplement 15 of this PCN introduces **Avaya Aura System Manager 8.1 Security Service Pack SSP #16**
(System_Manager_SSP_R8.1.0.0_Patch16_810014059.bin; PLDS ID SMGR81SSP16)

To determine that System Manager software that is being run on your server you can:


- Log on to the System Manager Web Interface.
- On the top-right corner click on the  icon and then select the “About” link. Verify version details present on About page.

IMPORTANT NOTE:

- System Manager 8.1 SSP #16 is applicable to System Manager 8.1.0 through 8.1.3.3
- This patch is not applicable for System Manager 8.1.x Software Only deployments. This patch should **NOT** be installed on System Manager 8.1.x Software Only deployments.

20-December-2021 – Supplement 14 – Supplement 14 of this PCN introduces **Avaya Aura System Manager 8.1 Security Service Pack SSP #15**
(System_Manager_SSP_R8.1.0.0_Patch15_810013886.bin; PLDS ID SMGR81SSP15)

To determine that System Manager software that is being run on your server you can:


- Log on to the System Manager Web Interface.
- On the top-right corner click on the  icon and then select the “About” link. Verify version details present on About page.

IMPORTANT NOTE:

- System Manager 8.1 SSP #15 is applicable to System Manager 8.1.0 through 8.1.3.3
- This patch is not applicable for System Manager 8.1.x Software Only deployments. This patch should **NOT** be installed on System Manager 8.1.x Software Only deployments.

15-November-2021 – Supplement 13 – Supplement 13 of this PCN introduces **Avaya Aura System Manager 8.1 Security Service Pack SSP #14**
(System_Manager_SSP_R8.1.0.0_Patch14_810013693.bin; PLDS ID SMGR81SSP14)

To determine that System Manager software that is being run on your server you can:


- Log on to the System Manager Web Interface.
- On the top-right corner click on the  icon and then select the “About” link. Verify version details present on About page.

IMPORTANT NOTE:

- System Manager 8.1 SSP #14 is applicable to System Manager 8.1.0 through 8.1.3.3
- This patch is not applicable for System Manager 8.1.x Software Only deployments. This patch should **NOT** be installed on System Manager 8.1.x Software Only deployments.

13-September-2021 – Supplement 12 – Supplement 12 of this PCN introduces **Avaya Aura System Manager 8.1 Security Service Pack SSP #13**
(System_Manager_SSP_R8.1.0.0_Patch13_810013160.bin; PLDS ID SMGR81SSP13)

To determine that System Manager software that is being run on your server you can:


- Log on to the System Manager Web Interface.
- On the top-right corner click on the  icon and then select the “About” link. Verify version details present on About page.

IMPORTANT NOTE:

- System Manager 8.1 SSP #13 is applicable to System Manager 8.1.0 through 8.1.3.2
- This patch is not applicable for System Manager 8.1.x Software Only deployments. This patch should **NOT** be installed on System Manager 8.1.x Software Only deployments.

9-August-2021 – Supplement 11 – Supplement 11 of this PCN introduces **Avaya Aura System Manager 8.1 Security Service Pack SSP #12**
(System_Manager_SSP_R8.1.0.0_Patch12_810012960.bin; PLDS ID SMGR81SSP12)

To determine that System Manager software that is being run on your server you can:


- Log on to the System Manager Web Interface.
- On the top-right corner click on the  icon and then select the “About” link. Verify version details present on About page.

IMPORTANT NOTE:

- System Manager 8.1 SSP #12 is applicable to System Manager 8.1.0 through 8.1.3.2
- This patch is not applicable for System Manager 8.1.x Software Only deployments. This patch should **NOT** be installed on System Manager 8.1.x Software Only deployments.

12-July-2021 – Supplement 10 – Supplement 10 of this PCN introduces **Avaya Aura System Manager 8.1 Security Service Pack SSP #11** (System_Manager_SSP_R8.1.0.0_Patch11_810012756.bin; PLDS ID SMGR81SSP11)

To determine that System Manager software that is being run on your server you can:


- Log on to the System Manager Web Interface.
- On the top-right corner click on the  icon and then select the “About” link. Verify version details present on About page.

IMPORTANT NOTE:

- System Manager 8.1 SSP #11 is applicable to System Manager 8.1.0 through 8.1.3.2
- This patch is not applicable for System Manager 8.1.x Software Only deployments. This patch should **NOT** be installed on System Manager 8.1.x Software Only deployments.

14-June-2021 – Supplement 9 – Supplement 9 of this PCN introduces **Avaya Aura System Manager 8.1 Security Service Pack SSP #10** (System_Manager_SSP_R8.1.0.0_Patch10_810012639.bin; PLDS ID SMGR81SSP10)

To determine that System Manager software that is being run on your server you can:

- Log on to the System Manager Web Interface.
- On the top-right corner click on the  icon and then select the “About” link. Verify version details present on About page.


IMPORTANT NOTE:

- System Manager 8.1 SSP #10 is applicable to System Manager 8.1.0 through 8.1.3.1
 - System Manager 8.1.3.2 has a tentative GA date of June 21, 2021.
 - System Manager 8.1.3.2 contains the security updates in SSP #10.
 - Therefore, System Manager SSP #10 does not need to be applied to System Manager 8.1.3.2
 - SSPs #8 and SSP #9 have been removed from PLDS due to the issue described in PSN005561u. SSP #10 should be used instead.
- This patch is not applicable for System Manager 8.1.x Software Only deployments. This patch should **NOT** be installed on System Manager 8.1.x Software Only deployments.

~~11 May 2021 – Supplement 8 – Supplement 8 of this PCN introduces Avaya Aura System Manager 8.1 Security Service Pack #9 (System_Manager_SSP_R8.1.0.0_Patch9_810012552.bin; PLDS ID SMGR810SSP9)~~

Removed – see Supplement 9 above.

To determine that System Manager software that is being run on your server you can:

- Log on to the System Manager Web Interface.
- On the top-right corner click on the  icon and then select the “About” link. Verify version details present on About page.


IMPORTANT NOTE:

- This patch is not applicable for System Manager 8.1.x Software Only deployments. This patch should **NOT** be installed on System Manager 8.1.x Software Only deployments.
- System Manager 8.1.0.0, 8.1.1.0, 8.1.2.0, 8.1.3.0 and 8.1.3.1 Releases do not include security fixes present in SSP 9 so System Manager 8.1 SSP 9 can be installed on top of 8.1.0.0 or 8.1.1.0 or 8.1.2.0 or 8.1.3.0 or 8.1.3.1 release.

~~5 April 2021 – Supplement 7 – Supplement 7 of this PCN introduces Avaya Aura System Manager 8.1 Security Service Pack #8 (System_Manager_SSP_R8.1.0.0_Patch8_810012429.bin; PLDS ID SMGR810SSP8)~~

Removed – see Supplement 9 above.

To determine that System Manager software that is being run on your server you can:

- Log on to the System Manager Web Interface.
- On the top-right corner click on the  icon and then select the “About” link. Verify version details present on About page.

IMPORTANT NOTE:

- This patch is not applicable for System Manager 8.1.x Software Only deployments. This patch should **NOT** be installed on System Manager 8.1.x Software Only deployments.
- System Manager 8.1.0.0, 8.1.1.0, 8.1.2.0, 8.1.3.0 and 8.1.3.1 Releases do not include security fixes present in SSP 8 so System Manager 8.1 SSP 8 can be installed on top of 8.1.0.0 or 8.1.1.0 or 8.1.2.0 or 8.1.3.0 or 8.1.3.1 release.

NOTE: The Avaya Aura® System Manager release/version must always be greater than or equal to the release/version of the components of the solution (Session Manager, Communication Manager, Application Enablement Services).


NOTE: System Manager 8.1 includes Enhanced Access Security Gateway (EASG) for robust product access security. Review the Avaya Aura Release notes for additional information.

NOTE: The VMware® vSphere™ Client can no longer connect to AVP. SDM or the VMware embedded host client must be used. Refer Avaya Aura documentation for additional information.

Also see the Avaya Aura Release Notes available on the Avaya Support Site for a complete list of Enhancements / Fixes available in 8.1.0.0/8.1.1.0/8.1.2.0/8.1.3.0/8.1.3.1 release.

8-February-2021 – Supplement 6 – Supplement 6 of this PCN introduces **Avaya Aura System Manager 8.1 Security Service Pack #7 (System_Manager_SSP_R8.1.0.0_Patch7_810012168.bin; PLDS ID SMGR810SSP7)**

To determine that System Manager software that is being run on your server you can:

- Log on to the System Manager Web Interface.
- On the top-right corner click on the  icon and then select the “About” link. Verify version details present on About page.

IMPORTANT NOTE:

- This patch is not applicable for System Manager 8.1.x Software Only deployments. This patch should **NOT** be installed on System Manager 8.1.x Software Only deployments.
- System Manager 8.1 SSP 7 security fixes are included in the System Manager 8.1.3.1 Service pack release.
- System Manager 8.1.0.0, 8.1.1.0, 8.1.2.0 and 8.1.3.0 Releases do not include security fixes present in SSP 7 so System Manager 8.1 SSP 7 can be installed on top of 8.1.0.0 or 8.1.1.0 or 8.1.2.0 or 8.1.3.0 release.

NOTE: The Avaya Aura® System Manager release/version must always be greater than or equal to the release/version of the components of the solution (Session Manager, Communication Manager, Application Enablement Services).


NOTE: System Manager 8.1 includes Enhanced Access Security Gateway (EASG) for robust product access security. Review the Avaya Aura Release notes for additional information.

NOTE: The VMware® vSphere™ Client can no longer connect to AVP. SDM or the VMware embedded host client must be used. Refer Avaya Aura documentation for additional information.

Also see the Avaya Aura Release Notes available on the Avaya Support Site for a complete list of Enhancements / Fixes available in 8.1.0.0/8.1.1.0/8.1.2.0/8.1.3.0 release.

14-December-2020 – Supplement 5 – Supplement 5 of this PCN introduces **Avaya Aura System Manager 8.1 Security Service Pack #6 (System_Manager_SSP_R8.1.0.0_Patch6_810011933.bin; PLDS ID SMGR810SSP6)**

To determine that System Manager software that is being run on your server you can:

- Log on to the System Manager Web Interface.
- On the top-right corner click on the  icon and then select the “About” link. Verify version

details present on About page.

IMPORTANT NOTE:

- This patch is not applicable for System Manager 8.1.x Software Only deployments. This patch should **NOT** be installed on System Manager 8.1.x Software Only deployments.
- System Manager 8.1.0.0, 8.1.1.0, 8.1.2.0 and 8.1.3.0 Releases do not include security fixes present in SSP 6 so System Manager 8.1 SSP 6 can be installed on top of 8.1.0.0 or 8.1.1.0 or 8.1.2.0 or 8.1.3.0 release.

NOTE: The Avaya Aura® System Manager release/version must always be greater than or equal to the release/version of the components of the solution (Session Manager, Communication Manager, Application Enablement Services).


NOTE: System Manager 8.1 includes Enhanced Access Security Gateway (EASG) for robust product access security. Review the Avaya Aura Release notes for additional information.

NOTE: The VMware® vSphere™ Client can no longer connect to AVP. SDM or the VMware embedded host client must be used. Refer Avaya Aura documentation for additional information.

Also see the Avaya Aura Release Notes available on the Avaya Support Site for a complete list of Enhancements / Fixes available in 8.1.0.0/8.1.1.0/8.1.2.0/8.1.3.0 release.

12-October-2020 – Supplement 4 – Supplement 4 of this PCN introduces **Avaya Aura System Manager 8.1 Security Service Pack #5 (System_Manager_SSP_R8.1.0.0_Patch5_810011775.bin; PLDS ID SMGR81SSP06)**

To determine that System Manager software that is being run on your server you can:

- Log on to the System Manager Web Interface.
- On the top-right corner click on the  icon and then select the “About” link. Verify version details present on About page.

IMPORTANT NOTE:

- This patch is not applicable for System Manager 8.1.x Software Only deployments. This patch should **NOT** be installed on System Manager 8.1.x Software Only deployments.
- System Manager 8.1 SSP 5 security fixes are included in the System Manager 8.1.3.0 feature pack release.
- System Manager 8.1.0.0, 8.1.1.0 and 8.1.2.0 Releases do not include security fixes present in SSP so System Manager 8.1 SSP 5 can be installed on top of 8.1.0.0 or 8.1.1.0 or 8.1.2.0 release.

NOTE: The Avaya Aura® System Manager release/version must always be greater than or equal to the release/version of the components of the solution (Session Manager, Communication Manager, Application Enablement Services).


NOTE: System Manager 8.1 includes Enhanced Access Security Gateway (EASG) for robust product access security. Review the Avaya Aura Release notes for additional information.

NOTE: The VMware® vSphere™ Client can no longer connect to AVP. SDM or the VMware embedded host client must be used. Refer Avaya Aura documentation for additional information.

Also see the Avaya Aura Release Notes available on the Avaya Support Site for a complete list of Enhancements / Fixes available in 8.1.0.0/8.1.1.0/8.1.2.0/8.1.3.0 release.

8-June-2020 – Supplement 3 – Supplement 3 of this PCN introduces **Avaya Aura System Manager 8.1 Security Service Pack #4 (System_Manager_SSP_R8.1.0.0_Patch4_810011383.bin; PLDS ID SMGR81SSP04)**

To determine that System Manager software that is being run on your server you can:

- Log on to the System Manager Web Interface.
- On the top-right corner click on the  icon and then select the “About” link. Verify version details present on About page.

IMPORTANT NOTE:

- This patch is not applicable for System Manager 8.1.x Software Only deployments. This patch should **NOT** be installed on System Manager 8.1.x Software Only deployments.
- System Manager 8.1 SSP 4 security fixes are **NOT** included in the System Manager 8.1.2.0 feature pack release.
- System Manager 8.1.0.0 and 8.1.1.0 Releases do not include security fixes present in SSP so System Manager 8.1 SSP 4 can be installed on top of 8.1.0.0 or 8.1.1.0 release.

NOTE: The Avaya Aura® System Manager release/version must always be greater than or equal to the release/version of the components of the solution (Session Manager, Communication Manager, Application Enablement Services).


NOTE: System Manager 8.1 includes Enhanced Access Security Gateway (EASG) for robust product access security. Review the Avaya Aura Release notes for additional information.

NOTE: The VMware® vSphere™ Client can no longer connect to AVP. SDM or the VMware embedded host client must be used. Refer Avaya Aura documentation for additional information.

Also see the Avaya Aura Release Notes available on the Avaya Support Site for a complete list of Enhancements / Fixes available in 8.1.0.0/8.1.1.0/8.1.2.0 release.

2-March-2020 – Supplement 2 – Supplement 2 of this PCN introduces **Avaya Aura System Manager 8.1 Security Service Pack #3 (System_Manager_SSP_R8.1.0.0_Patch3_810011047.bin; PLDS ID SMGR81SSP03)**

To determine that System Manager software that is being run on your server you can:

- Log on to the System Manager Web Interface.
- On the top-right corner click on the  icon and then select the “About” link. Verify version details present on About page.

IMPORTANT NOTE:

- This patch is not applicable for System Manager 8.1.x Software Only deployments. This patch should **NOT** be installed on System Manager 8.1.x Software Only deployments.
- System Manager 8.1 SSP 3 security fixes are also included in the System Manager 8.1.2.0 feature pack so no need to install System Manager SSP 3 on System Manager 8.1.2.0 release.
- System Manager 8.1.0.0 and 8.1.1.0 Releases do not include security fixes present in SSP so System Manager 8.1 SSP 3 can be installed on top of 8.1.0.0 or 8.1.1.0 release.

NOTE: The Avaya Aura® System Manager release/version must always be greater than or equal to the release/version of the components of the solution (Session Manager, Communication Manager, Application Enablement Services).

NOTE: System Manager 8.1 includes Enhanced Access Security Gateway (EASG) for robust product access security. Review the Avaya Aura Release notes for additional information.


NOTE: The VMware® vSphere™ Client can no longer connect to AVP. SDM or the VMware embedded host client must be used. Refer Avaya Aura documentation for additional information.

Also see the Avaya Aura Release Notes available on the Avaya Support Site for a complete list of Enhancements / Fixes available in 8.1.0.0/8.1.1.0/8.1.2.0 release.

28-October-2019 – Supplement 1 – Supplement 1 of this PCN introduces **Avaya Aura System Manager 8.1 Security Service Pack #2 (System_Manager_SSP_R8.1.0.0_Patch2_810010394.bin; PLDS ID SMGR81SSP02)**

SMGR 8.1 SSP patch can be installed on top of 8.1.0.0 and 8.1.1.0 Releases.

To determine that System Manager software that is being run on your server you can:

- Log on to the System Manager Web Interface.
- On the top-right corner click on the  icon and then select the “About” link. Verify version details present on About page.

IMPORTANT NOTE: This patch is not applicable for System Manager 8.1.x Software Only deployments. This patch should **NOT** be installed on System Manager 8.1.x Software Only deployments.

NOTE: The Avaya Aura® System Manager release/version must always be greater than or equal to the release/version of the components of the solution (Session Manager, Communication Manager, Application Enablement Services).

NOTE: System Manager 8.1 includes Enhanced Access Security Gateway (EASG) for robust product access security. Review the Avaya Aura Release notes for additional information.

NOTE: The VMware® vSphere™ Client can no longer connect to AVP. SDM or the VMware embedded host client must be used. Refer Avaya Aura documentation for additional information.

Also see the Avaya Aura Release Notes available on the Avaya Support Site for a complete list of Enhancements / Fixes available in 8.1 and 8.1.1 release.

15-July-2019 – This PCN introduces **Avaya Aura System Manager 8.1 Security Service Pack #1 (System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin; PLDS ID SMGR81SSP01)**

- **Appliance Virtualization Platform (AVP) 8.1.0.0.13 (avaya-avp-8.1.0.0.13.iso or upgrade-avaya-avp-8.1.0.0.13.zip.)** The System Manager software specified in this PCN was verified and is compatible with AVP release 8.1.0.0.13. See PCN2097S for more information. AVP must be upgraded to the compatible release before upgrading System Manager.

NOTE: The Avaya Aura® System Manager release/version must always be greater than or equal to the release/version of the components of the solution (Session Manager, Communication Manager, Application Enablement Services).


NOTE: System Manager 8.1 includes Enhanced Access Security Gateway (EASG) for robust product

access security. Review the Avaya Aura Release notes for additional information.

NOTE: The VMware® vSphere™ Client can no longer connect to AVP. SDM or the VMware embedded host client must be used. Refer Avaya Aura documentation for additional information.

Also see the Avaya Aura Release Notes available on the Avaya Support Site for a complete list of Enhancements / Fixes available in 8.1 release.

To determine that System Manager software that is being run on your server you can:

- Log on to the System Manager Web Interface.
- On the top-right corner click on the  icon and then select the “About” link. Verify version details present on About page.

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 Avaya Aura® System Manager 8.1.x release.

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?

Yes. This security service Pack will disrupt service in that it requires a system reboot to take effect. System Manager services are re-started during installation or upgrade so web access to System Manager will be disrupted during security service Pack deployment, so security service Pack deployment 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 Security 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. 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 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 System 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 System 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 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 **System Manager** when Avaya Aura® System 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® System Manager 8.1 Security Service Pack**.
7. Select the Download link to begin the download.

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 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 **System Manager** in the **Product Line** search field to display frequently downloaded System Manager Software, including recent Service Packs and updates.

2. Previous System Manager Release Software's are also available on PLDS. In the PLDS **View Downloads** section under the **Search by Download** tab, select **System Manager** in the **Application** search field and **8.1** in the **Version** search field to display all available System Manager 8.1 software downloads.

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

NOTE: If deploying System Manager on AVP the compatible AVP software is also required.

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

Important Security Service Pack Installation Notes:

- If System Manager installation is a Geo-Redundancy enabled deployment, disable Geo-Redundancy, and apply the SSP patch on Both System Manager systems, and then re-enable Geo-Redundancy.
- 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.
- Installing System Manager Security Service Pack through Software Upgrade Management(SDM) is not supported.
- This patch is **NOT** applicable for System Manager 8.1.x Software Only deployments. This patch should not be installed on System Manager 8.1.x Software Only deployments.
- System Manager 8.1 SSP #30 is applicable to System Manager 8.1.0 through 8.1.3.7.
Note - No need to install Security Service Pack(SSP) #30 on the 8.1.3.8 Service Pack as 8.1.3.8 already contains all security updates included in SSP #30.

Security Service Pack Installation instructions:

- Create a snapshot of System Manager virtual machine.
Note: Make sure its non-live(non-running) snapshot. This activity might impact the service.
- Copy the Security Service Pack patch installer file to the System Manager server at /swlibrary location.
- Log in to the System Manager virtual machine using user having administrative privileges.
#cd /swlibrary/
- Verify md5sum of the bin file with the value mentioned in the support site.
#md5sum <Security Service Pack Patch bin file name>
- Run the patch installer using the following command:
#SMGRPachdeploy <Security Service Pack Patch bin file name>
- Accept the EULA to proceed installation.
- Wait for the system to execute the patch installer in the background and display the installer prompt.
- Please verify below output in SSP installation logs to confirm successful patch installation
#tail -f /var/log/Avaya/SMGRSSP_Patch.log
#####Patch execution completed successfully in the background #####
- swversion output will have below content
SMGR SSP 8.1.x.x Build Number 8.1.x.x.x
Patch 8.1.x.xxxxxx Build Number 8.1.x.x.xx15698

- All the services will be down post SSP installation and Security service Pack requires a system reboot to take effect so **reboot** System Manager virtual machine after SSP installation.
- Verify System functionality post system reboot and delete old VM snapshot post successful verification.

IMPORTANT NOTE - If you have configured a NFS mount on System Manager for Session Manager Performance Data (perfdata) collection, then, if and when you reboot / boot your System Manager virtual machine, you need to ensure that you manually re-mount the NFS store once the System Manager VM is up, and you are able to login to the VM via SSH. Failure to re-mount the NSF partition will result in the Session Manager perfdata to go, by default, into a folder which is in the root (/) partition of the System Manager filesystem. This may cause the partition to get full which in-turn may cause issues with the System Manager application.

Important Security Service Pack Installation Notes:

- 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.

SECTION 1A – SOFTWARE SERVICE PACK INFORMATION

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

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

To verify the successful installation of System Manager Security Service Pack.

- Log on to the System Manager command line interface.
- Execute command “swversion”, verify that the output contains as below:
SMGR SSP 8.1.x.x Build Number 8.1.x.x.x
Patch 8.1.x.xxxxxx Build Number 8.1.x.x.xx15698

What you should do if the Service Pack installation fails?

- Please refer Contact support tasks of System Manager 8.1.x release notes section to collect logs from the system.
- Escalate to Avaya **Global Support Services (GSS)** or an Avaya authorized Business Partner if issue persists.

How to remove the Service Pack if malfunction of your system occurs:

N/A

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 as noted.

Avaya Security

Note: A Classification of None in the tables below means the affected components are installed, but

**Vulnerability
Classification:**

the vulnerability is not exploitable.

As noted in the Description section of 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.

Beginning with SMGR SSP#9, the format of the information in this section is expanded.

Security Service Packs (SSP) are cumulative. This means that all fixes in previous 8.1.x SSPs are included in the most recent SSP.

SSP Patch #30 contains the fixes from the following previous patches:

System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin
 System_Manager_SSP_R8.1.0.0_Patch2_810010394.bin
 System_Manager_SSP_R8.1.0.0_Patch3_810011047.bin
 System_Manager_SSP_R8.1.0.0_Patch4_810011383.bin
 System_Manager_SSP_R8.1.0.0_Patch5_810011775.bin
 System_Manager_SSP_R8.1.0.0_Patch6_810011933.bin
 System_Manager_SSP_R8.1.0.0_Patch7_810012168.bin
 System_Manager_SSP_R8.1.0.0_Patch8_810012429.bin
 System_Manager_SSP_R8.1.0.0_Patch9_810012552.bin
 System_Manager_SSP_R8.1.0.0_Patch10_810012639.bin
 System_Manager_SSP_R8.1.0.0_Patch11_810012756.bin
 System_Manager_SSP_R8.1.0.0_Patch12_810012960.bin
 System_Manager_SSP_R8.1.0.0_Patch13_810013160.bin
 System_Manager_SSP_R8.1.0.0_Patch14_810013693.bin
 System_Manager_SSP_R8.1.0.0_Patch15_810013886.bin
 System_Manager_SSP_R8.1.0.0_Patch16_810014059.bin
 System_Manager_SSP_R8.1.0.0_Patch17_810014187.bin
 System_Manager_SSP_R8.1.0.0_Patch18_810014282.bin
 System_Manager_SSP_R8.1.0.0_Patch19_810014363.bin
 System_Manager_SSP_R8.1.0.0_Patch20_810014469.bin
 System_Manager_SSP_R8.1.0.0_Patch21_810014593.bin
 System_Manager_SSP_R8.1.0.0_Patch22_810014775.bin
 System_Manager_SSP_R8.1.0.0_Patch23_810014926.bin
 System_Manager_SSP_R8.1.0.0_Patch24_810015019.bin
 System_Manager_SSP_R8.1.0.0_Patch25_810015188.bin
 System_Manager_SSP_R8.1.0.0_Patch26_810015327.bin
 System_Manager_SSP_R8.1.0.0_Patch27_810015404.bin
 System_Manager_SSP_R8.1.0.0_Patch28_810015486.bin
 System_Manager_SSP_R8.1.0.0_Patch29_810015565.bin

Therefore, old SSP patches are removed from PLDS/support site.

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

bind-export-libs-32:9.11.4-26.P2.el7_9.13.x86_64.rpm	libsss_idmap-1.16.5-10.el7_9.15.x86_64.rpm
bind-libs-32:9.11.4-26.P2.el7_9.13.x86_64.rpm	libsss_nss_idmap-1.16.5-10.el7_9.15.x86_64.rpm
bind-libs-lite-32:9.11.4-26.P2.el7_9.13.x86_64.rpm	nss-3.79.0-5.el7_9.x86_64.rpm
bind-license-32:9.11.4-26.P2.el7_9.13.noarch.rpm	nss-sysinit-3.79.0-5.el7_9.x86_64.rpm
bind-utils-32:9.11.4-26.P2.el7_9.13.x86_64.rpm	nss-tools-3.79.0-5.el7_9.x86_64.rpm
bpftool-3.10.0-1160.88.1.el7.x86_64.rpm	openssl-1:1.0.2k-26.el7_9.x86_64.rpm

git-1.8.3.1-24.el7_9.x86_64.rpm java-1.8.0-openjdk-1:1.8.0.362.b08-1.el7_9.x86_64.rpm 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 kernel-3.10.0-1160.88.1.el7.x86_64.rpm kernel-tools-3.10.0-1160.88.1.el7.x86_64.rpm kernel-tools-libs-3.10.0-1160.88.1.el7.x86_64.rpm	openssl-libs-1:1.0.2k-26.el7_9.x86_64.rpm perl-Git-1.8.3.1-24.el7_9.noarch.rpm python-perf-3.10.0-1160.88.1.el7.x86_64.rpm sssd-client-1.16.5-10.el7_9.15.x86_64.rpm sudo-1.8.23-10.el7_9.3.x86_64.rpm zlib-1.2.7-21.el7_9.i686.rpm tzdata-2023c-1.el7.noarch.rpm tzdata-java-2023c-1.el7.noarch.rpm
--	---

Security vulnerabilities resolved in System Manager 8.1 Security Service Pack Patch #30:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-72683	bind-export-libs bind-libs bind-libs-elite bind-license bind-utils	RHSA-2023:0402	CVE-2021-25220 CVE-2022-2795	Moderate	ASA-2023-014	Medium
SMGR-72680	bpftool kernel kernel-tools kernel-tools-libs python-perf	RHSA-2023:0399	CVE-2021-26401 CVE-2022-2964	Important	N/A	N/A
SMGR-72692	bpftool kernel kernel-tools kernel-tools-libs python-perf	RHSA-2023:1091	CVE-2022-42703 CVE-2022-4378	Important	ASA-2023-029	High
SMGR-72689	git perl-Git	RHSA-2023:0978	CVE-2022-23521 CVE-2022-41903	Important	ASA-2023-026	Critical
SMGR-72674	java-1.8.0-openjdk 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
SMGR-72686	sss-idmap libsss_nss_idmap sssd_client	RHSA-2023:0403	CVE-2022-4254	Important	ASA-2023-013	Low
SMGR-72698	nss nss-sysinit nss-tools	RHSA-2023:1332	CVE-2023-0767	Important	N/A	N/A
SMGR-72701	openssl openssl-libs	RHSA-2023:1335	CVE-2023-0286	Important	ASA-2023-030	High
SMGR-72677	sudo	RHSA-2023:0291	CVE-2023-22809	Important	N/A	N/A
SMGR-72695	zlib	RHSA-2023:1095	CVE-2022-37434	Moderate	N/A	Moderate

SMGR-72705	tzdata tzdata-java	RHBA-2023:1534	N/A	Bug Fix	N/A	N/A
------------	-----------------------	----------------	-----	---------	-----	-----

SSP Patch #29 contains the fixes from the following previous patches:

System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin
 System_Manager_SSP_R8.1.0.0_Patch2_810010394.bin
 System_Manager_SSP_R8.1.0.0_Patch3_810011047.bin
 System_Manager_SSP_R8.1.0.0_Patch4_810011383.bin
 System_Manager_SSP_R8.1.0.0_Patch5_810011775.bin
 System_Manager_SSP_R8.1.0.0_Patch6_810011933.bin
 System_Manager_SSP_R8.1.0.0_Patch7_810012168.bin
 System_Manager_SSP_R8.1.0.0_Patch8_810012429.bin
 System_Manager_SSP_R8.1.0.0_Patch9_810012552.bin
 System_Manager_SSP_R8.1.0.0_Patch10_810012639.bin
 System_Manager_SSP_R8.1.0.0_Patch11_810012756.bin
 System_Manager_SSP_R8.1.0.0_Patch12_810012960.bin
 System_Manager_SSP_R8.1.0.0_Patch13_810013160.bin
 System_Manager_SSP_R8.1.0.0_Patch14_810013693.bin
 System_Manager_SSP_R8.1.0.0_Patch15_810013886.bin
 System_Manager_SSP_R8.1.0.0_Patch16_810014059.bin
 System_Manager_SSP_R8.1.0.0_Patch17_810014187.bin
 System_Manager_SSP_R8.1.0.0_Patch18_810014282.bin
 System_Manager_SSP_R8.1.0.0_Patch19_810014363.bin
 System_Manager_SSP_R8.1.0.0_Patch20_810014469.bin
 System_Manager_SSP_R8.1.0.0_Patch21_810014593.bin
 System_Manager_SSP_R8.1.0.0_Patch22_810014775.bin
 System_Manager_SSP_R8.1.0.0_Patch23_810014926.bin
 System_Manager_SSP_R8.1.0.0_Patch24_810015019.bin
 System_Manager_SSP_R8.1.0.0_Patch25_810015188.bin
 System_Manager_SSP_R8.1.0.0_Patch26_810015327.bin
 System_Manager_SSP_R8.1.0.0_Patch27_810015404.bin
 System_Manager_SSP_R8.1.0.0_Patch28_810015486.bin

Therefore, old SSP patches are removed from PLDS/support site.

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

bind-export-libs-32:9.11.4-26.P2.el7_9.13.x86_64.rpm bind-libs-32:9.11.4-26.P2.el7_9.13.x86_64.rpm bind-libs-lite-32:9.11.4-26.P2.el7_9.13.x86_64.rpm bind-license-32:9.11.4-26.P2.el7_9.13.noarch.rpm bind-utils-32:9.11.4-26.P2.el7_9.13.x86_64.rpm bpftool-3.10.0-1160.83.1.el7.x86_64.rpm java-1.8.0-openjdk-1:1.8.0.362.b08-1.el7_9.x86_64.rpm 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	kernel-3.10.0-1160.83.1.el7.x86_64.rpm kernel-tools-3.10.0-1160.83.1.el7.x86_64.rpm kernel-tools-libs-3.10.0-1160.83.1.el7.x86_64.rpm libsss_idmap-1.16.5-10.el7_9.15.x86_64.rpm libsss_nss_idmap-1.16.5-10.el7_9.15.x86_64.rpm python-perf-3.10.0-1160.83.1.el7.x86_64.rpm sssd-client-1.16.5-10.el7_9.15.x86_64.rpm sudo-1.8.23-10.el7_9.3.x86_64.rpm
--	--

Security vulnerabilities resolved in System Manager 8.1 Security Service Pack Patch #29:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-72331	sss-idmap libsss_nss_idmap sssd_client	RHSA-2023:0403	CVE-2022-4254	Important	ASA-2023-013	Low
SMGR-72328	bind-export-libs bind-libs bind-libs-elite bind-license bind-utils	RHSA-2023:0402	CVE-2021-25220 CVE-2022-2795	Moderate	ASA-2023-014	Medium
SMGR-72325	bpftool kernel kernel-tools kernel-tools-libs python-perf	RHSA-2023:0399	CVE-2021-26401 CVE-2022-2964	Important	N/A	N/A
SMGR-72322	sudo	RHSA-2023:0291	CVE-2023-22809	Important	N/A	N/A
SMGR-72319	java-1.8.0-openjdk 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

SSP Patch#28 contains the fixes from the following previous patches:

System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin
System_Manager_SSP_R8.1.0.0_Patch2_810010394.bin
System_Manager_SSP_R8.1.0.0_Patch3_810011047.bin
System_Manager_SSP_R8.1.0.0_Patch4_810011383.bin
System_Manager_SSP_R8.1.0.0_Patch5_810011775.bin
System_Manager_SSP_R8.1.0.0_Patch6_810011933.bin
System_Manager_SSP_R8.1.0.0_Patch7_810012168.bin
System_Manager_SSP_R8.1.0.0_Patch8_810012429.bin
System_Manager_SSP_R8.1.0.0_Patch9_810012552.bin
System_Manager_SSP_R8.1.0.0_Patch10_810012639.bin
System_Manager_SSP_R8.1.0.0_Patch11_810012756.bin
System_Manager_SSP_R8.1.0.0_Patch12_810012960.bin
System_Manager_SSP_R8.1.0.0_Patch13_810013160.bin
System_Manager_SSP_R8.1.0.0_Patch14_810013693.bin
System_Manager_SSP_R8.1.0.0_Patch15_810013886.bin
System_Manager_SSP_R8.1.0.0_Patch16_810014059.bin
System_Manager_SSP_R8.1.0.0_Patch17_810014187.bin
System_Manager_SSP_R8.1.0.0_Patch18_810014282.bin
System_Manager_SSP_R8.1.0.0_Patch19_810014363.bin
System_Manager_SSP_R8.1.0.0_Patch20_810014469.bin
System_Manager_SSP_R8.1.0.0_Patch21_810014593.bin

System_Manager_SSP_R8.1.0.0_Patch22_810014775.bin
 System_Manager_SSP_R8.1.0.0_Patch23_810014926.bin
 System_Manager_SSP_R8.1.0.0_Patch24_810015019.bin
 System_Manager_SSP_R8.1.0.0_Patch25_810015188.bin
 System_Manager_SSP_R8.1.0.0_Patch26_810015327.bin
 System_Manager_SSP_R8.1.0.0_Patch27_810015404.bin

Therefore, old SSP patches are removed from PLDS/support site.

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

krb5-libs-1.15.1-55.el7_9.i686 grub2-1:2.02-0.87.el7_9.11.x86_64 grub2-common-1:2.02-0.87.el7_9.11.noarch grub2-pc-1:2.02-0.87.el7_9.11.x86_64 grub2-pc-modules-1:2.02-0.87.el7_9.11.noarch	grub2-tools-1:2.02-0.87.el7_9.11.x86_64 grub2-tools-extra-1:2.02-0.87.el7_9.11.x86_64 grub2-tools-minimal-1:2.02-0.87.el7_9.11.x86_64 tzdata-2022g-1.el7.noarch tzdata-java-2022g-1.el7.noarch
---	--

Security vulnerabilities resolved in System Manager 8.1 Security Service Pack Patch #28:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-71991	krb5-libs	RHSA-2022:8640	CVE-2022-42898	Important	ASA-2022-161	Medium
SMGR-71993	grub2 grub2-common grub2-pc grub2-pc-modules grub2-tools grub2-tools-extra grub2-tools-minimul	RHSA-2022:8900	CVE-2022- 28733	Important	ASA-2022-162	High
SMGR-71999	tzdata tzdata-java	RHBA-2022:8785	N/A	Bug Fix	N/A	N/A
SMGR-72100	After installing SSP #27, Data replication between SMGR and other elements is not working in some scenarios due TLS 1.3 getting enabled by default.	N/A	N/A	Bug Fix	N/A	N/A

SSP Patch#27 contains the fixes from the following previous patches:

System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin
 System_Manager_SSP_R8.1.0.0_Patch2_810010394.bin
 System_Manager_SSP_R8.1.0.0_Patch3_810011047.bin
 System_Manager_SSP_R8.1.0.0_Patch4_810011383.bin
 System_Manager_SSP_R8.1.0.0_Patch5_810011775.bin

System_Manager_SSP_R8.1.0.0_Patch6_810011933.bin
 System_Manager_SSP_R8.1.0.0_Patch7_810012168.bin
 System_Manager_SSP_R8.1.0.0_Patch8_810012429.bin
 System_Manager_SSP_R8.1.0.0_Patch9_810012552.bin
 System_Manager_SSP_R8.1.0.0_Patch10_810012639.bin
 System_Manager_SSP_R8.1.0.0_Patch11_810012756.bin
 System_Manager_SSP_R8.1.0.0_Patch12_810012960.bin
 System_Manager_SSP_R8.1.0.0_Patch13_810013160.bin
 System_Manager_SSP_R8.1.0.0_Patch14_810013693.bin
 System_Manager_SSP_R8.1.0.0_Patch15_810013886.bin
 System_Manager_SSP_R8.1.0.0_Patch16_810014059.bin
 System_Manager_SSP_R8.1.0.0_Patch17_810014187.bin
 System_Manager_SSP_R8.1.0.0_Patch18_810014282.bin
 System_Manager_SSP_R8.1.0.0_Patch19_810014363.bin
 System_Manager_SSP_R8.1.0.0_Patch20_810014469.bin
 System_Manager_SSP_R8.1.0.0_Patch21_810014593.bin
 System_Manager_SSP_R8.1.0.0_Patch22_810014775.bin
 System_Manager_SSP_R8.1.0.0_Patch23_810014926.bin
 System_Manager_SSP_R8.1.0.0_Patch24_810015019.bin
 System_Manager_SSP_R8.1.0.0_Patch25_810015188.bin
 System_Manager_SSP_R8.1.0.0_Patch26_810015327.bin

Therefore, old SSP patches are removed from PLDS/support site.

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

bpftool-3.10.0-1160.80.1.el7.x86_64 kernel-3.10.0-1160.80.1.el7.x86_64 kernel-tools-3.10.0-1160.80.1.el7.x86_64 kernel-tools-libs-3.10.0-1160.80.1.el7.x86_64	kpartx-0.4.9-136.el7_9.x86_64 python-perf-3.10.0-1160.80.1.el7.x86_64 tzdata-2022f-1.el7.noarch tzdata-java-2022f-1.el7.noarch
--	---

Security vulnerabilities resolved in System Manager 8.1 Security Service Pack Patch #27:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-71734	kpartx	RHSA-2022:7186	CVE-2022-41974	Important	N/A	N/A
SMGR-71737	bpftool kernel kernel-tools kernel-tools-libs python-perf	RHSA-2022:7337	CVE-2022-23816 CVE-2022-23825 CVE-2022-2588 CVE-2022-26373 CVE-2022-29900 CVE-2022-29901	Important	ASA-2022-152	High
SMGR-71740	tzdata tzdata-java	RHBA-2022:7404	N/A	Bug Fix	N/A	N/A

SSP Patch#26 contains the fixes from the following previous patches:

System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin
 System_Manager_SSP_R8.1.0.0_Patch2_810010394.bin
 System_Manager_SSP_R8.1.0.0_Patch3_810011047.bin
 System_Manager_SSP_R8.1.0.0_Patch4_810011383.bin
 System_Manager_SSP_R8.1.0.0_Patch5_810011775.bin
 System_Manager_SSP_R8.1.0.0_Patch6_810011933.bin
 System_Manager_SSP_R8.1.0.0_Patch7_810012168.bin
 System_Manager_SSP_R8.1.0.0_Patch8_810012429.bin
 System_Manager_SSP_R8.1.0.0_Patch9_810012552.bin
 System_Manager_SSP_R8.1.0.0_Patch10_810012639.bin
 System_Manager_SSP_R8.1.0.0_Patch11_810012756.bin
 System_Manager_SSP_R8.1.0.0_Patch12_810012960.bin
 System_Manager_SSP_R8.1.0.0_Patch13_810013160.bin
 System_Manager_SSP_R8.1.0.0_Patch14_810013693.bin
 System_Manager_SSP_R8.1.0.0_Patch15_810013886.bin
 System_Manager_SSP_R8.1.0.0_Patch16_810014059.bin
 System_Manager_SSP_R8.1.0.0_Patch17_810014187.bin
 System_Manager_SSP_R8.1.0.0_Patch18_810014282.bin
 System_Manager_SSP_R8.1.0.0_Patch19_810014363.bin
 System_Manager_SSP_R8.1.0.0_Patch20_810014469.bin
 System_Manager_SSP_R8.1.0.0_Patch21_810014593.bin
 System_Manager_SSP_R8.1.0.0_Patch22_810014775.bin
 System_Manager_SSP_R8.1.0.0_Patch23_810014926.bin
 System_Manager_SSP_R8.1.0.0_Patch24_810015019.bin
 System_Manager_SSP_R8.1.0.0_Patch25_810015188.bin

Therefore, old SSP patches are removed from PLDS/support site.

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

bind-export-libs-32:9.11.4-26.P2.el7_9.10.x86_64 bind-libs-32:9.11.4-26.P2.el7_9.10.x86_64 bind-libs-lite-32:9.11.4-26.P2.el7_9.10.x86_64 bind-license-32:9.11.4-26.P2.el7_9.10.noarch bind-utils-32:9.11.4-26.P2.el7_9.10.x86_64 expat-2.1.0-15.el7_9.x86_64	java-1.8.0-openjdk-1:1.8.0.352.b08-2.el7_9.x86_64 java-1.8.0-openjdk-devel-1:1.8.0.352.b08-2.el7_9.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.352.b08-2.el7_9.x86_64 tzdata-2022d-1.el7.noarch tzdata-java-2022d-1.el7.noarch
--	---

Security vulnerabilities resolved in System Manager 8.1 Security Service Pack Patch #26:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-71462	bind-export-libs bind-libs bind-libs-elite bind-license bind-utils	RHSA-2022:6765	CVE-2022-38177 CVE-2022-38178	Important	ASA-2022-124	High

SMGR-71465	expat	RHSA-2022:6834	CVE-2022-40674	Important	ASA-2022-125	Critical
SMGR-71468	java-1.8.0-openjdk java-1.8.0-openjdk-devel java-1.8.0-openjdk-headless	RHSA-2022:7002	CVE-2022-21619 CVE-2022-21624 CVE-2022-21626 CVE-2022-21628	Moderate	ASA-2022-127	Medium
SMGR-71471	tzdata tzdata-java	RHBA-2021:6827	N/A	Bug Fix	N/A	N/A

SSP Patch#25 contains the fixes from the following previous patches:

System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin
System_Manager_SSP_R8.1.0.0_Patch2_810010394.bin
System_Manager_SSP_R8.1.0.0_Patch3_810011047.bin
System_Manager_SSP_R8.1.0.0_Patch4_810011383.bin
System_Manager_SSP_R8.1.0.0_Patch5_810011775.bin
System_Manager_SSP_R8.1.0.0_Patch6_810011933.bin
System_Manager_SSP_R8.1.0.0_Patch7_810012168.bin
System_Manager_SSP_R8.1.0.0_Patch8_810012429.bin
System_Manager_SSP_R8.1.0.0_Patch9_810012552.bin
System_Manager_SSP_R8.1.0.0_Patch10_810012639.bin
System_Manager_SSP_R8.1.0.0_Patch11_810012756.bin
System_Manager_SSP_R8.1.0.0_Patch12_810012960.bin
System_Manager_SSP_R8.1.0.0_Patch13_810013160.bin
System_Manager_SSP_R8.1.0.0_Patch14_810013693.bin
System_Manager_SSP_R8.1.0.0_Patch15_810013886.bin
System_Manager_SSP_R8.1.0.0_Patch16_810014059.bin
System_Manager_SSP_R8.1.0.0_Patch17_810014187.bin
System_Manager_SSP_R8.1.0.0_Patch18_810014282.bin
System_Manager_SSP_R8.1.0.0_Patch19_810014363.bin
System_Manager_SSP_R8.1.0.0_Patch20_810014469.bin
System_Manager_SSP_R8.1.0.0_Patch21_810014593.bin
System_Manager_SSP_R8.1.0.0_Patch22_810014775.bin
System_Manager_SSP_R8.1.0.0_Patch23_810014926.bin
System_Manager_SSP_R8.1.0.0_Patch24_810015019.bin

Therefore, old SSP patches are removed from PLDS/support site.

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

open-vm-tools-11.0.5-3.el7_9.4.x86_64 rsync-3.1.2-11.el7_9.x86_64 systemd-219-78.el7_9.7.x86_64 systemd-libs-219-78.el7_9.7.i686	systemd-python-219-78.el7_9.7.x86_64 systemd-sysv-219-78.el7_9.7.x86_64 tzdata-2022c-1.el7.noarch tzdata-java-2022c-1.el7.noarch
---	---

Security vulnerabilities resolved in System Manager 8.1 Security Service Pack Patch #25:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-71248	open-vm-tools	RHSA-2022:6381	CVE-2022-31676	Important	ASA-2022-119	High
SMGR-71245	rsync	RHSA-2022:6170	CVE-2022-29154	Important	N/A	N/A
SMGR-71242	system system-libs system-python system-sysv	RHSA-2022:6160	CVE-2022-2526	Important	ASA-2022-115	High
SMGR-71401	tzdata tzdata-java	RHBA-2021:3790 RHBA-2021:4003 RHBA-2021:4543 RHBA-2022:1032 RHBA-2022:6138	N/A	Bug Fix	N/A	N/A

SSP Patch#24 contains the fixes from the following previous patches:

System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin
System_Manager_SSP_R8.1.0.0_Patch2_810010394.bin
System_Manager_SSP_R8.1.0.0_Patch3_810011047.bin
System_Manager_SSP_R8.1.0.0_Patch4_810011383.bin
System_Manager_SSP_R8.1.0.0_Patch5_810011775.bin
System_Manager_SSP_R8.1.0.0_Patch6_810011933.bin
System_Manager_SSP_R8.1.0.0_Patch7_810012168.bin
System_Manager_SSP_R8.1.0.0_Patch8_810012429.bin
System_Manager_SSP_R8.1.0.0_Patch9_810012552.bin
System_Manager_SSP_R8.1.0.0_Patch10_810012639.bin
System_Manager_SSP_R8.1.0.0_Patch11_810012756.bin
System_Manager_SSP_R8.1.0.0_Patch12_810012960.bin
System_Manager_SSP_R8.1.0.0_Patch13_810013160.bin
System_Manager_SSP_R8.1.0.0_Patch14_810013693.bin
System_Manager_SSP_R8.1.0.0_Patch15_810013886.bin
System_Manager_SSP_R8.1.0.0_Patch16_810014059.bin
System_Manager_SSP_R8.1.0.0_Patch17_810014187.bin
System_Manager_SSP_R8.1.0.0_Patch18_810014282.bin
System_Manager_SSP_R8.1.0.0_Patch19_810014363.bin
System_Manager_SSP_R8.1.0.0_Patch20_810014469.bin
System_Manager_SSP_R8.1.0.0_Patch21_810014593.bin
System_Manager_SSP_R8.1.0.0_Patch22_810014775.bin
System_Manager_SSP_R8.1.0.0_Patch23_810014926.bin

Therefore, old SSP patches are removed from PLDS/support site.

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

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

Security vulnerabilities resolved in System Manager 8.1 Security Service Pack Patch #24:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-70890	java-1.8.0-openjdk 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
SMGR-70893	bpftool kernel kernel-tools kernel-tools-libs python-perf	RHSA-2022:5937	CVE-2022-21123 CVE-2022-21125 CVE-2022-21166	Moderate	ASA-2022-113	Medium

SSP Patch#23 contains the fixes from the following previous patches:

System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin
 System_Manager_SSP_R8.1.0.0_Patch2_810010394.bin
 System_Manager_SSP_R8.1.0.0_Patch3_810011047.bin
 System_Manager_SSP_R8.1.0.0_Patch4_810011383.bin
 System_Manager_SSP_R8.1.0.0_Patch5_810011775.bin
 System_Manager_SSP_R8.1.0.0_Patch6_810011933.bin
 System_Manager_SSP_R8.1.0.0_Patch7_810012168.bin
 System_Manager_SSP_R8.1.0.0_Patch8_810012429.bin
 System_Manager_SSP_R8.1.0.0_Patch9_810012552.bin
 System_Manager_SSP_R8.1.0.0_Patch10_810012639.bin
 System_Manager_SSP_R8.1.0.0_Patch11_810012756.bin
 System_Manager_SSP_R8.1.0.0_Patch12_810012960.bin
 System_Manager_SSP_R8.1.0.0_Patch13_810013160.bin
 System_Manager_SSP_R8.1.0.0_Patch14_810013693.bin
 System_Manager_SSP_R8.1.0.0_Patch15_810013886.bin
 System_Manager_SSP_R8.1.0.0_Patch16_810014059.bin
 System_Manager_SSP_R8.1.0.0_Patch17_810014187.bin
 System_Manager_SSP_R8.1.0.0_Patch18_810014282.bin
 System_Manager_SSP_R8.1.0.0_Patch19_810014363.bin
 System_Manager_SSP_R8.1.0.0_Patch20_810014469.bin
 System_Manager_SSP_R8.1.0.0_Patch21_810014593.bin
 System_Manager_SSP_R8.1.0.0_Patch22_810014775.bin

Therefore, old SSP patches are removed from PLDS/support site.

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

bpftool-3.10.0-1160.71.1.el7.x86_64 kernel-3.10.0-1160.71.1.el7.x86_64 kernel-tools-3.10.0-1160.71.1.el7.x86_64 kernel-tools-libs-3.10.0-1160.71.1.el7.x86_64	python-2.7.5-92.el7_9.x86_64 python-libs-2.7.5-92.el7_9.x86_64 python-perf-3.10.0-1160.71.1.el7.x86_64
--	--

Security vulnerabilities resolved in System Manager 8.1 Security Service Pack Patch #23:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-70554	python python-libs	RHSA-2022:5235	CVE-2020-26116 CVE-2020-26137 CVE-2021-3177	Moderate	N/A	N/A
SMGR-70551	bpftool kernel kernel-tools kernel-tools-libs python-perf	RHSA-2022:5232	CVE-2022-1729 CVE-2022-1966 CVE-2022-32250	Important	ASA-2022-097	High
SMGR-70616	SSP #22 (System_Manager_SSP_R8.1.0.0_Patch22_810014775.bin) installation fails on SMGR 8.1.3.5 secondary server.	N/A	N/A	N/A	N/A	N/A

SSP Patch#22 contains the fixes from the following previous patches:

System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin
System_Manager_SSP_R8.1.0.0_Patch2_810010394.bin
System_Manager_SSP_R8.1.0.0_Patch3_810011047.bin
System_Manager_SSP_R8.1.0.0_Patch4_810011383.bin
System_Manager_SSP_R8.1.0.0_Patch5_810011775.bin
System_Manager_SSP_R8.1.0.0_Patch6_810011933.bin
System_Manager_SSP_R8.1.0.0_Patch7_810012168.bin
System_Manager_SSP_R8.1.0.0_Patch8_810012429.bin
System_Manager_SSP_R8.1.0.0_Patch9_810012552.bin
System_Manager_SSP_R8.1.0.0_Patch10_810012639.bin
System_Manager_SSP_R8.1.0.0_Patch11_810012756.bin
System_Manager_SSP_R8.1.0.0_Patch12_810012960.bin
System_Manager_SSP_R8.1.0.0_Patch13_810013160.bin
System_Manager_SSP_R8.1.0.0_Patch14_810013693.bin
System_Manager_SSP_R8.1.0.0_Patch15_810013886.bin
System_Manager_SSP_R8.1.0.0_Patch16_810014059.bin
System_Manager_SSP_R8.1.0.0_Patch17_810014187.bin
System_Manager_SSP_R8.1.0.0_Patch18_810014282.bin
System_Manager_SSP_R8.1.0.0_Patch19_810014363.bin

System_Manager_SSP_R8.1.0.0_Patch20_810014469.bin
 System_Manager_SSP_R8.1.0.0_Patch21_810014593.bin

Therefore, old SSP patches are removed from PLDS/support site.

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

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

Security vulnerabilities resolved in System Manager 8.1 Security Service Pack Patch #22:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-70244	bpftool kernel kernel-tools kernel-tools-libs python-perf	RHSA-2022:4642	CVE-2022-0492	Important	ASA-2022-087	High
SMGR-70247	rsyslog rsyslog-gnutls	RHSA-2022:4803	CVE-2022-24903	Important	ASA-2022-076	High
SMGR-70250	xz xz-libs	RHSA-2022:5052	CVE-2022-1271	Important	ASA-2022-081	High

SSP Patch#21 contains the fixes from the following previous patches:

System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin
 System_Manager_SSP_R8.1.0.0_Patch2_810010394.bin
 System_Manager_SSP_R8.1.0.0_Patch3_810011047.bin
 System_Manager_SSP_R8.1.0.0_Patch4_810011383.bin
 System_Manager_SSP_R8.1.0.0_Patch5_810011775.bin
 System_Manager_SSP_R8.1.0.0_Patch6_810011933.bin
 System_Manager_SSP_R8.1.0.0_Patch7_810012168.bin
 System_Manager_SSP_R8.1.0.0_Patch8_810012429.bin
 System_Manager_SSP_R8.1.0.0_Patch9_810012552.bin
 System_Manager_SSP_R8.1.0.0_Patch10_810012639.bin
 System_Manager_SSP_R8.1.0.0_Patch11_810012756.bin
 System_Manager_SSP_R8.1.0.0_Patch12_810012960.bin
 System_Manager_SSP_R8.1.0.0_Patch13_810013160.bin
 System_Manager_SSP_R8.1.0.0_Patch14_810013693.bin
 System_Manager_SSP_R8.1.0.0_Patch15_810013886.bin
 System_Manager_SSP_R8.1.0.0_Patch16_810014059.bin
 System_Manager_SSP_R8.1.0.0_Patch17_810014187.bin
 System_Manager_SSP_R8.1.0.0_Patch18_810014282.bin
 System_Manager_SSP_R8.1.0.0_Patch19_810014363.bin
 System_Manager_SSP_R8.1.0.0_Patch20_810014469.bin

Therefore, old SSP patches are removed from PLDS/support site.

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

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

Security vulnerabilities resolved in System Manager 8.1 Security Service Pack Patch #21:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-69729	java-1.8.0-openjdk 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
SMGR-69732	gzip	RHSA-2022:2191	CVE-2022-1271	Important	N/A	N/A
SMGR-69735	zlib	RHSA-2022:2213	CVE-2018-25032	Important	ASA-2022-064	High

SSP Patch#20 contains the fixes from the following previous patches:

System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin
 System_Manager_SSP_R8.1.0.0_Patch2_810010394.bin
 System_Manager_SSP_R8.1.0.0_Patch3_810011047.bin
 System_Manager_SSP_R8.1.0.0_Patch4_810011383.bin
 System_Manager_SSP_R8.1.0.0_Patch5_810011775.bin
 System_Manager_SSP_R8.1.0.0_Patch6_810011933.bin
 System_Manager_SSP_R8.1.0.0_Patch7_810012168.bin
 System_Manager_SSP_R8.1.0.0_Patch8_810012429.bin
 System_Manager_SSP_R8.1.0.0_Patch9_810012552.bin
 System_Manager_SSP_R8.1.0.0_Patch10_810012639.bin
 System_Manager_SSP_R8.1.0.0_Patch11_810012756.bin
 System_Manager_SSP_R8.1.0.0_Patch12_810012960.bin
 System_Manager_SSP_R8.1.0.0_Patch13_810013160.bin
 System_Manager_SSP_R8.1.0.0_Patch14_810013693.bin
 System_Manager_SSP_R8.1.0.0_Patch15_810013886.bin
 System_Manager_SSP_R8.1.0.0_Patch16_810014059.bin
 System_Manager_SSP_R8.1.0.0_Patch17_810014187.bin
 System_Manager_SSP_R8.1.0.0_Patch18_810014282.bin
 System_Manager_SSP_R8.1.0.0_Patch19_810014363.bin

Therefore, old SSP patches are removed from PLDS/support site.

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

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

Security vulnerabilities resolved in System Manager 8.1 Security Service Pack Patch #20:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-69243	kernel kernel-tools kernel-tools-libs bpftool python-perf	RHSA-2022:1198	CVE-2021-4028, CVE-2021-4083	Important	ASA-2022-037	High
SMGR-69240	expat	RHSA-2022:1069	CVE-2022-25235, CVE-2022-25236, CVE-2022-25315, 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	Important	ASA-2022-031	Critical
SMGR-69237	openssl openssl-libs	RHSA-2022:1066	CVE-2022-0778	Important	ASA-2022-036	High

SSP Patch#19 contains the fixes from the following previous patches:

System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin
System_Manager_SSP_R8.1.0.0_Patch2_810010394.bin
System_Manager_SSP_R8.1.0.0_Patch3_810011047.bin
System_Manager_SSP_R8.1.0.0_Patch4_810011383.bin
System_Manager_SSP_R8.1.0.0_Patch5_810011775.bin
System_Manager_SSP_R8.1.0.0_Patch6_810011933.bin
System_Manager_SSP_R8.1.0.0_Patch7_810012168.bin
System_Manager_SSP_R8.1.0.0_Patch8_810012429.bin
System_Manager_SSP_R8.1.0.0_Patch9_810012552.bin
System_Manager_SSP_R8.1.0.0_Patch10_810012639.bin
System_Manager_SSP_R8.1.0.0_Patch11_810012756.bin
System_Manager_SSP_R8.1.0.0_Patch12_810012960.bin
System_Manager_SSP_R8.1.0.0_Patch13_810013160.bin
System_Manager_SSP_R8.1.0.0_Patch14_810013693.bin
System_Manager_SSP_R8.1.0.0_Patch15_810013886.bin
System_Manager_SSP_R8.1.0.0_Patch16_810014059.bin
System_Manager_SSP_R8.1.0.0_Patch17_810014187.bin

System_Manager_SSP_R8.1.0.0_Patch18_810014282.bin

Therefore, old SSP patches are removed from PLDS/support site.

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

kernel-3.10.0-1160.59.1.el7.x86_64	openldap-2.4.44-25.el7_9.x86_64
kernel-tools-3.10.0-1160.59.1.el7.x86_64	cyrus-sasl-2.1.26-24.el7_9.x86_64
kernel-tools-libs-3.10.0-1160.59.1.el7.x86_64	cyrus-sasl-lib-2.1.26-24.el7_9.x86_64
python-perf-3.10.0-1160.59.1.el7.x86_64	cyrus-sasl-plain-2.1.26-24.el7_9.x86_64

Security vulnerabilities resolved in System Manager 8.1 Security Service Pack Patch #19:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-68859	cyrus-sasl cyrus-sasl-lib cyrus-sasl-plain	RHSA-2022:0666	CVE-2022-24407	Important	ASA-2022-027	Critical
SMGR-68856	openldap	RHSA-2022:0621	CVE-2020-25709, CVE-2020-25710	Moderate	ASA-2022-025	High
SMGR-68853	kernel kernel-tools kernel-tools-libs python-perf	RHSA-2022:0620	CVE-2020-0466, CVE-2021-0920, CVE-2021-4155, CVE-2022-0330, CVE-2022-22942, CVE-2020-0465, CVE-2021-3564, CVE-2021-3573, CVE-2021-3752	Important	ASA-2022-026	High

Security Service Packs (SSP) are cumulative. This means that all fixes in previous 8.1.x SSPs are included in the most recent SSP.

SSP Patch#18 contains the fixes from the following previous patches:

System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin
 System_Manager_SSP_R8.1.0.0_Patch2_810010394.bin
 System_Manager_SSP_R8.1.0.0_Patch3_810011047.bin
 System_Manager_SSP_R8.1.0.0_Patch4_810011383.bin
 System_Manager_SSP_R8.1.0.0_Patch5_810011775.bin
 System_Manager_SSP_R8.1.0.0_Patch6_810011933.bin
 System_Manager_SSP_R8.1.0.0_Patch7_810012168.bin
 System_Manager_SSP_R8.1.0.0_Patch8_810012429.bin
 System_Manager_SSP_R8.1.0.0_Patch9_810012552.bin
 System_Manager_SSP_R8.1.0.0_Patch10_810012639.bin
 System_Manager_SSP_R8.1.0.0_Patch11_810012756.bin
 System_Manager_SSP_R8.1.0.0_Patch12_810012960.bin
 System_Manager_SSP_R8.1.0.0_Patch13_810013160.bin
 System_Manager_SSP_R8.1.0.0_Patch14_810013693.bin
 System_Manager_SSP_R8.1.0.0_Patch15_810013886.bin

System_Manager_SSP_R8.1.0.0_Patch16_810014059.bin
 System_Manager_SSP_R8.1.0.0_Patch17_810014187.bin

Therefore, old SSP patches are removed from PLDS/support site.

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

java-1.8.0-openjdk-1:1.8.0.322.b06-1.el7_9.x86_64	aide-0.15.1-13.el7_9.1.x86_64
java-1.8.0-openjdk-devel-1:1.8.0.322.b06-1.el7_9.x86_64	polkit-0.112-26.el7_9.1.x86_64
java-1.8.0-openjdk-headless-1:1.8.0.322.b06-1.el7_9.x86_64	

Security vulnerabilities resolved in System Manager 8.1 Security Service Pack Patch #18:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-68561	java	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	Medium
SMGR-68564	aide	RHSA-2022:0473	CVE-2021-45417	Important	ASA-2022-021	High
SMGR-68558	polkit	RHSA-2022:0274	CVE-2021-4034	Important	ASA-2022-010	High

Security Service Packs (SSP) are cumulative. This means that all fixes in previous 8.1.x SSPs are included in the most recent SSP.

SSP Patch#17 contains the fixes from the following previous patches:

System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin
 System_Manager_SSP_R8.1.0.0_Patch2_810010394.bin
 System_Manager_SSP_R8.1.0.0_Patch3_810011047.bin
 System_Manager_SSP_R8.1.0.0_Patch4_810011383.bin
 System_Manager_SSP_R8.1.0.0_Patch5_810011775.bin
 System_Manager_SSP_R8.1.0.0_Patch6_810011933.bin
 System_Manager_SSP_R8.1.0.0_Patch7_810012168.bin
 System_Manager_SSP_R8.1.0.0_Patch8_810012429.bin
 System_Manager_SSP_R8.1.0.0_Patch9_810012552.bin
 System_Manager_SSP_R8.1.0.0_Patch10_810012639.bin
 System_Manager_SSP_R8.1.0.0_Patch11_810012756.bin

System_Manager_SSP_R8.1.0.0_Patch12_810012960.bin
 System_Manager_SSP_R8.1.0.0_Patch13_810013160.bin
 System_Manager_SSP_R8.1.0.0_Patch14_810013693.bin
 System_Manager_SSP_R8.1.0.0_Patch15_810013886.bin
 System_Manager_SSP_R8.1.0.0_Patch16_810014059.bin

Therefore, old SSP patches are removed from PLDS/support site.

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

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

Security vulnerabilities resolved in System Manager 8.1 Security Service Pack Patch #17:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-67942	bpftool kernel-tools kernel-tools-libs kernel python-perf	RHSA-2022:0063	CVE-2020-25704, CVE-2020-36322, CVE-2021-42739	Moderate	ASA-2022-011	Medium
SMGR-67945	openssl openssl-libs	RHSA-2022:0064	CVE-2021-3712	Moderate	ASA-2022-004	High

Security Service Packs (SSP) are cumulative. This means that all fixes in previous 8.1.x SSPs are included in the most recent SSP.

SSP Patch#16 contains the fixes from the following previous patches:

System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin
 System_Manager_SSP_R8.1.0.0_Patch2_810010394.bin
 System_Manager_SSP_R8.1.0.0_Patch3_810011047.bin
 System_Manager_SSP_R8.1.0.0_Patch4_810011383.bin
 System_Manager_SSP_R8.1.0.0_Patch5_810011775.bin
 System_Manager_SSP_R8.1.0.0_Patch6_810011933.bin
 System_Manager_SSP_R8.1.0.0_Patch7_810012168.bin
 System_Manager_SSP_R8.1.0.0_Patch8_810012429.bin
 System_Manager_SSP_R8.1.0.0_Patch9_810012552.bin
 System_Manager_SSP_R8.1.0.0_Patch10_810012639.bin
 System_Manager_SSP_R8.1.0.0_Patch11_810012756.bin
 System_Manager_SSP_R8.1.0.0_Patch12_810012960.bin
 System_Manager_SSP_R8.1.0.0_Patch13_810013160.bin
 System_Manager_SSP_R8.1.0.0_Patch14_810013693.bin
 System_Manager_SSP_R8.1.0.0_Patch15_810013886.bin

Therefore, old SSP patches are removed from PLDS/support site.

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

bpftool-3.10.0-1160.49.1.el7.x86_64 kernel-tools-3.10.0-1160.49.1.el7.x86_64 kernel-tools-libs-3.10.0-1160.49.1.el7.x86_64 kernel-3.10.0-1160.49.1.el7.x86_64 python-perf-3.10.0-1160.49.1.el7.x86_64 openssh-7.4p1-22.el7_9.x86_64 openssh-askpass-7.4p1-22.el7_9.x86_64 openssh-clients-7.4p1-22.el7_9.x86_64 openssh-server-7.4p1-22.el7_9.x86_64	rpm-4.11.3-48.el7_9.x86_64 rpm-build-libs-4.11.3-48.el7_9.x86_64 rpm-libs-4.11.3-48.el7_9.x86_64 rpm-python-4.11.3-48.el7_9.x86_64 krb5-libs-1.15.1-51.el7_9.i686 nss-3.67.0-4.el7_9.x86_64 nss-sysinit-3.67.0-4.el7_9.x86_64 nss-tools-3.67.0-4.el7_9.x86_64
--	--

Security vulnerabilities resolved in System Manager 8.1 Security Service Pack Patch #16:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-67694	nss nss-sysinit nss-tools	RHSA-2021:4904	CVE-2021-43527	Critical	ASA-2021-184	Critical
SMGR-67691	krb5	RHSA-2021:4788	CVE-2021-37750	Moderate	ASA-2021-179	Medium
SMGR-67688	rpm rpm-build-libs rpm-libs rpm-python	RHSA-2021:4785	CVE-2021-20271	Moderate	ASA-2021-180	Medium
SMGR-67685	openssh- openssh-askpass openssh-clients openssh-server	RHSA-2021:4782	CVE-2021-41617	Moderate	ASA-2021-183	Medium
SMGR-67682	bpftool kernel-tools kernel-tools-libs kernel python-perf	RHSA-2021:4777	CVE-2020-36385	Important	ASA-2021-182	High

Security Service Packs (SSP) are cumulative. This means that all fixes in previous 8.1.x SSPs are included in the most recent SSP.

SSP Patch#15 contains the fixes from the following previous patches:

System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin
System_Manager_SSP_R8.1.0.0_Patch2_810010394.bin
System_Manager_SSP_R8.1.0.0_Patch3_810011047.bin
System_Manager_SSP_R8.1.0.0_Patch4_810011383.bin

System_Manager_SSP_R8.1.0.0_Patch5_810011775.bin
 System_Manager_SSP_R8.1.0.0_Patch6_810011933.bin
 System_Manager_SSP_R8.1.0.0_Patch7_810012168.bin
 System_Manager_SSP_R8.1.0.0_Patch8_810012429.bin
 System_Manager_SSP_R8.1.0.0_Patch9_810012552.bin
 System_Manager_SSP_R8.1.0.0_Patch10_810012639.bin
 System_Manager_SSP_R8.1.0.0_Patch11_810012756.bin
 System_Manager_SSP_R8.1.0.0_Patch12_810012960.bin
 System_Manager_SSP_R8.1.0.0_Patch13_810013160.bin
 System_Manager_SSP_R8.1.0.0_Patch14_810013693.bin

Therefore, old SSP patches are removed from PLDS/support site.

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

kernel-3.10.0-1160.45.1.el7.x86_64.rpm	java-1.8.0-openjdk-1.8.0.312.b07-1.el7_9.x86_64.rpm
kernel-tools-3.10.0-1160.45.1.el7.x86_64.rpm	java-1.8.0-openjdk-debuginfo-1.8.0.312.b07-1.el7_9.x86_64.rpm
kernel-tools-libs-3.10.0-1160.45.1.el7.x86_64.rpm	java-1.8.0-openjdk-devel-1.8.0.312.b07-1.el7_9.x86_64.rpm
openssl-1.0.2k-22.el7_9.x86_64.rpm	java-1.8.0-openjdk-headless-1.8.0.312.b07-1.el7_9.x86_64.rpm
openssl-libs-1.0.2k-22.el7_9.i686.rpm	binutils-2.27-44.base.el7_9.1.x86_64.rpm
openssl-libs-1.0.2k-22.el7_9.x86_64.rpm	
libxml2-2.9.1-6.el7_9.6.x86_64.rpm	

Security vulnerabilities resolved in System Manager 8.1 Security Service Pack Patch #15:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-67272	binutils	RHSA-2021:4033	CVE-2021-42574	Moderate	ASA-2021-128	High
SMGR-67269	java	RHSA-2021:3889	CVE-2021-35565 CVE-2021-35567 CVE-2021-35550 CVE-2021-35556 CVE-2021-35559 CVE-2021-35561 CVE-2021-35564 CVE-2021-35578 CVE-2021-35586 CVE-2021-35588 CVE-2021-35603	Important	ASA-2021-124	Medium
SMGR-67266	libxml2	RHSA-2021:3810	CVE-2016-4658	Moderate	ASA-2021-129	Medium
SMGR-67263	kernel	RHSA-2021:3801	CVE-2021-22543 CVE-2021-37576 CVE-2021-3653 CVE-2021-3656	Important	ASA-2021-118	High
SMGR-67260	Openssl	RHSA-2021:3798	CVE-2021-23841 CVE-2021-23840	Moderate	ASA-2021-120	High

Security Service Packs (SSP) are cumulative. This means that all fixes in previous 8.1.x SSPs are included in the most recent SSP.

SSP Patch#14 contains the fixes from the following previous patches:

System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin
 System_Manager_SSP_R8.1.0.0_Patch2_810010394.bin
 System_Manager_SSP_R8.1.0.0_Patch3_810011047.bin
 System_Manager_SSP_R8.1.0.0_Patch4_810011383.bin
 System_Manager_SSP_R8.1.0.0_Patch5_810011775.bin
 System_Manager_SSP_R8.1.0.0_Patch6_810011933.bin
 System_Manager_SSP_R8.1.0.0_Patch7_810012168.bin
 System_Manager_SSP_R8.1.0.0_Patch8_810012429.bin
 System_Manager_SSP_R8.1.0.0_Patch9_810012552.bin
 System_Manager_SSP_R8.1.0.0_Patch10_810012639.bin
 System_Manager_SSP_R8.1.0.0_Patch11_810012756.bin
 System_Manager_SSP_R8.1.0.0_Patch12_810012960.bin
 System_Manager_SSP_R8.1.0.0_Patch13_810013160.bin

Therefore, old SSP patches are removed from PLDS/support site.

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

sssd-client-1.16.5-10.el7_9.10.x86_64.rpm libX11-1.6.7-4.el7_9.x86_64.rpm libX11-common-1.6.7-4.el7_9.noarch.rpm kernel-3.10.0-1160.42.2.el7.x86_64.rpm kernel-tools-3.10.0-1160.42.2.el7.x86_64.rpm kernel-tools-libs-3.10.0-1160.42.2.el7.x86_64.rpm libsss_idmap-1.16.5-10.el7_9.10.x86_64.rpm libsss_nss_idmap-1.16.5-10.el7_9.10.x86_64.rpm	python-perf-3.10.0-1160.42.2.el7.x86_64.rpm bpftool-3.10.0-1160.42.2.el7.x86_64.rpm libxml2-2.9.1-6.el7.5.x86_64.rpm bind-export-libs-9.11.4-26.P2.el7_9.7.x86_64.rpm bind-libs-9.11.4-26.P2.el7_9.7.x86_64.rpm bind-libs-lite-9.11.4-26.P2.el7_9.7.x86_64.rpm bind-license-9.11.4-26.P2.el7_9.7.noarch.rpm bind-utils-9.11.4-26.P2.el7_9.7.x86_64.rpm
---	---

Security vulnerabilities resolved in System Manager 8.1 Security Service Pack Patch #14:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-66896	kernel python perf bpftool	RHSA-2021:3438	CVE-2021-3715	Moderate	ASA-2021-113	High
SMGR-66916	kernel python perf bpftool	RHSA-2021:3327	CVE-2020-27777 CVE-2021-22555 CVE-2021-29154 CVE-2021-29650 CVE-2021-32399	Important	ASA-2021-110	High
SMGR-66892	libx11	RHSA-2021:3296	CVE-2021-31535	Important	ASA-2021-114	High

SMGR-66888	sssd	RHSA-2021:3336	CVE-2021-3621	Important	ASA-2021-111	Medium
SMGR-66894	Libxml2	RHSA-2020:3996	CVE-2019-19956 CVE-2019-20388 CVE-2020-7595	Moderate	ASA-2020-122	High
SMGR-66898	bind	RHSA-2021:3325	CVE-2021-25214	Moderate	ASA-2021-122	Medium

Security Service Packs (SSP) are cumulative. This means that all fixes in previous 8.1.x SSPs are included in the most recent SSP.

SSP Patch#13 contains the fixes from the following previous patches:

System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin
 System_Manager_SSP_R8.1.0.0_Patch2_810010394.bin
 System_Manager_SSP_R8.1.0.0_Patch3_810011047.bin
 System_Manager_SSP_R8.1.0.0_Patch4_810011383.bin
 System_Manager_SSP_R8.1.0.0_Patch5_810011775.bin
 System_Manager_SSP_R8.1.0.0_Patch6_810011933.bin
 System_Manager_SSP_R8.1.0.0_Patch7_810012168.bin
 System_Manager_SSP_R8.1.0.0_Patch8_810012429.bin
 System_Manager_SSP_R8.1.0.0_Patch9_810012552.bin
 System_Manager_SSP_R8.1.0.0_Patch10_810012639.bin
 System_Manager_SSP_R8.1.0.0_Patch11_810012756.bin
 System_Manager_SSP_R8.1.0.0_Patch12_810012960.bin

Therefore, old SSP patches are removed from PLDS/support site.

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

kernel-3.10.0-1160.36.2.el7.x86_64 kernel-tools-3.10.0-1160.36.2.el7.x86_64 kernel-tools-libs-3.10.0-1160.36.2.el7.x86_64 python-perf-3.10.0-1160.36.2.el7.x86_64 bpftool-3.10.0-1160.36.2.el7.x86_64	java-1.8.0-openjdk-headless-1.8.0.302.b08-0.el7_9.x86_64 java-1.8.0-openjdk-devel-1.8.0.302.b08-0.el7_9.x86_64 java-1.8.0-openjdk-debuginfo-1.8.0.302.b08-0.el7_9.x86_64 java-1.8.0-openjdk-1.8.0.302.b08-0.el7_9.x86_64
---	---

Security vulnerabilities resolved in System Manager 8.1 Security Service Pack Patch #13:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-61603	kernel python bpftool	RHSA-2021:2725	CVE-2019-20934 CVE-2020-11668 CVE-2021-33033 CVE-2021-33034 CVE-2021-33909	Important	ASA-2021-103	High
SMGR-61605	Java	RHSA-2021:2845	CVE-2021-2341 CVE-2021-2369 CVE-2021-2388	Important	ASA-2021-095	High

Security Service Packs (SSP) are cumulative. This means that all fixes in previous 8.1.x SSPs are included in the most recent SSP.

SSP Patch#12 contains the fixes from the following previous patches:

System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin
 System_Manager_SSP_R8.1.0.0_Patch2_810010394.bin
 System_Manager_SSP_R8.1.0.0_Patch3_810011047.bin
 System_Manager_SSP_R8.1.0.0_Patch4_810011383.bin
 System_Manager_SSP_R8.1.0.0_Patch5_810011775.bin
 System_Manager_SSP_R8.1.0.0_Patch6_810011933.bin
 System_Manager_SSP_R8.1.0.0_Patch7_810012168.bin
 System_Manager_SSP_R8.1.0.0_Patch8_810012429.bin
 System_Manager_SSP_R8.1.0.0_Patch9_810012552.bin
 System_Manager_SSP_R8.1.0.0_Patch10_810012639.bin
 System_Manager_SSP_R8.1.0.0_Patch11_810012756.bin

Therefore, old SSP patches are removed from PLDS/support site.

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

kernel-3.10.0-1160.31.1.el7.x86_64 kernel-tools-3.10.0-1160.31.1.el7.x86_64 kernel-tools-libs-3.10.0-1160.31.1.el7.x86_64 python-perf-3.10.0-1160.31.1.el7.x86_64 bpftool-3.10.0-1160.31.1.el7.x86_64	dhclient-12:4.2.5-83.el7_9.1.x86_64 dhcp-common-12:4.2.5-83.el7_9.1.x86_64 dhcp-libs-12:4.2.5-83.el7_9.1.x86_64 microcode_ctl-2:2.1-73.9.el7_9.x86_64
---	--

Security vulnerabilities resolved in System Manager 8.1 Security Service Pack Patch #12:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-60965	microcode_ctl	RHSA-2021:2305	CVE-2020-24489 CVE-2020-24511 CVE-2020-24512 CVE-2020-24513	Important	ASA-2021-079	High
SMGR-60963	kernel python bpftool	RHSA-2021:2314	CVE-2020-12362 CVE-2021-3347 CVE-2020-8648 CVE-2020-12363 CVE-2020-12364 CVE-2020-27170	Important	ASA-2021-083	High
SMGR-60961	dhcp	RHSA-2021:2357	CVE-2021-25217	Important	ASA-2021-085	High

Security Service Packs (SSP) are cumulative. This means that all fixes in previous 8.1.x SSPs are included in the most recent SSP.

SSP Patch#11 contains the fixes from the following previous patches:

System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin
 System_Manager_SSP_R8.1.0.0_Patch2_810010394.bin
 System_Manager_SSP_R8.1.0.0_Patch3_810011047.bin
 System_Manager_SSP_R8.1.0.0_Patch4_810011383.bin
 System_Manager_SSP_R8.1.0.0_Patch5_810011775.bin
 System_Manager_SSP_R8.1.0.0_Patch6_810011933.bin
 System_Manager_SSP_R8.1.0.0_Patch7_810012168.bin
 System_Manager_SSP_R8.1.0.0_Patch8_810012429.bin
 System_Manager_SSP_R8.1.0.0_Patch9_810012552.bin
 System_Manager_SSP_R8.1.0.0_Patch10_810012639.bin

Therefore, old SSP patches are removed from PLDS/support site.

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

glib2-2.56.1-9.el7_9.x86_64.rpm	
---------------------------------	--

Security vulnerabilities resolved in System Manager 8.1 Security Service Pack Patch #11:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-60504	glib2	RHSA-2021:2147	CVE-2021-27219	Important	ASA-2021-072	Critical

Security Service Packs (SSP) are cumulative. This means that all fixes in previous 8.1.x SSPs are included in the most recent SSP.

SSP Patch#10 contains the fixes from the following previous patches:

System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin
 System_Manager_SSP_R8.1.0.0_Patch2_810010394.bin
 System_Manager_SSP_R8.1.0.0_Patch3_810011047.bin
 System_Manager_SSP_R8.1.0.0_Patch4_810011383.bin
 System_Manager_SSP_R8.1.0.0_Patch5_810011775.bin
 System_Manager_SSP_R8.1.0.0_Patch6_810011933.bin
 System_Manager_SSP_R8.1.0.0_Patch7_810012168.bin
 System_Manager_SSP_R8.1.0.0_Patch8_810012429.bin
 System_Manager_SSP_R8.1.0.0_Patch9_810012552.bin

Therefore, old SSP patches are removed from PLDS/support site.

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

libxml2-2.9.1-6.el7.5.x86_64.rpm	java-1.8.0-openjdk-1.8.0.292.b10-1.el7_9.x86_64.rpm
----------------------------------	---

openldap-2.4.44-23.el7_9.x86_64.rpm nss-3.53.1-7.el7_9.x86_64.rpm nss-softokn-3.53.1-6.el7_9.x86_64.rpm nss-softokn-freebl-3.53.1-6.el7_9.i686.rpm nss-softokn-freebl-3.53.1-6.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 nss-util-3.53.1-1.el7_9.x86_64.rpm	java-1.8.0-openjdk-debuginfo-1.8.0.292.b10-1.el7_9.x86_64.rpm java-1.8.0-openjdk-devel-1.8.0.292.b10-1.el7_9.x86_64.rpm java-1.8.0-openjdk-headless-1.8.0.292.b10-1.el7_9.x86_64.rpm bind-export-libs-9.11.4-26.P2.el7_9.5.x86_64.rpm bind-libs-9.11.4-26.P2.el7_9.5.x86_64.rpm bind-libs-lite-9.11.4-26.P2.el7_9.5.x86_64.rpm bind-license-9.11.4-26.P2.el7_9.5.noarch.rpm bind-utils-9.11.4-26.P2.el7_9.5.x86_64.rpm
---	---

Security vulnerabilities resolved in System Manager 8.1 Security Service Pack Patch #10:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-60253	libxml2	RHSA-2020:3996	CVE-2019-19956, CVE-2019-20388, CVE-2020-7595	Moderate	ASA-2020-122	High
SMGR-60245	openldap	RHSA-2021:1389	CVE-2020-25692	Moderate	ASA-2021-042	High
SMGR-60242	nss nss-softokn nss-softokn-freebl nss-sysinit nss-tools nss-util	RHSA-2021:1384	CVE-2020-25648	Moderate	ASA-2021-035	High
SMGR-60236	bind-export-libs bind-libs bind-libs-lite bind-license bind-utils	RHSA-2021:1469	CVE-2021-25215	Important	ASA-2021-037	High
SMGR-60239	java-1.8.0-openjdk java-1.8.0-openjdk-debuginfo java-1.8.0-openjdk-devel java-1.8.0-openjdk-headless	RHSA-2021:1298	CVE-2021-2163	Moderate	ASA-2021-034	Medium

Security Service Packs (SSP) are cumulative. This means that all fixes in previous 8.1.x SSPs are included in the most recent SSP.

SSP Patch#9 contains the fixes from the following previous patches:

System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin

System_Manager_SSP_R8.1.0.0_Patch2_810010394.bin
 System_Manager_SSP_R8.1.0.0_Patch3_810011047.bin
 System_Manager_SSP_R8.1.0.0_Patch4_810011383.bin
 System_Manager_SSP_R8.1.0.0_Patch5_810011775.bin
 System_Manager_SSP_R8.1.0.0_Patch6_810011933.bin
 System_Manager_SSP_R8.1.0.0_Patch7_810012168.bin
 System_Manager_SSP_R8.1.0.0_Patch8_810012429.bin

Therefore, old SSP patches are removed from PLDS/support site.

Note – On 04- June 2021, System Manager 8.1 SSP #8 and #9 have been removed from Avaya Support Site/PLDS. Please refer PSN005561u for more details.

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

nettle-2.7.1-9.el7_9.x86_64.rpm 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	python-perf-3.10.0-1160.24.1.el7.x86_64.rpm wpa_supplicant-2.6-12.el7_9.2.x86_64.rpm net-snmp-5.7.3-3.smgr.el7.x86_64.rpm bpftool-3.10.0-1160.24.1.el7.x86_64.rpm
--	--

Security vulnerabilities resolved in System Manager 8.1 Security Service Pack Patch #9:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-59861	Nettle	RHSA-2021:1145	CVE-2021-20305	Important	ASA-2021-028	High
SMGR-59883	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
SMGR-59886	wpa_supplicant	RHSA-2021:0808	CVE-2021-27803	Important	ASA-2021-022	High
SMGR-59851	net-snmp	RHSA-2020:5350	CVE-2020-15862	Important	ASA-2020-205	High

Security Service Packs (SSP) are cumulative. This means that all fixes in previous 8.1.x SSPs are included in the most recent SSP.

SSP Patch#8 contains the fixes from the following previous patches:

System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin
 System_Manager_SSP_R8.1.0.0_Patch2_810010394.bin
 System_Manager_SSP_R8.1.0.0_Patch3_810011047.bin

System_Manager_SSP_R8.1.0.0_Patch4_810011383.bin
 System_Manager_SSP_R8.1.0.0_Patch5_810011775.bin
 System_Manager_SSP_R8.1.0.0_Patch6_810011933.bin
 System_Manager_SSP_R8.1.0.0_Patch7_810012168.bin

Therefore, old SSP patches are removed from PLDS/support site.

Security vulnerabilities resolved in System Manager 8.1 Security Service Pack Patch #8:

Fix ID	RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-59545	RHSA-2021:0336	Moderate	N/A	N/A
SMGR-59536	RHSA-2021:0348	Moderate	ASA-2021-014	High
SMGR-59535	RHSA-2021:0671	Important	N/A	N/A
SMGR-59534	RHSA-2021:0699	Moderate	ASA-2021-019	High
SMGR-59323	RHSA-2021:0343	Moderate	ASA-2021-013	High
SMGR-59285	RHSA-2021:0339	Important	ASA-2021-011	High
SMGR-59192	RHSA-2021:0221	Important	ASA-2021-009	High
SMGR-59318	nmap license remediation	Bug Fix Advisory	N/A	N/A

Security Service Packs (SSP) are cumulative. This means that all fixes in previous 8.1.x SSPs are included in the most recent SSP.

SSP Patch#7 contains the fixes from the following previous patches:

System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin
 System_Manager_SSP_R8.1.0.0_Patch2_810010394.bin
 System_Manager_SSP_R8.1.0.0_Patch3_810011047.bin
 System_Manager_SSP_R8.1.0.0_Patch4_810011383.bin
 System_Manager_SSP_R8.1.0.0_Patch5_810011775.bin
 System_Manager_SSP_R8.1.0.0_Patch6_810011933.bin

Therefore, old SSP patches are removed from PLDS/support site.

As noted in the Description section of 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.

Security vulnerabilities resolved in System Manager 8.1 Security Service Pack Patch #7:

Fix ID	RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-58810	RHSA-2020:5083	Moderate	ASA-2020-193	Medium
SMGR-58814	RHSA-2020:5023	Moderate	ASA-2020-186	Medium
SMGR-58802	RHSA-2020:5002	Moderate	ASA-2020-192	Medium
SMGR-58812	RHSA-2020:5437	Important	N/A	N/A
SMGR-58808	RHSA-2020:5011	Moderate	ASA-2020-203	High
SMGR-58806	RHSA-2020:5566	Important	ASA-2021-001	Medium
SMGR-58804	RHSA-2020:5009	Moderate	N/A	N/A

Security Service Packs (SSP) are cumulative. This means that all fixes in previous 8.1.x SSPs are included in the most recent SSP.

SSP Patch#6 contains the fixes from the following previous patches:

System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin
 System_Manager_SSP_R8.1.0.0_Patch2_810010394.bin
 System_Manager_SSP_R8.1.0.0_Patch3_810011047.bin
 System_Manager_SSP_R8.1.0.0_Patch4_810011383.bin
 System_Manager_SSP_R8.1.0.0_Patch5_810011775.bin

Therefore, old SSP patches are removed from PLDS/support site.

As noted in the Description section of 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.

Security vulnerabilities resolved in System Manager 8.1 Security Service Pack Patch #6:

Fix ID	RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-58058	RHSA-2020:3996	High	ASA-2020-122	High
SMGR-58054	RHSA-2020:4005	High	ASA-2020-138	High
SMGR-58050	RHSA-2020:4011	High	ASA-2020-133	High
SMGR-58046	RHSA-2020:4032	High	ASA-2020-136	High
SMGR-58044	RHSA-2020:4041	High	ASA-2020-121	High
SMGR-58042	RHSA-2020:4060	High	ASA-2020-140	High
SMGR-58040	RHSA-2020:4072	High	ASA-2020-131	High
SMGR-58038	RHSA-2020:4076	High	ASA-2020-119	High
SMGR-58036	RHSA-2020:4276	High	ASA-2020-146	High
SMGR-58074	RHSA-2020:3864	Medium	ASA-2020-129	Medium
SMGR-58070	RHSA-2020:3908	Medium	ASA-2020-120	Medium
SMGR-58068	RHSA-2020:3911	Medium	ASA-2020-134	Medium
SMGR-58066	RHSA-2020:3915	Medium	ASA-2020-135	Medium
SMGR-58064	RHSA-2020:3916	Medium	ASA-2020-132	Medium
SMGR-58062	RHSA-2020:3952	Medium	ASA-2020-116	Medium
SMGR-58060	RHSA-2020:3978	Medium	ASA-2020-125	Medium
SMGR-58048	RHSA-2020:4026	Medium	ASA-2020-112	Medium
SMGR-58056	RHSA-2020:4003	Medium	ASA-2020-127	Medium
SMGR-58072	RHSA-2020:3901	Low	ASA-2020-130	Low
SMGR-58052	RHSA-2020:4007	Low	ASA-2020-128	Low
SMGR-58078	RHSA-2020:3848	Low	ASA-2020-137	Low
SMGR-58076	RHSA-2020:3861	Low	ASA-2020-124	Low
SMGR-58034	RHSA-2020:4350	Bug Fix Advisory	N/A	N/A
SMGR-58032	RHSA-2020:4907	Bug Fix Advisory	N/A	N/A
SMGR-58030	RHSA-2020:4908	Bug Fix Advisory	N/A	N/A

Security Service Packs (SSP) are cumulative. This means that all fixes in previous 8.1.x SSPs are included in the most recent SSP.

SSP Patch#5 contains the fixes from the following previous patches:

System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin
 System_Manager_SSP_R8.1.0.0_Patch2_810010394.bin
 System_Manager_SSP_R8.1.0.0_Patch3_810011047.bin
 System_Manager_SSP_R8.1.0.0_Patch4_810011383.bin

Therefore, old SSP patches are removed from PLDS/support site.

Security vulnerabilities resolved in System Manager 8.1 Security Service Pack Patch #5:

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2020:2337	High	ASA-2020-080	High
RHSA-2020:2344	High	ASA-2020-079	High
RHSA-2020:3217	High	ASA-2020-102	High
RHSA-2020:2968	High	ASA-2020-098	High
RHSA-2020:3220	High	ASA-2020-103	High
RHSA-2020:2663	High	ASA-2020-090	High
RHSA-2020:2894	Medium	ASA-2020-092	Medium
RHSA-2020:2432	Medium	ASA-2020-083	Medium
RHSA-2020:2664	Medium	ASA-2020-089	Medium

Security Service Packs (SSP) are cumulative. This means that all fixes in previous 8.1.x SSPs are included in the most recent SSP.

SSP Patch#4 contains the fixes from the following previous patches:

System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin
 System_Manager_SSP_R8.1.0.0_Patch2_810010394.bin
 System_Manager_SSP_R8.1.0.0_Patch3_810011047.bin

Therefore, old SSP patches are removed from PLDS/support site.

Security vulnerabilities resolved in System Manager 8.1 Security Service Pack Patch #4:

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2020:1000	High	ASA-2020-041	High
RHSA-2020:1050	High	ASA-2020-042	High
RHSA-2020:1080	High	ASA-2020-034	High
RHSA-2020:0834	High	ASA-2020-026	High
RHSA-2020:0897	High	ASA-2020-031	High
RHSA-2020:1333	High	ASA-2020-053	High
RHSA-2020:1016	High	ASA-2020-036	High
RHSA-2020:1190	High	ASA-2020-050	High
RHSA-2020:0568	High	ASA-2020-025	High
RHSA-2020:0124	High	ASA-2020-004	High
RHSA-2020:1511	High	ASA-2020-067	High
RHSA-2020:1131	High	ASA-2020-038	High
RHSA-2020:1061	High	ASA-2020-059	High
RHSA-2020:1081	High	ASA-2020-056	High

RHSA-2020:1512	High	ASA-2020-071	High
RHSA-2020:1135	Medium	ASA-2020-051	Medium
RHSA-2020:1020	Medium	ASA-2020-040	Medium
RHSA-2020:1047	Medium	ASA-2020-044	Medium
RHSA-2020:1021	Medium	ASA-2020-033	Medium
RHSA-2020:1100	Medium	ASA-2020-032	Medium
RHSA-2020:1176	Medium	ASA-2020-049	Medium
RHSA-2020:1022	Medium	ASA-2020-043	Medium
RHSA-2020:1011	Medium	ASA-2020-037	Medium
RHSA-2020:1138	Medium	ASA-2020-057	Medium
RHSA-2020:1113	Medium	ASA-2020-061	Medium
RHSA-2020:1181	Low	ASA-2020-055	Low
RHSA-2020:2082	Bug Fix Advisory	N/A	N/A

Security Service Packs (SSP) are cumulative. This means that all fixes in previous 8.1.x SSPs are included in the most recent SSP.

SSP Patch#3 contains the fixes from the following previous patches:

System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin
System_Manager_SSP_R8.1.0.0_Patch2_810010394.bin

Therefore, old SSP patches are removed from PLDS/support site.

Security vulnerabilities resolved in System Manager 8.1 Security Service Pack Patch #3:

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2019:3055	High	ASA-2019-228	High
RHSA-2019:4190	High	ASA-2019-247	High
RHSA-2019:4326	High	ASA-2019-251	High
RHSA-2019:3872	High	ASA-2019-241	High
RHSA-2019:4190	High	ASA-2019-247	High
RHSA-2019:3979	High	ASA-2019-245	High
RHSA-2019:3128	Medium	ASA-2019-230	Medium
RHSA-2019:3976	Medium	ASA-2019-248	Medium
RHSA-2019:3834	Medium	ASA-2019-237	Medium

Security Service Packs (SSP) are cumulative. This means that all fixes in previous 8.1.x SSPs are included in the most recent SSP.

SSP Patch#2 contains the fixes from the following previous patches:

System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin

Therefore, old SSP patch removed from PLDS/support site.

Security vulnerabilities resolved in System Manager 8.1 Security Service Pack Patch #2:

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
--------------------	----------------------	-------------------	-----------------------------

RHSA-2019:2571	Critical	ASA-2019-218	Critical
RHSA-2019:2077	High	ASA-2019-189	High
RHSA-2019:2046	High	ASA-2019-152	High
RHSA-2019:2052	High	ASA-2019-216	High
RHSA-2019:1228	High	ASA-2019-106	High
RHSA-2019:2075	High	ASA-2019-188	High
RHSA-2019:2053	High	ASA-2019-217	High
RHSA-2019:2030	High	ASA-2019-191	High
RHSA-2019:2029	High	ASA-2019-208	High
RHSA-2019:2028	High	ASA-2019-206	High
RHSA-2019:2057	Medium	ASA-2019-202	Medium
RHSA-2019:2197	Medium	ASA-2019-154	Medium
RHSA-2019:2189	Medium	ASA-2019-158	Medium
RHSA-2019:2136	Medium	ASA-2019-185	Medium
RHSA-2019:2047	Medium	ASA-2019-147	Medium
RHSA-2019:1815	Medium	ASA-2019-130	Medium
RHSA-2019:2091	Medium	ASA-2019-203	Medium
RHSA-2019:2143	Medium	ASA-2019-204	Medium
RHSA-2019:2079	Medium	ASA-2019-175	Medium
RHSA-2019:2049	Medium	ASA-2019-169	Medium
RHSA-2019:2327	Medium	ASA-2019-155	Medium
RHSA-2019:1619	Medium	ASA-2019-121	Medium
RHSA-2019:2110	Medium	ASA-2019-211	Medium
RHSA-2019:2118	Medium	ASA-2019-192	Medium
RHSA-2019:2177	Medium	ASA-2019-209	Medium
RHSA-2019:2060	Medium	ASA-2019-194	Medium
RHSA-2019:2304	Medium	ASA-2019-193	Medium
RHSA-2019:2237	Medium	ASA-2019-205	Medium
RHSA-2019:2181	Low	ASA-2019-183	Low
RHSA-2019:2159	Low	ASA-2019-198	Low

Security vulnerabilities resolved in System Manager 8.1 Security Service Pack Patch #1:

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2019:1481	High	ASA-2019-109	High
RHSA-2019:1228	High	ASA-2019-106	High
RHSA-2019:1294	High	ASA-2019-100	High
RHSA-2019:1235	High	ASA-2019-107	High
RHSA-2019:1619	Medium	ASA-2019-121	Medium
RHSA-2019:1587	Critical	ASA-2019-120	Critical

Mitigation: N/A**SECTION 1C – ENTITLEMENTS AND CONTACTS**

**Material
Coverage
Entitlements:**

This PCN is being offered at no charge to the customer with valid support / upgrade contracts. 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](#).