

Product Correction Notice (PCN)

Issue Date: April 18, 2022
 Supplement Date: Nov 10, 2025
 Expiration Date: NA
 PCN Number: 2138S

SECTION 1 - CUSTOMER NOTICE

Products affected by this PCN: Avaya Aura® System Manager, Release 10.1.x vAppliance running on Avaya provided servers: Avaya Solutions Platform 130 R5.x (Dell® PowerEdge R640).
 Avaya Aura® System Manager 10.1 vAppliance running on customer provided VMware® certified hardware.
 Reference the Avaya Aura® Platform Offer Definition for details.

Description: **Effective 01-January-2026 Avaya will no longer provide Manufacturer Support for Avaya Aura® Platform Release 10.1 as noted in the [Product Lifecycle Notice](#). Avaya is providing SMGR 10.1.3.7 as a final Service Pack and SMGR SSP37 as a final Security Service Pack on top of the 10.1.x release.**

IMPORTANT NOTES –

- Starting with System Manager release 10.1.3.4, SSP's will no longer be bundled within the Feature Pack/Service Pack release. They will only be provided separately and must be installed separately independent of the Feature Pack / Service Pack.
- Approximately 4 weeks prior to GA, new SSPs are built and pick up all RHSA fixes that are available from Red Hat at that point in time. New RHSAs/updated packages available from Red Hat after that point in time will be included in the next SSP.
- In order to maintain code stability and compatibility, Red Hat typically does not rebase packages to older versions. Instead, they backport fixes to older versions. This can result in security scanners that only consider the Red Hat version to report vulnerabilities that are false positives. See **Section 1B** of this PCN for additional information.
- Installing Security Service Pack SSP32 and later, on System Manager Releases 10.1.3.1 to 10.1.3.3, Please refer to the **Finding the Installation Instructions** section.

10-Nov-2025 – Supplement 36 – Supplement 36 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #37 (AV-SMGR10.1-RHEL8.4-SSP-037-01.tar.bz2; PLDS ID SMGR101SSP37)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) or 10.1.x Feature Pack (10.1.2.0 or 10.1.3.0) or 10.1.3.1 or 10.1.3.2 or 10.1.3.3 or 10.1.3.4 or 10.1.3.5 or 10.1.3.6 or 10.1.3.7 release installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This

- patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #37 is applicable to System Manager 10.1.x release.
- 10.1 SSPs will not work on the 10.2 release and there will be different SSPs for both 10.1 and 10.2.
- Reference the “*Finding the installation instructions*” section of this PCN for detailed installation instructions.
- Reference the “*Security Information*” section of this PCN for updates to the rpm and RHSAs for SSP #37.

System Manager feature packs and service packs have SSP's bundled with it (see table below for details on which SSP is bundled with which feature pack/service pack of SMGR).

If running on System Manager release 10.1.0.1 with a 10.1.0.1 hot fix installed or release 10.1.0.2 with a 10.1.0.2 hot fix installed and you are trying to upgrade to 10.1.0.2 (scenario only applies when on 10.1.0.1 +hotfix) or 10.1.2.0, then the SSP bundled along with 10.1.0.2 or 10.1.2.0 will not get installed as part of the feature pack/service pack installation. In such cases one can:

- Install either the same or higher version of the SSP manually on the system.
- Upgrade to 10.1.3.0 or higher version of System Manager which fixes the issue.

Below table provides the default SSP release bundled with the Feature Pack/Service Pack release.

Feature Pack/Service Pack Release	SSP Bundled
10.1 GA	No
10.1.0.1	SSP01 (System_Manager_10.1.0.1_r1010114394.bin)
10.1.0.2	SSP05 (AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2)
10.1.2.0	SSP09 (AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2)
10.1.3.0	SSP13 (AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2)
10.1.3.1	SSP16 (AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2)
10.1.3.2	SSP 21 (AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2)
10.1.3.3	SSP 24 (AV-SMGR10.1-RHEL8.4-SSP-024-02.tar.bz2)
10.1.3.4 or later release	No

13-Oct-2025 – Supplement 35 – Supplement 35 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #36 (AV-SMGR10.1-RHEL8.4-SSP-036-01.tar.bz2; PLDS ID SMGR101SSP36)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) or 10.1.x Feature Pack (10.1.2.0 or 10.1.3.0) or 10.1.3.1 or 10.1.3.2 or 10.1.3.3 or 10.1.3.4 or 10.1.3.5 or 10.1.3.6 release installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.

- System Manager 10.1 SSP #36 is applicable to System Manager 10.1.x release.
- 10.1 SSPs will not work on the 10.2 release and there will be different SSPs for both 10.1 and 10.2.
- Reference the ***"Finding the installation instructions"*** section of this PCN for detailed installation instructions.
- Reference the ***"Security Information"*** section of this PCN for updates to the rpm and RHSAs for SSP #36.

System Manager feature packs and service packs have SSP's bundled with it (see table below for details on which SSP is bundled with which feature pack/service pack of SMGR).

If running on System Manager release 10.1.0.1 with a 10.1.0.1 hot fix installed or release 10.1.0.2 with a 10.1.0.2 hot fix installed and you are trying to upgrade to 10.1.0.2 (scenario only applies when on 10.1.0.1 +hotfix) or 10.1.2.0, then the SSP bundled along with 10.1.0.2 or 10.1.2.0 will not get installed as part of the feature pack/service pack installation. In such cases one can:

- Install either the same or higher version of the SSP manually on the system.
- Upgrade to 10.1.3.0 or higher version of System Manager which fixes the issue.

Below table provides the default SSP release bundled with the Feature Pack/Service Pack release.

Feature Pack/Service Pack Release	SSP Bundled
10.1 GA	No
10.1.0.1	SSP01 (System_Manager_10.1.0.1_r1010114394.bin)
10.1.0.2	SSP05 (AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2)
10.1.2.0	SSP09 (AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2)
10.1.3.0	SSP13 (AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2)
10.1.3.1	SSP16 (AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2)
10.1.3.2	SSP 21 (AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2)
10.1.3.3	SSP 24 (AV-SMGR10.1-RHEL8.4-SSP-024-02.tar.bz2)
10.1.3.4 or later release	No

08-Sep-2025 – Supplement 34 – Supplement 34 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #35 (AV-SMGR10.1-RHEL8.4-SSP-035-02.tar.bz2; PLDS ID SMGR101SSP35)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) or 10.1.x Feature Pack (10.1.2.0 or 10.1.3.0) or 10.1.3.1 or 10.1.3.2 or 10.1.3.3 or 10.1.3.4 or 10.1.3.5 or 10.1.3.6 release installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.

- System Manager 10.1 SSP #35 is applicable to System Manager 10.1.x release.
- 10.1 SSPs will not work on the 10.2 release and there will be different SSPs for both 10.1 and 10.2.
- Reference the **“Finding the installation instructions”** section of this PCN for detailed installation instructions.
- Reference the **“Security Information”** section of this PCN for updates to the rpm and RHSAs for SSP #35.

System Manager feature packs and service packs have SSP's bundled with it (see table below for details on which SSP is bundled with which feature pack/service pack of SMGR).

If running on System Manager release 10.1.0.1 with a 10.1.0.1 hot fix installed or release 10.1.0.2 with a 10.1.0.2 hot fix installed and you are trying to upgrade to 10.1.0.2 (scenario only applies when on 10.1.0.1 +hotfix) or 10.1.2.0, then the SSP bundled along with 10.1.0.2 or 10.1.2.0 will not get installed as part of the feature pack/service pack installation. In such cases one can:

- Install either the same or higher version of the SSP manually on the system.
- Upgrade to 10.1.3.0 or higher version of System Manager which fixes the issue.

Below table provides the default SSP release bundled with the Feature Pack/Service Pack release.

Feature Pack/Service Pack Release	SSP Bundled
10.1 GA	No
10.1.0.1	SSP01 (System_Manager_10.1.0.1_r1010114394.bin)
10.1.0.2	SSP05 (AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2)
10.1.2.0	SSP09 (AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2)
10.1.3.0	SSP13 (AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2)
10.1.3.1	SSP16 (AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2)
10.1.3.2	SSP 21 (AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2)
10.1.3.3	SSP 24 (AV-SMGR10.1-RHEL8.4-SSP-024-02.tar.bz2)
10.1.3.4 or later release	No

21-July-2025 – Supplement 33 – Supplement 33 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #34 (AV-SMGR10.1-RHEL8.4-SSP-034-01.tar.bz2; PLDS ID SMGR101SSP34)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) or 10.1.x Feature Pack (10.1.2.0 or 10.1.3.0) or 10.1.3.1 or 10.1.3.2 or 10.1.3.3 or 10.1.3.4 or 10.1.3.5 or 10.1.3.6 release installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #34 is applicable to System Manager 10.1.x release.

- 10.1 SSPs will not work on the 10.2 release and there will be different SSPs for both 10.1 and 10.2.
- Reference the ***"Finding the installation instructions"*** section of this PCN for detailed installation instructions.
- Reference the ***"Security Information"*** section of this PCN for updates to the rpm and RHSAs for SSP #34.

System Manager feature packs and service packs have SSP's bundled with it (see table below for details on which SSP is bundled with which feature pack/service pack of SMGR).

If running on System Manager release 10.1.0.1 with a 10.1.0.1 hot fix installed or release 10.1.0.2 with a 10.1.0.2 hot fix installed and you are trying to upgrade to 10.1.0.2 (scenario only applies when on 10.1.0.1 +hotfix) or 10.1.2.0, then the SSP bundled along with 10.1.0.2 or 10.1.2.0 will not get installed as part of the feature pack/service pack installation. In such cases one can:

- Install either the same or higher version of the SSP manually on the system.
- Upgrade to 10.1.3.0 or higher version of System Manager which fixes the issue.

Below table provides the default SSP release bundled with the Feature Pack/Service Pack release.

Feature Pack/Service Pack Release	SSP Bundled
10.1 GA	No
10.1.0.1	SSP01 (System_Manager_10.1.0.1_r1010114394.bin)
10.1.0.2	SSP05 (AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2)
10.1.2.0	SSP09 (AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2)
10.1.3.0	SSP13 (AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2)
10.1.3.1	SSP16 (AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2)
10.1.3.2	SSP 21 (AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2)
10.1.3.3	SSP 24 (AV-SMGR10.1-RHEL8.4-SSP-024-02.tar.bz2)
10.1.3.4 or later release	No

09-June-2025 – Supplement 32 – Supplement 32 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #33 (AV-SMGR10.1-RHEL8.4-SSP-033-05.tar.bz2; PLDS ID SMGR101SSP33)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) or 10.1.x Feature Pack (10.1.2.0 or 10.1.3.0) or 10.1.3.1 or 10.1.3.2 or 10.1.3.3 or 10.1.3.4 or 10.1.3.5 or 10.1.3.6 release installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #33 is applicable to System Manager 10.1.x release.
- 10.1 SSPs will not work on the 10.2 release and there will be different SSPs for both 10.1 and

10.2.

- Reference the **“Finding the installation instructions”** section of this PCN for detailed installation instructions.
- Reference the **“Security Information”** section of this PCN for updates to the rpm and RHSAs for SSP #33.

System Manager feature packs and service packs have SSP's bundled with it (see table below for details on which SSP is bundled with which feature pack/service pack of SMGR).

If running on System Manager release 10.1.0.1 with a 10.1.0.1 hot fix installed or release 10.1.0.2 with a 10.1.0.2 hot fix installed and you are trying to upgrade to 10.1.0.2 (scenario only applies when on 10.1.0.1 +hotfix) or 10.1.2.0, then the SSP bundled along with 10.1.0.2 or 10.1.2.0 will not get installed as part of the feature pack/service pack installation. In such cases one can:

- Install either the same or higher version of the SSP manually on the system.
- Upgrade to 10.1.3.0 or higher version of System Manager which fixes the issue.

Below table provides the default SSP release bundled with the Feature Pack/Service Pack release.

Feature Pack/Service Pack Release	SSP Bundled
10.1 GA	No
10.1.0.1	SSP01 (System_Manager_10.1.0.1_r1010114394.bin)
10.1.0.2	SSP05 (AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2)
10.1.2.0	SSP09 (AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2)
10.1.3.0	SSP13 (AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2)
10.1.3.1	SSP16 (AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2)
10.1.3.2	SSP 21 (AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2)
10.1.3.3	SSP 24 (AV-SMGR10.1-RHEL8.4-SSP-024-02.tar.bz2)
10.1.3.4 or later release	No

21-April-2025 – Supplement 31 – Supplement 31 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #32 (AV-SMGR10.1-RHEL8.4-SSP-032-01.tar.bz2; PLDS ID SMGR101SSP32)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) or 10.1.x Feature Pack (10.1.2.0 or 10.1.3.0) or 10.1.3.1 or 10.1.3.2 or 10.1.3.3 or 10.1.3.4 or 10.1.3.5 release installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #32 is applicable to System Manager 10.1.x release.
- 10.1 SSPs will not work on the 10.2 release and there will be different SSPs for both 10.1 and 10.2.

- Reference the “**Finding the installation instructions**” section of this PCN for detailed installation instructions.
- Reference the “**Security Information**” section of this PCN for updates to the rpm and RHSAs for SSP #32.

System Manager feature packs and service packs have SSP's bundled with it (see table below for details on which SSP is bundled with which feature pack/service pack of SMGR).

If running on System Manager release 10.1.0.1 with a 10.1.0.1 hot fix installed or release 10.1.0.2 with a 10.1.0.2 hot fix installed and you are trying to upgrade to 10.1.0.2 (scenario only applies when on 10.1.0.1 +hotfix) or 10.1.2.0, then the SSP bundled along with 10.1.0.2 or 10.1.2.0 will not get installed as part of the feature pack/service pack installation. In such cases one can:

- Install either the same or higher version of the SSP manually on the system.
- Upgrade to 10.1.3.0 or higher version of System Manager which fixes the issue.

Below table provides the default SSP release bundled with the Feature Pack/Service Pack release.

Feature Pack/Service Pack Release	SSP Bundled
10.1 GA	No
10.1.0.1	SSP01 (System_Manager_10.1.0.1_r1010114394.bin)
10.1.0.2	SSP05 (AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2)
10.1.2.0	SSP09 (AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2)
10.1.3.0	SSP13 (AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2)
10.1.3.1	SSP16 (AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2)
10.1.3.2	SSP 21 (AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2)
10.1.3.3	SSP 24 (AV-SMGR10.1-RHEL8.4-SSP-024-02.tar.bz2)
10.1.3.4 or later release	No

17-February-2025 – Supplement 30 – Supplement 30 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #31 (AV-SMGR10.1-RHEL8.4-SSP-031-01.tar.bz2; PLDS ID SMGR101SSP31)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) or 10.1.x Feature Pack (10.1.2.0 or 10.1.3.0) or 10.1.3.1 or 10.1.3.2 or 10.1.3.3 or 10.1.3.4 or 10.1.3.5 release installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #31 is applicable to System Manager 10.1.x release.
- 10.1 SSPs will not work on the 10.2 release and there will be different SSPs for both 10.1 and 10.2.
- Reference the “**Finding the installation instructions**” section of this PCN for detailed

installation instructions.

- Reference the “**Security Information**” section of this PCN for updates to the rpm and RHSAs for SSP #31.

System Manager feature packs and service packs have SSP's bundled with it (see table below for details on which SSP is bundled with which feature pack/service pack of SMGR).

If running on System Manager release 10.1.0.1 with a 10.1.0.1 hot fix installed or release 10.1.0.2 with a 10.1.0.2 hot fix installed and you are trying to upgrade to 10.1.0.2 (scenario only applies when on 10.1.0.1 +hotfix) or 10.1.2.0, then the SSP bundled along with 10.1.0.2 or 10.1.2.0 will not get installed as part of the feature pack/service pack installation. In such cases one can:

- Install either the same or higher version of the SSP manually on the system.
- Upgrade to 10.1.3.0 or higher version of System Manager which fixes the issue.

Below table provides the default SSP release bundled with the Feature Pack/Service Pack release.

Feature Pack/Service Pack Release	SSP Bundled
10.1 GA	No
10.1.0.1	SSP01 (System_Manager_10.1.0.1_r1010114394.bin)
10.1.0.2	SSP05 (AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2)
10.1.2.0	SSP09 (AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2)
10.1.3.0	SSP13 (AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2)
10.1.3.1	SSP16 (AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2)
10.1.3.2	SSP 21 (AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2)
10.1.3.3	SSP 24 (AV-SMGR10.1-RHEL8.4-SSP-024-02.tar.bz2)
10.1.3.4	No
10.1.3.5	No

13-January-2025 – Supplement 29 – Supplement 29 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #30 (AV-SMGR10.1-RHEL8.4-SSP-030-01.tar.bz2; PLDS ID SMGR101SSP30)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) or 10.1.x Feature Pack (10.1.2.0 or 10.1.3.0) or 10.1.3.1 or 10.1.3.2 or 10.1.3.3 or 10.1.3.4 release installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #30 is applicable to System Manager 10.1.x release.
- 10.1 SSPs will not work on the 10.2 release and there will be different SSPs for both 10.1 and 10.2.

- Reference the “**Finding the installation instructions**” section of this PCN for detailed installation instructions.
- Reference the “**Security Information**” section of this PCN for updates to the rpm and RHSAs for SSP #30.

System Manager feature packs and service packs have SSP's bundled with it (see table below for details on which SSP is bundled with which feature pack/service pack of SMGR).

If running on System Manager release 10.1.0.1 with a 10.1.0.1 hot fix installed or release 10.1.0.2 with a 10.1.0.2 hot fix installed and you are trying to upgrade to 10.1.0.2 (scenario only applies when on 10.1.0.1 +hotfix) or 10.1.2.0, then the SSP bundled along with 10.1.0.2 or 10.1.2.0 will not get installed as part of the feature pack/service pack installation. In such cases one can:

- Install either the same or higher version of the SSP manually on the system.
- Upgrade to 10.1.3.0 or higher version of System Manager which fixes the issue.

Below table provides the default SSP release bundled with the Feature Pack/Service Pack release.

Feature Pack/Service Pack Release	SSP Bundled
10.1 GA	No
10.1.0.1	SSP01 (System_Manager_10.1.0.1_r1010114394.bin)
10.1.0.2	SSP05 (AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2)
10.1.2.0	SSP09 (AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2)
10.1.3.0	SSP13 (AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2)
10.1.3.1	SSP16 (AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2)
10.1.3.2	SSP 21 (AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2)
10.1.3.3	SSP 24 (AV-SMGR10.1-RHEL8.4-SSP-024-02.tar.bz2)
10.1.3.4	No

16-December-2024 – Supplement 28 – Supplement 28 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #29 (AV-SMGR10.1-RHEL8.4-SSP-029-01.tar.bz2; PLDS ID SMGR101SSP29)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) or 10.1.x Feature Pack (10.1.2.0 or 10.1.3.0) or 10.1.3.1 or 10.1.3.2 or 10.1.3.3 or 10.1.3.4 release installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #29 is applicable to System Manager 10.1.x release.
- 10.1 SSPs will not work on the 10.2 release and there will be different SSPs for both 10.1 and 10.2.

- Reference the “**Finding the installation instructions**” section of this PCN for detailed installation instructions.
- Reference the “**Security Information**” section of this PCN for updates to the rpm and RHSAs for SSP #29.

System Manager feature packs and service packs have SSP's bundled with it (see table below for details on which SSP is bundled with which feature pack/service pack of SMGR).

If running on System Manager release 10.1.0.1 with a 10.1.0.1 hot fix installed or release 10.1.0.2 with a 10.1.0.2 hot fix installed and you are trying to upgrade to 10.1.0.2 (scenario only applies when on 10.1.0.1 +hotfix) or 10.1.2.0, then the SSP bundled along with 10.1.0.2 or 10.1.2.0 will not get installed as part of the feature pack/service pack installation. In such cases one can:

- Install either the same or higher version of the SSP manually on the system.
- Upgrade to 10.1.3.0 or higher version of System Manager which fixes the issue.

Below table provides the default SSP release bundled with the Feature Pack/Service Pack release.

Feature Pack/Service Pack Release	SSP Bundled
10.1 GA	No
10.1.0.1	SSP01 (System_Manager_10.1.0.1_r1010114394.bin)
10.1.0.2	SSP05 (AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2)
10.1.2.0	SSP09 (AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2)
10.1.3.0	SSP13 (AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2)
10.1.3.1	SSP16 (AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2)
10.1.3.2	SSP 21 (AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2)
10.1.3.3	SSP 24 (AV-SMGR10.1-RHEL8.4-SSP-024-02.tar.bz2)
10.1.3.4	No

21-October-2024 – Supplement 27 – Supplement 27 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #28 (AV-SMGR10.1-RHEL8.4-SSP-028-01.tar.bz2; PLDS ID SMGR101SSP28)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) or 10.1.x Feature Pack (10.1.2.0 or 10.1.3.0) or 10.1.3.1 or 10.1.3.2 or 10.1.3.3 or 10.1.3.4 release installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #28 is applicable to System Manager 10.1.x release.
- 10.1 SSPs will not work on the 10.2 release and there will be different SSPs for both 10.1 and 10.2.
- Reference the “**Finding the installation instructions**” section of this PCN for detailed

installation instructions.

- Reference the **“Security Information”** section of this PCN for updates to the rpm and RHSAs for SSP #28.

System Manager feature packs and service packs have SSP's bundled with it (see table below for details on which SSP is bundled with which feature pack/service pack of SMGR).

If running on System Manager release 10.1.0.1 with a 10.1.0.1 hot fix installed or release 10.1.0.2 with a 10.1.0.2 hot fix installed and you are trying to upgrade to 10.1.0.2 (scenario only applies when on 10.1.0.1 +hotfix) or 10.1.2.0, then the SSP bundled along with 10.1.0.2 or 10.1.2.0 will not get installed as part of the feature pack/service pack installation. In such cases one can:

- Install either the same or higher version of the SSP manually on the system.
- Upgrade to 10.1.3.0 or higher version of System Manager which fixes the issue.

Below table provides the default SSP release bundled with the Feature Pack/Service Pack release.

Feature Pack/Service Pack Release	SSP Bundled
10.1 GA	No
10.1.0.1	SSP01 (System_Manager_10.1.0.1_r1010114394.bin)
10.1.0.2	SSP05 (AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2)
10.1.2.0	SSP09 (AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2)
10.1.3.0	SSP13 (AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2)
10.1.3.1	SSP16 (AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2)
10.1.3.2	SSP 21 (AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2)
10.1.3.3	SSP 24 (AV-SMGR10.1-RHEL8.4-SSP-024-02.tar.bz2)
10.1.3.4	No

9-September-2024 – Supplement 26 – Supplement 26 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #27 (AV-SMGR10.1-RHEL8.4-SSP-027-01.tar.bz2; PLDS ID SMGR101SSP27)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) or 10.1.x Feature Pack (10.1.2.0 or 10.1.3.0) or 10.1.3.1 or 10.1.3.2 or 10.1.3.3 release installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #27 is applicable to System Manager 10.1.x release.
- 10.1 SSPs will not work on the 10.2 release and there will be different SSPs for both 10.1 and 10.2.
- Reference the **“Finding the installation instructions”** section of this PCN for detailed installation instructions.
- Reference the **“Security Information”** section of this PCN for updates to the rpm and RHSAs

for SSP #27.

System Manager feature packs and service packs have SSP's bundled with it (see table below for details on which SSP is bundled with which feature pack/service pack of SMGR).

If running on System Manager release 10.1.0.1 with a 10.1.0.1 hot fix installed or release 10.1.0.2 with a 10.1.0.2 hot fix installed and you are trying to upgrade to 10.1.0.2 (scenario only applies when on 10.1.0.1 +hotfix) or 10.1.2.0, then the SSP bundled along with 10.1.0.2 or 10.1.2.0 will not get installed as part of the feature pack/service pack installation. In such cases one can:

- Install either the same or higher version of the SSP manually on the system.
- Upgrade to 10.1.3.0 or higher version of System Manager which fixes the issue.

Below table provides the default SSP release bundled with the Feature Pack/Service Pack release.

Feature Pack/Service Pack Release	SSP Bundled
10.1 GA	No
10.1.0.1	SSP01 (System_Manager_10.1.0.1_r1010114394.bin)
10.1.0.2	SSP05 (AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2)
10.1.2.0	SSP09 (AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2)
10.1.3.0	SSP13 (AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2)
10.1.3.1	SSP16 (AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2)
10.1.3.2	SSP 21 (AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2)
10.1.3.3	SSP 24 (AV-SMGR10.1-RHEL8.4-SSP-024-02.tar.bz2)

19-August-2024 – Supplement 25 – Supplement 25 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #26 (AV-SMGR10.1-RHEL8.4-SSP-026-03.tar.bz2; PLDS ID SMGR101SSP26)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) or 10.1.x Feature Pack (10.1.2.0 or 10.1.3.0) or 10.1.3.1 or 10.1.3.2 or 10.1.3.3 release installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #26 is applicable to System Manager 10.1.x release.
- 10.1 SSPs will not work on the 10.2 release and there will be different SSPs for both 10.1 and 10.2.
- Reference the “**Finding the installation instructions**” section of this PCN for detailed installation instructions.
- Reference the “**Security Information**” section of this PCN for updates to the rpm and RHSAs

for SSP #26.

System Manager feature packs and service packs have SSP's bundled with it (see table below for details on which SSP is bundled with which feature pack/service pack of SMGR).

If running on System Manager release 10.1.0.1 with a 10.1.0.1 hot fix installed or release 10.1.0.2 with a 10.1.0.2 hot fix installed and you are trying to upgrade to 10.1.0.2 (scenario only applies when on 10.1.0.1 +hotfix) or 10.1.2.0, then the SSP bundled along with 10.1.0.2 or 10.1.2.0 will not get installed as part of the feature pack/service pack installation. In such cases one can:

- Install either the same or higher version of the SSP manually on the system.
- Upgrade to 10.1.3.0 or higher version of System Manager which fixes the issue.

Below table provides the default SSP release bundled with the Feature Pack/Service Pack release.

Feature Pack/Service Pack Release	SSP Bundled
10.1 GA	No
10.1.0.1	SSP01 (System_Manager_10.1.0.1_r1010114394.bin)
10.1.0.2	SSP05 (AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2)
10.1.2.0	SSP09 (AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2)
10.1.3.0	SSP13 (AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2)
10.1.3.1	SSP16 (AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2)
10.1.3.2	SSP 21 (AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2)
10.1.3.3	SSP 24 (AV-SMGR10.1-RHEL8.4-SSP-024-02.tar.bz2)

8-July-2024 – Supplement 24 – Supplement 24 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #25 (AV-SMGR10.1-RHEL8.4-SSP-025-01.tar.bz2; PLDS ID SMGR101SSP25)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) or 10.1.x Feature Pack (10.1.2.0 or 10.1.3.0) or 10.1.3.1 or 10.1.3.2 or 10.1.3.3 release installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #25 is applicable to System Manager 10.1.x release.
- 10.1 SSPs will not work on the 10.2 release and there will be different SSPs for both 10.1 and 10.2.
- Reference the “**Finding the installation instructions**” section of this PCN for detailed installation instructions.
- Reference the “**Security Information**” section of this PCN for updates to the rpm and RHSAs for SSP #25.

System Manager feature packs and service packs have SSP's bundled with it (see table below for details on which SSP is bundled with which feature pack/service pack of SMGR).

If running on System Manager release 10.1.0.1 with a 10.1.0.1 hot fix installed or release 10.1.0.2 with a 10.1.0.2 hot fix installed and you are trying to upgrade to 10.1.0.2 (scenario only applies when on 10.1.0.1 +hotfix) or 10.1.2.0, then the SSP bundled along with 10.1.0.2 or 10.1.2.0 will not get installed as part of the feature pack/service pack installation. In such cases one can:

- Install either the same or higher version of the SSP manually on the system.
- Upgrade to 10.1.3.0 or higher version of System Manager which fixes the issue.

Below table provides the default SSP release bundled with the Feature Pack/Service Pack release.

Feature Pack/Service Pack Release	SSP Bundled
10.1 GA	No
10.1.0.1	SSP01 (System_Manager_10.1.0.1_r1010114394.bin)
10.1.0.2	SSP05 (AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2)
10.1.2.0	SSP09 (AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2)
10.1.3.0	SSP13 (AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2)
10.1.3.1	SSP16 (AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2)
10.1.3.2	SSP 21 (AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2)
10.1.3.3	SSP 24 (AV-SMGR10.1-RHEL8.4-SSP-024-02.tar.bz2)

10-June-2024 – Supplement 23 – Supplement 23 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #24 (AV-SMGR10.1-RHEL8.4-SSP-024-02.tar.bz2; PLDS ID SMGR101SSP24)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) or 10.1.x Feature Pack (10.1.2.0 or 10.1.3.0) or 10.1.3.1 or 10.1.3.2 or 10.1.3.3 release installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #24 is applicable to System Manager 10.1.x releases except 10.1.3.3 release.
- 10.1 SSPs will not work on the 10.2 release and there will be different SSPs for both 10.1 and 10.2.
- Reference the “**Finding the installation instructions**” section of this PCN for detailed installation instructions.
- Reference the “**Security Information**” section of this PCN for updates to the rpm and RHSAs

for SSP #24.

System Manager feature packs and service packs have SSP's bundled with it (see table below for details on which SSP is bundled with which feature pack/service pack of SMGR).

If running on System Manager release 10.1.0.1 with a 10.1.0.1 hot fix installed or release 10.1.0.2 with a 10.1.0.2 hot fix installed and you are trying to upgrade to 10.1.0.2 (scenario only applies when on 10.1.0.1 +hotfix) or 10.1.2.0, then the SSP bundled along with 10.1.0.2 or 10.1.2.0 will not get installed as part of the feature pack/service pack installation. In such cases one can:

- Install either the same or higher version of the SSP manually on the system.
- Upgrade to 10.1.3.0 or higher version of System Manager which fixes the issue.

Below table provides the default SSP release bundled with the Feature Pack/Service Pack release.

Feature Pack/Service Pack Release	SSP Bundled
10.1 GA	No
10.1.0.1	SSP01 (System_Manager_10.1.0.1_r1010114394.bin)
10.1.0.2	SSP05 (AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2)
10.1.2.0	SSP09 (AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2)
10.1.3.0	SSP13 (AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2)
10.1.3.1	SSP16 (AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2)
10.1.3.2	SSP 21 (AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2)
10.1.3.3	SSP 24 (AV-SMGR10.1-RHEL8.4-SSP-024-02.tar.bz2)

22-April-2024 – Supplement 22 – Supplement 22 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #23 (AV-SMGR10.1-RHEL8.4-SSP-023-01.tar.bz2; PLDS ID SMGR101SSP23)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) or 10.1.x Feature Pack (10.1.2.0 or 10.1.3.0) or 10.1.3.1 or 10.1.3.2 release installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP #23.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #23 is applicable to System Manager 10.1.x release.
- 10.1 SSPs will not work on the 10.2 release and there will be different SSPs for both 10.1 and 10.2.
- Reference the “**Finding the installation instructions**” section of this PCN for detailed installation instructions.
- Reference the “**Security Information**” section of this PCN for updates to the rpm and RHSAs

for SSP #23.

System Manager feature packs and service packs have SSP's bundled with it (see table below for details on which SSP is bundled with which feature pack/service pack of SMGR).

If running on System Manager release 10.1.0.1 with a 10.1.0.1 hot fix installed or release 10.1.0.2 with a 10.1.0.2 hot fix installed and you are trying to upgrade to 10.1.0.2 (scenario only applies when on 10.1.0.1 +hotfix) or 10.1.2.0, then the SSP bundled along with 10.1.0.2 or 10.1.2.0 will not get installed as part of the feature pack/service pack installation. In such cases one can:

- Install either the same or higher version of the SSP manually on the system.
- Upgrade to 10.1.3.0 or higher version of System Manager which fixes the issue.

Below table provides the default SSP release bundled with the Feature Pack/Service Pack release.

Feature Pack/Service Pack Release	SSP Bundled
10.1 GA	No
10.1.0.1	SSP01 (System_Manager_10.1.0.1_r1010114394.bin)
10.1.0.2	SSP05 (AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2)
10.1.2.0	SSP09 (AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2)
10.1.3.0	SSP13 (AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2)
10.1.3.1	SSP16 (AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2)
10.1.3.2	SSP 21 (AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2)

18-March-2024 – Supplement 21 – Supplement 21 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #22 (AV-SMGR10.1-RHEL8.4-SSP-022-05.tar.bz2; PLDS ID SMGR101SSP22)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) or 10.1.x Feature Pack (10.1.2.0 or 10.1.3.0) or 10.1.3.1 or 10.1.3.2 release installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP #22.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #22 is applicable to System Manager 10.1.x release.
- 10.1 SSPs will not work on the 10.2 release and there will be different SSPs for both 10.1 and 10.2.
- Reference the “**Finding the installation instructions**” section of this PCN for detailed installation instructions.
- Reference the “**Security Information**” section of this PCN for updates to the rpm and RHSAs for SSP #22.

System Manager feature packs and service packs have SSP's bundled with it (see table below for details on which SSP is bundled with which feature pack/service pack of SMGR).

If running on System Manager release 10.1.0.1 with a 10.1.0.1 hot fix installed or release 10.1.0.2 with a 10.1.0.2 hot fix installed and you are trying to upgrade to 10.1.0.2 (scenario only applies when on 10.1.0.1 +hotfix) or 10.1.2.0, then the SSP bundled along with 10.1.0.2 or 10.1.2.0 will not get installed as part of the feature pack/service pack installation. In such cases one can:

- Install either the same or higher version of the SSP manually on the system.
- Upgrade to 10.1.3.0 or higher version of System Manager which fixes the issue.

Below table provides the default SSP release bundled with the Feature Pack/Service Pack release.

Feature Pack/Service Pack Release	SSP Bundled
10.1 GA	No
10.1.0.1	SSP01 (System_Manager_10.1.0.1_r1010114394.bin)
10.1.0.2	SSP05 (AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2)
10.1.2.0	SSP09 (AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2)
10.1.3.0	SSP13 (AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2)
10.1.3.1	SSP16 (AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2)
10.1.3.2	SSP 21 (AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2)

16-January-2024 – Supplement 20 – Supplement 20 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #21 (AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2; PLDS ID SMGR101SSP21)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) or 10.1.x Feature Pack (10.1.2.0 or 10.1.3.0) or 10.1.3.1 release installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP #21.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #21 is applicable to System Manager 10.1.x release.
- 10.1 SSPs will not work on the 10.2 release and there will be different SSPs for both 10.1 and 10.2.
- Reference the “**Finding the installation instructions**” section of this PCN for detailed installation instructions.
- Reference the “**Security Information**” section of this PCN for updates to the rpm and RHSAs for SSP #21.

System Manager feature packs and service packs have SSP's bundled with it (see table below for details on which SSP is bundled with which feature pack/service pack of SMGR).

If running on System Manager release 10.1.0.1 with a 10.1.0.1 hot fix installed or release 10.1.0.2 with a 10.1.0.2 hot fix installed and you are trying to upgrade to 10.1.0.2 (scenario only applies when on 10.1.0.1 +hotfix) or 10.1.2.0, then the SSP bundled along with 10.1.0.2 or 10.1.2.0 will not get installed as part of the feature pack/service pack installation. In such cases one can:

- Install either the same or higher version of the SSP manually on the system.
- Upgrade to 10.1.3.0 or higher version of System Manager which fixes the issue.

Below table provides the default SSP release bundled with the Feature Pack/Service Pack release.

Feature Pack/Service Pack Release	SSP Bundled
10.1 GA	No
10.1.0.1	SSP01 (System_Manager_10.1.0.1_r1010114394.bin)
10.1.0.2	SSP05 (AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2)
10.1.2.0	SSP09 (AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2)
10.1.3.0	SSP13 (AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2)
10.1.3.1	SSP16 (AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2)
10.1.3.2	SSP 21 (AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2)

18-December-2023 – Supplement 19 – Supplement 19 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #20 (AV-SMGR10.1-RHEL8.4-SSP-020-01.tar.bz2; PLDS ID SMGR101SSP20)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) or 10.1.x Feature Pack (10.1.2.0 or 10.1.3.0) or 10.1.3.1 release installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP #20.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #20 is applicable to System Manager 10.1.x release.
- 10.1 SSPs will not work on the 10.2 release and there will be different SSPs for both 10.1 and 10.2.
- Reference the “**Finding the installation instructions**” section of this PCN for detailed installation instructions.
- Reference the “**Security Information**” section of this PCN for updates to the rpm and RHSAs for SSP #20.

System Manager feature packs and service packs have SSP's bundled with it (see table below for details on which SSP is bundled with which feature pack/service pack of SMGR).

If running on System Manager release 10.1.0.1 with a 10.1.0.1 hot fix installed or release 10.1.0.2 with a 10.1.0.2 hot fix installed and you are trying to upgrade to 10.1.0.2 (scenario only applies when on 10.1.0.1 +hotfix) or 10.1.2.0, then the SSP bundled along with 10.1.0.2 or 10.1.2.0 will not get installed as part of the feature pack/service pack installation. In such cases one can:

- Install either the same or higher version of the SSP manually on the system.
- Upgrade to 10.1.3.0 or higher version of System Manager which fixes the issue.

Below table provides the default SSP release bundled with the Feature Pack/Service Pack release.

Feature Pack/Service Pack Release	SSP Bundled
10.1 GA	No
10.1.0.1	SSP01 (System_Manager_10.1.0.1_r1010114394.bin)
10.1.0.2	SSP05 (AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2)
10.1.2.0	SSP09 (AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2)
10.1.3.0	SSP13 (AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2)
10.1.3.1	SSP16 (AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2)

20-November-2023 – Supplement 18 – Supplement 18 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #19 (AV-SMGR10.1-RHEL8.4-SSP-019-01.tar.bz2; PLDS ID SMGR101SSP19)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) or 10.1.x Feature Pack (10.1.2.0 or 10.1.3.0) or 10.1.3.1 release installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP #19.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #19 is applicable to System Manager 10.1.x release.
- Reference the “**Finding the installation instructions**” section of this PCN for detailed installation instructions.
- Reference the “**Security Information**” section of this PCN for updates to the rpm and RHSAs for SSP #19.

System Manager feature packs and service packs have SSP's bundled with it (see table below for details on which SSP is bundled with which feature pack/service pack of SMGR).

If running on System Manager release 10.1.0.1 with a 10.1.0.1 hot fix installed or release 10.1.0.2 with a 10.1.0.2 hot fix installed and you are trying to upgrade to 10.1.0.2 (scenario only applies when on 10.1.0.1 +hotfix) or 10.1.2, then the SSP bundled along with 10.1.0.2 or 10.1.2 will not get installed as part of the feature pack/service pack installation. In such cases one can:

- Install either the same or higher version of the SSP manually on the system.
- Upgrade to 10.1.3 or higher version of System Manager which fixes the issue.

Below table provides the default SSP release bundled with the Feature Pack/Service Pack release.

Feature Pack/Service Pack Release	SSP Bundled
10.1 GA	No
10.1.0.1	SSP01 (System_Manager_10.1.0.1_r1010114394.bin)
10.1.0.2	SSP05 (AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2)
10.1.2.0	SSP09 (AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2)
10.1.3.0	SSP13 (AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2)
10.1.3.1	SSP16 (AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2)

16-October-2023 – Supplement 17 – Supplement 17 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #18 (AV-SMGR10.1-RHEL8.4-SSP-018-01.tar.bz2; PLDS ID SMGR101SSP18)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) or 10.1.x Feature Pack (10.1.2.0 or 10.1.3.0) or 10.1.3.1 release installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP #18.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #18 is applicable to System Manager 10.1.x release.
- Reference the “**Finding the installation instructions**” section of this PCN for detailed installation instructions.
- Reference the “**Security Information**” section of this PCN for updates to the rpm and RHSAs for SSP #18.

System Manager feature packs and service packs have SSP's bundled with it (see table below for details on which SSP is bundled with which feature pack/service pack of SMGR).

If running on System Manager release 10.1.0.1 with a 10.1.0.1 hot fix installed or release 10.1.0.2 with a 10.1.0.2 hot fix installed and you are trying to upgrade to 10.1.0.2 (scenario only applies when on 10.1.0.1 +hotfix) or 10.1.2, then the SSP bundled along with 10.1.0.2 or 10.1.2 will not get installed as part of the feature pack/service pack installation. In such cases one can:

- Install either the same or higher version of the SSP manually on the system.
- Upgrade to 10.1.3 or higher version of System Manager which fixes the issue.

Below table provides the default SSP release bundled with the Feature Pack/Service Pack release.

Feature Pack/Service Pack Release	SSP Bundled
10.1 GA	No
10.1.0.1	SSP01 (System_Manager_10.1.0.1_r1010114394.bin)
10.1.0.2	SSP05 (AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2)
10.1.2.0	SSP09 (AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2)
10.1.3.0	SSP13 (AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2)
10.1.3.1	SSP16 (AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2)

18-September-2023 – Supplement 16 – Supplement 16 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #17 (AV-SMGR10.1-RHEL8.4-SSP-017-03.tar.bz2; PLDS ID SMGR101SSP17)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) or 10.1.x Feature Pack (10.1.2.0 or 10.1.3.0) or 10.1.3.1 release installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP #17.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #17 is applicable to System Manager 10.1.x release.
- Reference the “**Finding the installation instructions**” section of this PCN for detailed installation instructions.
- Reference the “**Security Information**” section of this PCN for updates to the rpm and RHSAs for SSP #17.

System Manager feature packs and service packs have SSP's bundled with it (see table below for details on which SSP is bundled with which feature pack/service pack of SMGR).

If running on System Manager release 10.1.0.1 with a 10.1.0.1 hot fix installed or release 10.1.0.2 with a 10.1.0.2 hot fix installed and you are trying to upgrade to 10.1.0.2 (scenario only applies when on 10.1.0.1 +hotfix) or 10.1.2, then the SSP bundled along with 10.1.0.2 or 10.1.2 will not get installed as part of the feature pack/service pack installation. In such cases one can:

- Install either the same or higher version of the SSP manually on the system.
- Upgrade to 10.1.3 or higher version of System Manager which fixes the issue.

Below table provides the default SSP release bundled with the Feature Pack/Service Pack release.

Feature Pack/Service Pack Release	SSP Bundled
10.1 GA	No

10.1.0.1	SSP01 (System_Manager_10.1.0.1_r1010114394.bin)
10.1.0.2	SSP05 (AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2)
10.1.2.0	SSP09 (AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2)
10.1.3.0	SSP13 (AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2)
10.1.3.1	SSP16 (AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2)

28-August-2023 – Supplement 15 – Supplement 15 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #16 (AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2; PLDS ID SMGR101SSP16)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) or 10.1.x Feature Pack (10.1.2.0 or 10.1.3.0) release installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP #16.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #16 is applicable to System Manager 10.1.x release.
- Reference the “**Finding the installation instructions**” section of this PCN for detailed installation instructions.
- Reference the “**Security Information**” section of this PCN for updates to the rpm and RHSAs for SSP #16.

System Manager feature packs and service packs have SSP's bundled with it (see table below for details on which SSP is bundled with which feature pack/service pack of SMGR).

If running on System Manager release 10.1.0.1 with a 10.1.0.1 hot fix installed or release 10.1.0.2 with a 10.1.0.2 hot fix installed and you are trying to upgrade to 10.1.0.2 (scenario only applies when on 10.1.0.1 +hotfix) or 10.1.2, then the SSP bundled along with 10.1.0.2 or 10.1.2 will not get installed as part of the feature pack/service pack installation. In such cases one can:

- Install either the same or higher version of the SSP manually on the system.
- Upgrade to 10.1.3 or higher version of System Manager which fixes the issue.

Below table provides the default SSP release bundled with the Feature Pack/Service Pack release.

Feature Pack/Service Pack Release	SSP Bundled
10.1 GA	No
10.1.0.1	SSP01 (System_Manager_10.1.0.1_r1010114394.bin)
10.1.0.2	SSP05 (AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2)
10.1.2.0	SSP09 (AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2)

10.1.3.0	SSP13 (AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2)
10.1.3.1	SSP16 (AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2)

17-July-2023 – Supplement 14 – Supplement 14 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #15 (AV-SMGR10.1-RHEL8.4-SSP-015-01.tar.bz2; PLDS ID SMGR101SSP15)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) or 10.1.x Feature Pack (10.1.2.0 or 10.1.3.0) release installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP #15.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #15 is applicable to System Manager 10.1.x release.
- Reference the “**Finding the installation instructions**” section of this PCN for detailed installation instructions.
- Reference the “**Security Information**” section of this PCN for updates to the rpm and RHSAs for SSP #15.

System Manager feature packs and service packs have SSP's bundled with it (see table below for details on which SSP is bundled with which feature pack/service pack of SMGR).

If running on System Manager release 10.1.0.1 with a 10.1.0.1 hot fix installed or release 10.1.0.2 with a 10.1.0.2 hot fix installed and you are trying to upgrade to 10.1.0.2 (scenario only applies when on 10.1.0.1 +hotfix) or 10.1.2, then the SSP bundled along with 10.1.0.2 or 10.1.2 will not get installed as part of the feature pack/service pack installation. In such cases one can:

- Install either the same or higher version of the SSP manually on the system.
- Upgrade to 10.1.3 or higher version of System Manager which fixes the issue.

Below table provides the default SSP release bundled with the Feature Pack/Service Pack release.

Feature Pack/Service Pack Release	SSP Bundled
10.1 GA	No
10.1.0.1	SSP01 (System_Manager_10.1.0.1_r1010114394.bin)
10.1.0.2	SSP05 (AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2)
10.1.2.0	SSP09 (AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2)
10.1.3.0	SSP13 (AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2)

20-June-2023 – Supplement 13 – Supplement 13 of this PCN introduces **Avaya Aura System Manager**

10.1 Security Service Pack SSP #14 (AV-SMGR10.1-RHEL8.4-SSP-014-01.tar.bz2; PLDS ID SMGR101SSP14) for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) or 10.1.x Feature Pack (10.1.2.0 or 10.1.3.0) release installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP #14.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #14 is applicable to System Manager 10.1.x release.
- Reference the “**Finding the installation instructions**” section of this PCN for detailed installation instructions.
- Reference the “**Security Information**” section of this PCN for updates to the rpm and RHSAs for SSP #14.

Below table provides the default SSP release bundled with the Feature Pack/Service Pack release.

Feature Pack/Service Pack Release	SSP Bundled
10.1 GA	No
10.1.0.1	SSP01 (System_Manager_10.1.0.1_r1010114394.bin)
10.1.0.2	SSP05 (AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2)
10.1.2.0	SSP09 (AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2)
10.1.3.0	SSP13 (AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2)

22-May-2023 – Supplement 12 – Supplement 12 of this PCN introduces Avaya Aura System Manager 10.1 Security Service Pack SSP #13 (AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2; PLDS ID SMGR101SSP13) for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) or 10.1.x Feature Pack (10.1.2.0 or 10.1.3.0) release installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP #13.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #13 is applicable to System Manager 10.1.x release. (No need to install SSP #13 on SMGR 10.1.3.0 release as 10.1.3.0 bundled with SSP #13).
- Reference the “**Finding the installation instructions**” section of this PCN for detailed

installation instructions.

- Reference the “**Security Information**” section of this PCN for updates to the rpm and RHSAs for SSP #13.

Note – Below table gives System Manager SSP release bundled with in Service Pack or Feature Pack release.

Service or Feature Pack Release	SSP Bundled
10.1 GA	No
10.1.0.1	SSP01 (System_Manager_10.1.0.1_r1010114394.bin)
10.1.0.2	SSP05 (AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2)
10.1.2.0	SSP09 (AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2)
10.1.3.0	SSP13 (AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2)

17-April-2023 – Supplement 11 – Supplement 11 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #12 (AV-SMGR10.1-RHEL8.4-SSP-012-01.tar.bz2; PLDS ID SMGR101SSP12)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) or 10.1.x Feature Pack(10.1.2.0) or later release installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP #12.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #12 is applicable to System Manager 10.1.x release.
- Reference the “**Finding the installation instructions**” section of this PCN for detailed installation instructions.
- Reference the “**Security Information**” section of this PCN for updates to the rpm and RHSAs for SSP #12.

Note – Below table gives System Manager SSP release bundled with in Service Pack or Feature Pack release.

Service or Feature Pack Release	SSP Bundled
10.1 GA	No
10.1.0.1	SSP01 (System_Manager_10.1.0.1_r1010114394.bin)
10.1.0.2	SSP05 (AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2)
10.1.2.0	SSP09 (AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2)

20-March-2023 – Supplement 10 – Supplement 10 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #11 (AV-SMGR10.1-RHEL8.4-SSP-011-02.tar.bz2; PLDS ID SMGR101SSP11)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) or 10.1.x Feature Pack(10.1.2.0) installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP #11.
- System Manage Security Service Pack Installation fail unless Service Pack 10.1.0.1 or later is installed first.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #11 is applicable to System Manager 10.1.x release.
- Reference the “**Finding the installation instructions**” section of this PCN for detailed installation instructions.
- Reference the “**Security Information**” section of this PCN for updates to the rpm and RHSAs for SSP #11.
- There was no Aura February 2023 Security Service Pack update required for Communication Manager, Session Manager, System Manager and Application Enablement Services. Only WebLM required a February 2023 Security Service Pack update.

17-February-2023 – Supplement 9-1 – Supplement 9-1 of this PCN provides updates to the **Finding the installation instructions** section of this PCN, including examples and correction of a file path.

23-January-2023 – Supplement 9 – Supplement 9 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #10 (AV-SMGR10.1-RHEL8.4-SSP-010-01.tar.bz2; PLDS ID SMGR101SSP10) for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP #10.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #10 is applicable to System Manager 10.1.x release.

19-December-2022 – Supplement 8 – Supplement 8 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #9 (AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2; PLDS ID SMGR101SSP09) for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP #9.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #9 is applicable to System Manager 10.1.x release.

28-November-2022 – Supplement 7 – Supplement 7 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #8 (AV-SMGR10.1-RHEL8.4-SSP-008-01.tar.bz2; PLDS ID SMGR101SSP08)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP #8.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #8 is applicable to System Manager 10.1.x release.

17-October-2022 – Supplement 6 – Supplement 6 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #7 (AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2; PLDS ID SMGR101SSP07)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP #7.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #7 is applicable to System Manager 10.1.x release.

26-September-2022 – Supplement 5 – Supplement 5 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #6 (AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2; PLDS ID SMGR101SSP06)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.x service pack (10.1.0.0 Service Pack 1 or Service Pack 2) installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP #6.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #6 is applicable to System Manager 10.1.x release.

16-August-2022 – Supplement 4 – Supplement 4 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #5 (AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2; PLDS ID SMGR101SSP05)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.0.1 (10.1.0.0 Service Pack 1) installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP #5.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #5 is applicable to System Manager 10.1.x release.

22-July-2022 – Supplement 3 – Supplement 3 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #4(AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2; PLDS ID SMGR101SSP04)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.0.1 (10.1.0.0 Service Pack 1) installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP #4.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #4 is applicable to System Manager 10.1.x release.

21-June-2022 – Supplement 2 – Supplement 2 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #3(AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2; PLDS ID SMGR101SSP03)** for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.0.1 (10.1.0.0 Service Pack 1) installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP #3.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #3 is applicable to System Manager 10.1.x release.

16-May-2022 – Supplement 1 – Supplement 1 of this PCN introduces **Avaya Aura System Manager 10.1 Security Service Pack SSP #2(AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2; PLDS ID SMGR101SSP02) for System Manager 10.1.x 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.

IMPORTANT NOTE:

- System Manager 10.1.0.1 (10.1.0.0 Service Pack 1) installation is **mandatory** before installing Aura System Manager 10.1 Security Service Pack SSP #2.
- This SSP is not applicable for System Manager R10.1.x Software Only deployments. This patch should **NOT** be installed on System Manager R10.1.x Software Only deployments.
- System Manager 10.1 SSP #2 is applicable to System Manager 10.1.x release.

18-April-2022 – There is no separate System Manager Security Service Pack being released coincident with System Manager 10.1.0.1 (10.1.0.0 Service Pack 1) release. For SMGR 10.1, the SSP package is already embedded in 10.1.0.0 Service Pack 1 and will get installed automatically along with Service Pack 1. Reference PCN2137S for details.

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 10.1.0.1 Service Pack installation on Software Only release will not install any security fixes.

Level of Risk/Severity
Class 1=High
Class 2=Medium
Class 3=Low

Class 2

Is it required that this PCN be

This PCN is required for Avaya Aura® System Manager 10.1.x release.

applied to my system?

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. Security Service Packs 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** resolves vulnerabilities described by RHSAs/CVEs referenced in section 1B – Security information.

NOTE: The Avaya Security Advisory (ASA) process has been reworked to provide more timely updates. [Avaya's Product Security Vulnerability Response Policy](#) has been updated in support of the new ASA process. The following new documents provide a table of vulnerabilities impacting monitored, supported product versions:

[Security Advisory October-December 2023](#)

[Security Advisory for 2024](#)

[Security Advisory for 2025](#)

Previously created individual ASAs are still available on the [Avaya Support - Help Center - Avaya Product Security](#) page.

The **Avaya Aura® System Manager Release 10.1 Release Notes** can be obtained by performing the following steps from a browser:

1. Go to <http://support.avaya.com> then enter your **Username** and **Password** and select **LOG IN**.
2. Mouse over **Search Product** at the top of the page.
3. Begin to type **System Manager** and when Avaya Aura® System Manager appears as a selection below, select it.
4. Select **10.1.x** from the **Choose Release** pull down menu to the right.
5. Select **Product Documents** on the new page that is displayed. Scroll down (if necessary) and select **View All Product Documents**.

6. Under **Filters**, for category **TYPE** select **Manuals** and for category **SUB TYPE** select **Release Notes & Software Update Notes**.

7. Select the document titled **Avaya Aura® 10.1.x.x Release Notes**.

SSP required artifacts and fix IDs are no longer be tracked in the Avaya Aura 10.1.x Release Notes but will be included in this PCN.

Security Service Packs (SSP) are cumulative. This means that all fixes in previous 10.1.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** in the **Enter Product Name** box and when Avaya Aura® System Manager appears as a selection below, select it.
4. Select 10.1.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 and WebLM 10.1.x Security Service Pack**.
7. Scroll down the page to find the download link for the appropriate deployment file security service pack. This link will take you to the PLDS system with the **Download pub ID** already entered. This page also includes a link to this PCN and the Release Notes.
8. Select the Download link to begin the download from PLDS.

Software updates can also be downloaded directly from the PLDS system at <http://plds.avaya.com>.

1. Enter your login ID and password. You may have to search for and enter your company name and/or accept the one time EULA to gain access to software downloads.
2. Select **View Downloads**.
3. In the **Search by Download** tab enter the correct PLDS ID (corresponding PLDS IDs included in the Description section of this document) in the **Download pub ID** search field to access the download. Select the **Download** link to begin the download.

PLDS Hints:

1. In the PLDS **View Downloads** section under the **Suggested Downloads** tab, select **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 **10.1** in the **Version** search field to display all available System Manager 10.1 software downloads.

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

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

Important Security Service Pack Installation Notes:

- 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.
- Separate Security Pack patch is **NOT** applicable for System Manager 10.1.x Software Only deployments. Separate Security Pack patch should not be installed on System Manager 10.1.x Software Only deployments.

Problem – Installing Security Service Pack from SSP32 onwards on System Manager Releases 10.1.3.1 to 10.1.3.3, may fail with below error

08-Aug-2025 05:38:33: We are updating the RPMs, please wait

warning: /swlibrary/SMGR10.1/rpms/aide-0.16-14.el8_5.1.x86_64.rpm: Header V3

RSA/SHA256 Signature, key ID fd431d51: NOKEY

error: Failed dependencies:

subscription-manager is needed by insights-client-0:3.2.2-2.el8.noarch

08-Aug-2025 05:38:38: Unable to update SSP

Cause - From System Manager 10.1.3.4 onwards, the framework has been updated, and the issue is resolved.

Solution - In case of a certificate signature or key issue as mentioned above, if you're unable to install the SSP bundle, follow the workaround in [PSN](#) then proceed to install SSP34, or at the minimum, update System Manager to 10.1.3.4 or to latest 10.1.3.6 before installing SSP34 and higher SSP release.

Please ensure that VMware snapshots of the System Manager are taken prior to making any changes or updates.

Security Service Pack Installation instructions (the following uses SSP #9 as an example):

- 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 and on PLDS

```
#md5sum <Security Service Pack Patch bz2 file name>
```

```
EG:
```

```
#md5sum AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2
# 4043ae1ac95239e9b80c5135656b176d /swlibrary/AV-SMGR10.1-
RHEL8.4-SSP-009-01.tar.bz2
```

- Run the patch installer using the following command:

```
#av-update-os <Security Service Pack Patch bz2 file name>
```

```
EG:
```

```
#av-update-os AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2
```

- Wait for the system to execute the patch installer in the background and display the installer prompt.
- User having administrative privileges can monitor the SSP installation log with the following command:

```
#tail -f /var/log/avaya/SSP<XXX>.log-<%Y%m%d%H%M%S>
```

```
EG:
```

```
#tail -f /var/log/avaya/SSP009.log-20230215123000
```

Note that the log file name will change from system to system since it is generated based on when the Security Service Pack is installed. Verify the timestamp to ensure the correct file is being examined. This can be accomplished by executing the following command which will list the files sorted by time, with the most recent at the bottom of the list.

```
#ls -lartsh /var/log/avaya/
```

- User having administrative privileges can verify successful installation by looking for the following message in the relevant SSP log.
For example, in /var/log/avaya/SSP009.log-<%Y%m%d%H%M%S>
"New SSP version 009 and build number 01 updated successfully"
- All users can utilize the `swversion` output to verify the SSP installation. The `swversion` output will have below content relevant for the SSP being installed.

```
EG:
```

```
AV_SSP_VERSION : 009
```

- 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.
- Reboot system from VSphere Client GUI or using reboot command if you have root access to System Manager.

Note- Do not use `rebootVM` command to reboot System Manager.

- 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, relevant for the SSP being installed. In this example, SSP #9.
AV_SSP_VERSION : 009

What you should do if the Service Pack installation fails?

- 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:

By reverting System Manager VM snapshot if it was taken prior to SSP installation.

SECTION 1B – SECURITY INFORMATION

Are there any security risks involved?

Issues described by the RHSAs listed in the next section are corrected by the Security Service Pack as noted. Security Service Packs (SSPs) include the fixes from all previous SSPs respectively for a given System Manager release.

Avaya Security Vulnerability Classification:

The Avaya Security Advisory (ASA) process has been reworked to provide more timely updates. [Avaya’s Product Security Vulnerability Response Policy](#) has been updated in support of the new ASA process. The following new documents provide a table of vulnerabilities impacting monitored, supported product versions:

[Security Advisory October-December 2023](#)

[Security Advisory for 2024](#)

[Security Advisory for 2025](#)

Previously created individual ASAs are still available on the [Avaya Support - Help Center - Avaya Product Security](#) page.

NOTE: Red Hat typically does not rebase packages to older versions. However, Avaya ensures applicable fixes from the latest supported RHEL 8.x versions are applied to older RHEL minor releases being used in Avaya. A security scan that only considers the Red Hat version may incorrectly report that an older release of RHEL is unsupported. If a scan reports a RHEL vulnerability then please check the actual RPM version on the system to confirm that it is not a false positive. If it is not a false positive then perform the following:

- Please check when the RPM fix was released by RHEL. If the fix was released by RHEL within 4 weeks of the SSP going GA then it is possible that the fix was not picked up as part of the build and will be available in a subsequent SSP.
- If the fix was released by RHEL more than 4 weeks prior to the SSP going GA then open an SR with Avaya to have it reviewed.

Avaya picks up fixes from official RHEL repo's only. Even though a fix may be available, RHEL may take time to incorporate it into their base so it is important to look at RHEL CVE dates and not dates from any other source.

Security Service Packs (SSP) are cumulative. This means that all fixes in previous 10.1.x SSPs are included in the most recent SSP.

SSP Patch #37 contains the fixes from the following previous patches:

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-008-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-010-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-011-02.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-012-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-014-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-015-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-017-03.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-018-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-019-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-020-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-022-05.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-023-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-024-02.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-025-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-026-03.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-027-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-028-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-029-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-030-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-031-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-032-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-033-05.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-034-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-035-02.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-036-01.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #37 Nov 2025 release includes the following rpm updates:

Note: This list shows all package version updates since the previous SSP.

However, only the latest rpm version for a specific package is installed (if multiple versions are listed).

gnutls-3.6.16-8.el8_10.x86_64	kernel-tools-4.18.0-553.77.1.el8_10.x86_64
kernel-4.18.0-553.75.1.el8_10.x86_64	kernel-tools-4.18.0-553.78.1.el8_10.x86_64
kernel-4.18.0-553.76.1.el8_10.x86_64	kernel-tools-libs-4.18.0-553.75.1.el8_10.x86_64
kernel-4.18.0-553.77.1.el8_10.x86_64	kernel-tools-libs-4.18.0-553.76.1.el8_10.x86_64
kernel-4.18.0-553.78.1.el8_10.x86_64	kernel-tools-libs-4.18.0-553.77.1.el8_10.x86_64
kernel-core-4.18.0-553.75.1.el8_10.x86_64	kernel-tools-libs-4.18.0-553.78.1.el8_10.x86_64
kernel-core-4.18.0-553.76.1.el8_10.x86_64	open-vm-tools-12.3.5-2.el8_10.1.x86_64
kernel-core-4.18.0-553.77.1.el8_10.x86_64	openssh-8.0p1-26.el8_10.x86_64
kernel-core-4.18.0-553.78.1.el8_10.x86_64	openssh-askpass-8.0p1-26.el8_10.x86_64
kernel-headers-4.18.0-553.75.1.el8_10.x86_64	openssh-clients-8.0p1-26.el8_10.x86_64
kernel-headers-4.18.0-553.76.1.el8_10.x86_64	openssh-server-8.0p1-26.el8_10.x86_64
kernel-headers-4.18.0-553.77.1.el8_10.x86_64	python3-perf-4.18.0-553.75.1.el8_10.x86_64
kernel-headers-4.18.0-553.78.1.el8_10.x86_64	python3-perf-4.18.0-553.76.1.el8_10.x86_64
kernel-modules-4.18.0-553.75.1.el8_10.x86_64	python3-perf-4.18.0-553.77.1.el8_10.x86_64
kernel-modules-4.18.0-553.76.1.el8_10.x86_64	python3-perf-4.18.0-553.78.1.el8_10.x86_64
kernel-modules-4.18.0-553.77.1.el8_10.x86_64	vim-common-2:8.0.1763-21.el8_10.x86_64
kernel-modules-4.18.0-553.78.1.el8_10.x86_64	vim-enhanced-2:8.0.1763-21.el8_10.x86_64
kernel-tools-4.18.0-553.75.1.el8_10.x86_64	vim-filessystem-2:8.0.1763-21.el8_10.noarch
kernel-tools-4.18.0-553.76.1.el8_10.x86_64	vim-minimal-2:8.0.1763-21.el8_10.x86_64

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #37 Nov 2025 release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
SMGR-78698	kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:15785 RHSA-2025:16372 RHSA-2025:16919 RHSA-2025:17397	CVE-2023-53125, CVE-2025-38350, CVE-2025-38392 CVE-2025-38449, CVE-2025-38461, CVE-2025-38498 CVE-2025-38556, CVE-2025-22026, CVE-2025-37797 CVE-2022-50087, CVE-2025-38718, CVE-2025-38527 CVE-2025-39730	Important
SMGR-78700	openSSH	RHSA-2025:16823	CVE-2025-26465	Moderate
SMGR-78702	gnutls	RHSA-2025:17415	CVE-2025-32990, CVE-2025-32988, CVE-2025-6395	Moderate
SMGR-78704	open-vm-tools	RHSA-2025:17509	CVE-2025-41244	Important
SMGR-78706	vim	RHSA-2025:17715	CVE-2025-53906, CVE-2025-53905	Moderate

SSP Patch #36 contains the fixes from the following previous patches:

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-008-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-010-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-011-02.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-012-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-014-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-015-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-017-03.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-018-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-019-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-020-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-022-05.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-023-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-024-02.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-025-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-026-03.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-027-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-028-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-029-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-030-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-031-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-032-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-033-05.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-034-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-035-02.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #36 Oct 2025 release includes the following rpm updates:

Note: This list shows all package version updates since the previous SSP.
However, only the latest rpm version for a specific package is installed (if multiple versions are listed).

aide-0.16-15.el8_10.2.x86_64	libarchive-3.3.3-6.el8_10.x86_64
cups-libs-1:2.2.6-63.el8_10.x86_64	libudisks2-2.9.0-16.el8_10.1.x86_64
kernel-4.18.0-553.74.1.el8_10.x86_64	pam-1.3.1-38.el8_10.x86_64
kernel-core-4.18.0-553.74.1.el8_10.x86_64	platform-python-3.6.8-71.el8_10.x86_64
kernel-headers-4.18.0-553.74.1.el8_10.x86_64	python3-cryptography-3.2.1-8.el8_10.x86_64
kernel-modules-4.18.0-553.74.1.el8_10.x86_64	python3-libs-3.6.8-71.el8_10.x86_64
kernel-tools-4.18.0-553.74.1.el8_10.x86_64	python3-perf-4.18.0-553.74.1.el8_10.x86_64
kernel-tools-libs-4.18.0-553.74.1.el8_10.x86_64	udisks2-2.9.0-16.el8_10.1.x86_64

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #36 Oct 2025 release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
SMGR-78651	kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:13589 RHSA-2025:13960 RHSA-2025:14438 RHSA-2025:15008 RHSA-2025:15471	CVE-2025-21727, CVE-2025-21759, CVE-2021-47670 CVE-2025-38085, CVE-2025-38159, CVE-2025-22097 CVE-2025-37914, CVE-2025-38250, CVE-2025-22058 CVE-2025-38200, CVE-2025-38380, CVE-2025-38211 CVE-2025-38332, CVE-2025-38464, CVE-2025-38477	Important
SMGR-78653	libarchive	RHSA-2025:14135	CVE-2025-5914	Important
SMGR-78655	python-cryptography	RHSA-2025:14553	CVE-2023-49083	Moderate
SMGR-78657	pam	RHSA-2025:14557	CVE-2025-6020	Important
SMGR-78659	python3	RHSA-2025:14560	CVE-2025-8194	Important
SMGR-78661	aide	RHSA-2025:14573	CVE-2025-54389	Important
SMGR-78663	udisks2	RHSA-2025:15017	CVE-2025-8067	Important
SMGR-78665	cups	RHSA-2025:15702	CVE-2025-58060	Important

SSP Patch #35 contains the fixes from the following previous patches:

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-008-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-010-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-011-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-012-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-014-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-015-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-017-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-018-01.tar.bz2

AV-SMGR10.1-RHEL8.4-SSP-019-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-020-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-022-05.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-023-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-024-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-025-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-026-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-027-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-028-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-029-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-030-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-031-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-032-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-033-05.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-034-01.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #35 Sept 2025 release includes the following rpm updates:

emacs-filesystem-1:26.1-15.el8_10.noarch	kernel-tools-libs-4.18.0-553.62.1.el8_10.x86_64
gdk-pixbuf2-2.36.12-7.el8_10.x86_64	kernel-tools-libs-4.18.0-553.63.1.el8_10.x86_64
gdk-pixbuf2-modules-2.36.12-7.el8_10.x86_64	kernel-tools-libs-4.18.0-553.64.1.el8_10.x86_64
glib2-2.56.4-166.el8_10.x86_64	kernel-tools-libs-4.18.0-553.66.1.el8_10.x86_64
glibc-2.28-251.el8_10.25.i686	libblockdev-2.28-7.el8_10.x86_64
glibc-2.28-251.el8_10.25.x86_64	libblockdev-crypto-2.28-7.el8_10.x86_64
glibc-all-langpacks-2.28-251.el8_10.25.x86_64	libblockdev-fs-2.28-7.el8_10.x86_64
glibc-common-2.28-251.el8_10.25.x86_64	libblockdev-loop-2.28-7.el8_10.x86_64
glibc-devel-2.28-251.el8_10.25.x86_64	libblockdev-mdraid-2.28-7.el8_10.x86_64
glibc-headers-2.28-251.el8_10.25.x86_64	libblockdev-part-2.28-7.el8_10.x86_64
glibc-langpack-en-2.28-251.el8_10.25.x86_64	libblockdev-swap-2.28-7.el8_10.x86_64
java-1.8.0-openjdk-1:1.8.0.462.b08-2.el8.x86_64	libblockdev-utils-2.28-7.el8_10.x86_64
java-1.8.0-openjdk-devel-1:1.8.0.462.b08-2.el8.x86_64	libxml2-2.9.7-21.el8_10.1.x86_64
java-1.8.0-openjdk-headless-1:1.8.0.462.b08-2.el8.x86_64	libxml2-2.9.7-21.el8_10.2.x86_64
jq-1.6-11.el8_10.x86_64	libxml2-2.9.7-21.el8_10.3.x86_64
kernel-4.18.0-553.58.1.el8_10.x86_64	lz4-1.8.3-5.el8_10.x86_64
kernel-4.18.0-553.60.1.el8_10.x86_64	lz4-libs-1.8.3-5.el8_10.i686
kernel-4.18.0-553.62.1.el8_10.x86_64	lz4-libs-1.8.3-5.el8_10.x86_64
kernel-4.18.0-553.63.1.el8_10.x86_64	microcode_ctl-4:20250512-1.el8_10.x86_64
kernel-4.18.0-553.64.1.el8_10.x86_64	pam-1.3.1-37.el8_10.x86_64
kernel-4.18.0-553.66.1.el8_10.x86_64	perl-Ermo-1.28-423.el8_10.x86_64
kernel-core-4.18.0-553.58.1.el8_10.x86_64	perl-IO-1.38-423.el8_10.x86_64
kernel-core-4.18.0-553.60.1.el8_10.x86_64	perl-Math-Complex-1.59-423.el8_10.noarch
kernel-core-4.18.0-553.62.1.el8_10.x86_64	perl-SelfLoader-1.23-423.el8_10.noarch
kernel-core-4.18.0-553.63.1.el8_10.x86_64	perl-interpreter-4:5.26.3-423.el8_10.x86_64
kernel-core-4.18.0-553.64.1.el8_10.x86_64	perl-libs-4:5.26.3-423.el8_10.x86_64
kernel-core-4.18.0-553.66.1.el8_10.x86_64	perl-macros-4:5.26.3-423.el8_10.x86_64
kernel-headers-4.18.0-553.58.1.el8_10.x86_64	platform-python-3.6.8-70.el8_10.x86_64
kernel-headers-4.18.0-553.60.1.el8_10.x86_64	platform-python-setuptools-39.2.0-9.el8_10.noarch
kernel-headers-4.18.0-553.62.1.el8_10.x86_64	python3-libs-3.6.8-70.el8_10.x86_64
kernel-headers-4.18.0-553.63.1.el8_10.x86_64	python3-libxml2-2.9.7-21.el8_10.1.x86_64
kernel-headers-4.18.0-553.64.1.el8_10.x86_64	python3-libxml2-2.9.7-21.el8_10.2.x86_64
kernel-headers-4.18.0-553.66.1.el8_10.x86_64	python3-libxml2-2.9.7-21.el8_10.3.x86_64
kernel-modules-4.18.0-553.58.1.el8_10.x86_64	python3-perf-4.18.0-553.58.1.el8_10.x86_64
kernel-modules-4.18.0-553.60.1.el8_10.x86_64	python3-perf-4.18.0-553.60.1.el8_10.x86_64

kernel-modules-4.18.0-553.62.1.el8_10.x86_64	python3-perf-4.18.0-553.62.1.el8_10.x86_64
kernel-modules-4.18.0-553.63.1.el8_10.x86_64	python3-perf-4.18.0-553.63.1.el8_10.x86_64
kernel-modules-4.18.0-553.64.1.el8_10.x86_64	python3-perf-4.18.0-553.64.1.el8_10.x86_64
kernel-modules-4.18.0-553.66.1.el8_10.x86_64	python3-perf-4.18.0-553.66.1.el8_10.x86_64
kernel-tools-4.18.0-553.58.1.el8_10.x86_64	python3-requests-2.20.0-6.el8_10.noarch
kernel-tools-4.18.0-553.60.1.el8_10.x86_64	python3-setuptools-39.2.0-9.el8_10.noarch
kernel-tools-4.18.0-553.62.1.el8_10.x86_64	python3-setuptools-wheel-39.2.0-9.el8_10.noarch
kernel-tools-4.18.0-553.63.1.el8_10.x86_64	python3-unbound-1.16.2-5.9.el8_10.x86_64
kernel-tools-4.18.0-553.64.1.el8_10.x86_64	sqlite-3.26.0-20.el8_10.x86_64
kernel-tools-4.18.0-553.66.1.el8_10.x86_64	sqlite-libs-3.26.0-20.el8_10.x86_64
kernel-tools-libs-4.18.0-553.58.1.el8_10.x86_64	sudo-1.9.5p2-1.el8_10.1.x86_64
kernel-tools-libs-4.18.0-553.60.1.el8_10.x86_64	unbound-libs-1.16.2-5.9.el8_10.x86_64

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #35 Sept 2025 release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
SMGR-78543	linux-pam	RHSA-2025:10027	CVE-2025-6020	Important
SMGR-78545	sudo	RHSA-2025:10110	CVE-2025-32462	Important
SMGR-78547	python	RHSA-2025:10128	CVE-2025-4435 CVE-2024-12718 CVE-2025-4330 CVE-2025-4517 CVE-2025-4138	Important
SMGR-78549	jq	RHSA-2025:10618	CVE-2024-23337 CVE-2025-48060	Moderate
SMGR-78551	kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:10669 RHSA-2025:11298 RHSA-2025:11455 RHSA-2025:11850 RHSA-2025:12752 RHSA-2025:9580	CVE-2022-49111 CVE-2022-49136 CVE-2022-49846 CVE-2022-49058 CVE-2024-58002 CVE-2024-57980 CVE-2025-21991 CVE-2025-22004 CVE-2025-23150 CVE-2025-37738 CVE-2022-49788 CVE-2024-50154 CVE-2025-38086 CVE-2025-21905 CVE-2025-21919 CVE-2022-49977 CVE-2025-21928 CVE-2025-22020 CVE-2025-37890 CVE-2025-38052 CVE-2025-38079 CVE-2022-50020 CVE-2022-48919 CVE-2024-50301 CVE-2024-53064 CVE-2025-21764	Important
SMGR-78553	libxml2	RHSA-2025:10698	CVE-2025-49794 CVE-2025-49796 CVE-2025-6021	Important

SMGR-78555	java-1.8.0-openjdk	RHSA-2025:10862	CVE-2025-30749 CVE-2025-30754 CVE-2025-30761 CVE-2025-50106	Important
SMGR-78557	microcode_ctl	RHSA-2025:10991	CVE-2024-28956	Moderate
SMGR-78559	emacs	RHSA-2025:11030	CVE-2024-53920	Moderate
SMGR-78561	lz4	RHSA-2025:11035	CVE-2019-17543	Moderate
SMGR-78563	python-setuptools	RHSA-2025:11036	CVE-2025-47273	Moderate
SMGR-78565	glib2	RHSA-2025:11327	CVE-2024-34397 CVE-2024-52533 CVE-2025-4373	Moderate
SMGR-78567	perl	RHSA-2025:11805	CVE-2025-40909	Moderate
SMGR-78569	unbound	RHSA-2025:11884	CVE-2025-5994	Important
SMGR-78571	sqlite	RHSA-2025:12010	CVE-2025-6965	Important
SMGR-78573	python3-libxml2	RHSA-2025:12450 RHSA-2025:13203	CVE-2025-7425 CVE-2025-32415	Important
SMGR-78575	glibc	RHSA-2025:12980	CVE-2025-8058	Moderate
SMGR-78577	python-requests	RHSA-2025:13234	CVE-2024-47081	Moderate
SMGR-78579	gdk-pixbuf2	RHSA-2025:13315	CVE-2025-7345	Moderate
SMGR-78581	libblockdev	RHSA-2025:9878	CVE-2025-6019	Important

SSP Patch #34 contains the fixes from the following previous patches:

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-008-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-010-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-011-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-012-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-014-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-015-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-017-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-018-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-019-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-020-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-022-05.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-023-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-024-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-025-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-026-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-027-01.tar.bz2

AV-SMGR10.1-RHEL8.4-SSP-028-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-029-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-030-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-031-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-032-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-033-05.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #34 July 2025 release includes the following rpm updates:

glibc-2.28-251.el8_10.22.i686	kernel-4.18.0-553.54.1.el8_10.x86_64
glibc-2.28-251.el8_10.22.x86_64	kernel-4.18.0-553.56.1.el8_10.x86_64
glibc-all-langpacks-2.28-251.el8_10.22.x86_64	kernel-core-4.18.0-553.54.1.el8_10.x86_64
glibc-common-2.28-251.el8_10.22.x86_64	kernel-core-4.18.0-553.56.1.el8_10.x86_64
glibc-devel-2.28-251.el8_10.22.x86_64	kernel-headers-4.18.0-553.54.1.el8_10.x86_64
glibc-headers-2.28-251.el8_10.22.x86_64	kernel-headers-4.18.0-553.56.1.el8_10.x86_64
glibc-langpack-en-2.28-251.el8_10.22.x86_64	kernel-modules-4.18.0-553.54.1.el8_10.x86_64
krb5-libs-1.18.2-32.el8_10.x86_64	kernel-modules-4.18.0-553.56.1.el8_10.x86_64
libxml2-2.9.7-20.el8_10.x86_64	kernel-tools-4.18.0-553.54.1.el8_10.x86_64
libxslt-1.1.32-6.2.el8_10.x86_64	kernel-tools-4.18.0-553.56.1.el8_10.x86_64
python3-libxml2-2.9.7-20.el8_10.x86_64	kernel-tools-libs-4.18.0-553.54.1.el8_10.x86_64
python3-perf-4.18.0-553.54.1.el8_10.x86_64	kernel-tools-libs-4.18.0-553.56.1.el8_10.x86_64
rsync-3.1.3-23.el8_10.x86_64	python3-perf-4.18.0-553.56.1.el8_10.x86_64
	python36-3.6.8-39.module+el8.10.0+20784+edafcd43.x86_64

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #34 July 2025 release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
SMGR-78385	kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:8246 RHSA-2025:8743	CVE-2024-43842, CVE-2022-49395	Moderate
SMGR-78388	rsync	RHSA-2025:8395	CVE-2016-9840	Low
SMGR-78390	kerberos	RHSA-2025:8411	CVE-2025-3576	Moderate
SMGR-78392	python	RHSA-2025:8419	CVE-2024-5629	Low
SMGR-78394	libxslt	RHSA-2025:8676	CVE-2023-40403	Moderate
SMGR-78396	glibc	RHSA-2025:8686	CVE-2025-4802	Moderate
SMGR-78398	libxml2	RHSA-2025:8958	CVE-2025-32414	Moderate

SSP Patch #33 contains the fixes from the following previous patches:

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2

AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-008-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-010-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-011-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-012-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-014-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-015-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-017-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-018-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-019-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-020-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-022-05.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-023-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-024-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-025-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-026-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-027-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-028-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-029-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-030-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-031-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-032-01.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #33 June 2025 release includes the following rpm updates:

expat-2.2.5-17.el8_10.x86_64	kernel-headers-4.18.0-553.46.1.el8_10.x86_64
freetype-2.9.1-10.el8_10.x86_64	kernel-headers-4.18.0-553.50.1.el8_10.x86_64
glibc-2.28-251.el8_10.16.i686	kernel-headers-4.18.0-553.52.1.el8_10.x86_64
glibc-2.28-251.el8_10.16.x86_64	kernel-headers-4.18.0-553.53.1.el8_10.x86_64
glibc-all-langpacks-2.28-251.el8_10.16.x86_64	kernel-modules-4.18.0-553.46.1.el8_10.x86_64
glibc-common-2.28-251.el8_10.16.x86_64	kernel-modules-4.18.0-553.50.1.el8_10.x86_64
glibc-devel-2.28-251.el8_10.16.x86_64	kernel-modules-4.18.0-553.52.1.el8_10.x86_64
glibc-headers-2.28-251.el8_10.16.x86_64	kernel-modules-4.18.0-553.53.1.el8_10.x86_64
glibc-langpack-en-2.28-251.el8_10.16.x86_64	kernel-tools-4.18.0-553.46.1.el8_10.x86_64
gnutls-3.6.16-8.el8_10.3.x86_64	kernel-tools-4.18.0-553.50.1.el8_10.x86_64
grub2-common-1:2.02-162.el8_10.noarch	kernel-tools-4.18.0-553.52.1.el8_10.x86_64
grub2-efi-x64-1:2.02-162.el8_10.x86_64	kernel-tools-4.18.0-553.53.1.el8_10.x86_64
grub2-tools-1:2.02-162.el8_10.x86_64	kernel-tools-libs-4.18.0-553.46.1.el8_10.x86_64
grub2-tools-extra-1:2.02-162.el8_10.x86_64	kernel-tools-libs-4.18.0-553.50.1.el8_10.x86_64
grub2-tools-minimal-1:2.02-162.el8_10.x86_64	kernel-tools-libs-4.18.0-553.52.1.el8_10.x86_64
java-1.8.0-openjdk-1:1.8.0.452.b09-2.el8.x86_64	kernel-tools-libs-4.18.0-553.53.1.el8_10.x86_64
java-1.8.0-openjdk-devel-1:1.8.0.452.b09-2.el8.x86_64	libjpeg-turbo-1.5.3-14.el8_10.x86_64
java-1.8.0-openjdk-headless-1:1.8.0.452.b09-2.el8.x86_64	libtasn1-4.13-5.el8_10.x86_64
kernel-4.18.0-553.46.1.el8_10.x86_64	libtiff-4.0.9-34.el8_10.x86_64
kernel-4.18.0-553.50.1.el8_10.x86_64	libxslt-1.1.32-6.1.el8_10.x86_64

kernel-4.18.0-553.52.1.el8_10.x86_64 kernel-4.18.0-553.53.1.el8_10.x86_64 kernel-core-4.18.0-553.46.1.el8_10.x86_64 kernel-core-4.18.0-553.50.1.el8_10.x86_64 kernel-core-4.18.0-553.52.1.el8_10.x86_64 kernel-core-4.18.0-553.53.1.el8_10.x86_64	python3-perf-4.18.0-553.46.1.el8_10.x86_64 python3-perf-4.18.0-553.50.1.el8_10.x86_64 python3-perf-4.18.0-553.52.1.el8_10.x86_64 python3-perf-4.18.0-553.53.1.el8_10.x86_64 tzdata-2025b-1.el8.noarch
--	---

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #33 June 2025 release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
SMGR-78213	kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:3260 RHSA-2025:3893 RHSA-2025:7531 RHSA-2025:8056	CVE-2025-21785, CVE-2024-53241, CVE-2024-53150, CVE-2022-49011, CVE-2024-53141, CVE-2024-40906, CVE-2024-44970, CVE-2025-21756	Important
SMGR-78215	grub2	RHSA-2025:3367	CVE-2025-0624	Important
SMGR-78217	freeType	RHSA-2025:3421	CVE-2025-27363	Important
SMGR-78219	libxslt	RHSA-2025:3615	CVE-2025-24855, CVE-2024-55549	Important
SMGR-78221	glibc	RHSA-2025:3828	CVE-2025-0395	Moderate
SMGR-78223	java	RHSA-2025:3845	CVE-2025-21587, CVE-2025-30691, CVE-2025-30698	Moderate
SMGR-78225	expat	RHSA-2025:3913	CVE-2024-8176	Moderate
SMGR-78227	xmlrpc-c	RHSA-2025:4048	CVE-2024-8176	Moderate
SMGR-78229	libtasn1	RHSA-2025:4049	CVE-2024-12133	Moderate
SMGR-78231	gnutls	RHSA-2025:4051	CVE-2024-12243	Moderate
SMGR-78233	libtiff	RHSA-2025:4658	CVE-2017-17095	Moderate
SMGR-78274	libjpeg-turbo	RHBA-2025:7540	CVE-2020-13790	Moderate
SMGR-78235	tzdata-2025b-1	RHBA-2025:3394	N/A	Bugfix

SSP Patch #32 contains the fixes from the following previous patches:

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-008-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-010-01.tar.bz2

AV-SMGR10.1-RHEL8.4-SSP-011-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-012-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-014-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-015-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-017-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-018-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-019-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-020-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-022-05.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-023-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-024-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-025-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-026-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-027-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-028-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-029-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-030-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-031-01.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #32 April 2025 release includes the following rpm updates:

bind-32:9.11.36-16.el8_10.4.x86_64	kernel-4.18.0-553.37.1.el8_10.x86_64
bind-export-libs-32:9.11.36-16.el8_10.4.x86_64	kernel-core-4.18.0-553.37.1.el8_10.x86_64
bind-libs-32:9.11.36-16.el8_10.4.x86_64	kernel-headers-4.18.0-553.37.1.el8_10.x86_64
bind-libs-lite-32:9.11.36-16.el8_10.4.x86_64	kernel-modules-4.18.0-553.37.1.el8_10.x86_64
bind-license-32:9.11.36-16.el8_10.4.noarch	kernel-tools-4.18.0-553.37.1.el8_10.x86_64
bind-utils-32:9.11.36-16.el8_10.4.x86_64	kernel-tools-libs-4.18.0-553.37.1.el8_10.x86_64
python3-bind-32:9.11.36-16.el8_10.4.noarch	python3-perf-4.18.0-553.37.1.el8_10.x86_64
bzip2-1.0.6-28.el8_10.x86_64	kernel-4.18.0-553.40.1.el8_10.x86_64
bzip2-libs-1.0.6-28.el8_10.x86_64	kernel-core-4.18.0-553.40.1.el8_10.x86_64
cpp-8.5.0-23.el8_10.x86_64	kernel-headers-4.18.0-553.40.1.el8_10.x86_64
emacs-filesystem-1:26.1-13.el8_10.noarch	kernel-modules-4.18.0-553.40.1.el8_10.x86_64
gcc-8.5.0-23.el8_10.x86_64	kernel-tools-4.18.0-553.40.1.el8_10.x86_64
gcc-gdb-plugin-8.5.0-23.el8_10.x86_64	kernel-tools-libs-4.18.0-553.40.1.el8_10.x86_64
libgcc-8.5.0-23.el8_10.i686	python3-perf-4.18.0-553.40.1.el8_10.x86_64
libgcc-8.5.0-23.el8_10.x86_64	kernel-4.18.0-553.44.1.el8_10.x86_64
libgomp-8.5.0-23.el8_10.x86_64	kernel-core-4.18.0-553.44.1.el8_10.x86_64
libstdc++-8.5.0-23.el8_10.i686	kernel-headers-4.18.0-553.44.1.el8_10.x86_64
libstdc++-8.5.0-23.el8_10.x86_64	kernel-modules-4.18.0-553.44.1.el8_10.x86_64
krb5-libs-1.18.2-31.el8_10.x86_64	kernel-tools-4.18.0-553.44.1.el8_10.x86_64
libpq-13.20-1.el8_10.x86_64	kernel-tools-libs-4.18.0-553.44.1.el8_10.x86_64
libxml2-2.9.7-18.el8_10.2.x86_64	python3-perf-4.18.0-553.44.1.el8_10.x86_64
python3-libxml2-2.9.7-18.el8_10.2.x86_64	kernel-4.18.0-553.45.1.el8_10.x86_64
libxml2-2.9.7-19.el8_10.x86_64	kernel-core-4.18.0-553.45.1.el8_10.x86_64
python3-libxml2-2.9.7-19.el8_10.x86_64	kernel-headers-4.18.0-553.45.1.el8_10.x86_64
python3-rpm-4.14.3-19.el8_5.2.x86_64	kernel-modules-4.18.0-553.45.1.el8_10.x86_64
rpm-4.14.3-19.el8_5.2.x86_64	kernel-tools-4.18.0-553.45.1.el8_10.x86_64
rpm-build-libs-4.14.3-19.el8_5.2.x86_64	kernel-tools-libs-4.18.0-553.45.1.el8_10.x86_64
rpm-libs-4.14.3-19.el8_5.2.x86_64	python3-perf-4.18.0-553.45.1.el8_10.x86_64

rpm-plugin-selinux-4.14.3-19.el8_5.2.x86_64 rpm-plugin-systemd-inhibit-4.14.3-19.el8_5.2.x86_64 python3-rpm-4.14.3-28.el8_9.x86_64 rpm-4.14.3-28.el8_9.x86_64 rpm-build-libs-4.14.3-28.el8_9.x86_64 rsync-3.1.3-21.el8_10.x86_64	rpm-libs-4.14.3-28.el8_9.x86_64 rpm-plugin-selinux-4.14.3-28.el8_9.x86_64 rpm-plugin-systemd-inhibit-4.14.3-28.el8_9.x86_64 python3-unbound-1.16.2-5.8.el8_10.x86_64 unbound-libs-1.16.2-5.8.el8_10.x86_64 tzdata-2025a-1.el8
---	--

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #32 April 2025 release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
SMGR-78031	rpm package manager	RHSA-2022:0368 RHSA-2024:0647	CVE-2021-3521, CVE-2021-35937, CVE-2021-35938, CVE-2021-35939	Moderate
SMGR-78032	bzip2	RHSA-2025:0733	CVE-2019-12900	Moderate
SMGR-78034	unbound-libs	RHSA-2025:0837	CVE-2024-1488, CVE-2024-8508	Important
SMGR-78036	gcc	RHSA-2025:1301	CVE-2020-11023	Moderate
SMGR-78039	libxml2	RHSA-2025:1517	CVE-2022-49043	Moderate
SMGR-78040	bind	RHSA-2025:1675	CVE-2024-11187	Important
SMGR-78042	libpq	RHSA-2025:1737	CVE-2025-1094	Important
SMGR-78044	gnu	RHSA-2025:1917	CVE-2025-1244	Important
SMGR-78046	rsync	RHSA-2025:2600	CVE-2024-12087, CVE-2024-12088, CVE-2024-12747	Moderate
SMGR-78048	libxml2	RHSA-2025:2686	CVE-2024-56171, CVE-2025-24928	Important
SMGR-78050	kerberos	RHSA-2025:2722	CVE-2025-24528	Moderate
SMGR-78052	kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:1068 RHSA-2025:1266 RHSA-2025:2473 RHSA-2025:3026	CVE-2024-26935, CVE-2024-50275, CVE-2024-53104, CVE-2024-50302, CVE-2024-53197, CVE-2024-57807, CVE-2024-57979, CVE-2023-52922	Important
SMGR-78185	tzdata-2025a-1	RHBA-2025:1104	N/A	Bugfix

SSP Patch #31 contains the fixes from the following previous patches:

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-008-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-010-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-011-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-012-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-014-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-015-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-017-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-018-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-019-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-020-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-022-05.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-023-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-024-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-025-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-026-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-027-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-028-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-029-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-030-01.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #31 February 2025 release includes the following rpm updates:

NetworkManager-1:1.40.16-18.el8_10.x86_64 NetworkManager-config-server-1:1.40.16-18.el8_10.noarch NetworkManager-libnm-1:1.40.16-18.el8_10.x86_64 NetworkManager-team-1:1.40.16-18.el8_10.x86_64 NetworkManager-tui-1:1.40.16-18.el8_10.x86_64 cups-libs-1:2.2.6-62.el8_10.x86_64 rsync-3.1.3-20.el8_10.x86_64 tuned-2.22.1-5.el8_10.noarch	kernel-4.18.0-553.34.1.el8_10.x86_64 kernel-core-4.18.0-553.34.1.el8_10.x86_64 kernel-headers-4.18.0-553.34.1.el8_10.x86_64 kernel-modules-4.18.0-553.34.1.el8_10.x86_64 kernel-tools-4.18.0-553.34.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.34.1.el8_10.x86_64 python3-perf-4.18.0-553.34.1.el8_10.x86_64 python3-requests-2.20.0-5.el8_10.noarch
--	---

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #31 February 2025 release:

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

SMGR-77735	rsync	RHSA-2025:0325	CVE-2024-12085	Important
SMGR-77718	tuned	RHSA-2024:11161	CVE-2024-52337	Moderate
SMGR-77721	python-request	RHSA-2025:0012	CVE-2024-35195	Moderate
SMGR-77726	kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:0065	CVE-2024-53088, CVE-2024-53122	Important
SMGR-77729	cups	RHSA-2025:0083	CVE-2024-47175	Low
SMGR-77732	NetworkManager	RHSA-2025:0288	CVE-2024-3661	Moderate

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

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-008-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-010-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-011-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-012-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-014-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-015-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-017-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-018-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-019-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-020-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-022-05.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-023-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-024-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-025-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-026-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-027-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-028-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-029-01.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #30 January 2025 release includes the following rpm updates:

rsync-3.1.3-19.el8_7.1.x86_64 dbus-1:1.12.8-23.el8_7.1.x86_64 kernel-4.18.0-553.32.1.el8_10.x86_64 kernel-core-4.18.0-553.32.1.el8_10.x86_64 kernel-headers-4.18.0-553.32.1.el8_10.x86_64 kernel-modules-4.18.0-553.32.1.el8_10.x86_64 kernel-tools-4.18.0-553.32.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.32.1.el8_10.x86_64	openldap-2.4.46-20.el8_10.x86_64 python3-perf-4.18.0-553.32.1.el8_10.x86_64 pam-1.3.1-36.el8_10.x86_64 platform-python-3.6.8-69.el8_10.x86_64 python3-libs-3.6.8-69.el8_10.x86_64 python36-3.6.8-39.module+el8.10.0+20784+edafcd43.x86_64
--	--

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #30 January 2025 release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
SMGR-77592	rsync	RHSA-2022:7793	CVE-2022-37434	Moderate
SMGR-77589	dbus	RHSA-2023:0096	CVE-2022-42010, CVE-2022-42011, CVE-2022-42012	Moderate
SMGR-77583	kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2024:10943	CVE-2024-46695, CVE-2024-49949, CVE-2024-50082, CVE-2024-50099, CVE-2024-50110, CVE-2024-50142, CVE-2024-50192, CVE-2024-50256, CVE-2024-50264	Moderate
SMGR-77586	openldap	RHSA-2024:6033	CVE-2023-2953	Low
SMGR-77580	platform-python python3-libs	RHSA-2024:10779 RHSA-2024:10953	CVE-2024-9287, CVE-2024-11168, CVE-2024-53899	Moderate
SMGR-77577	pam	RHSA-2024:10379	CVE-2024-10041, CVE-2024-10963	Low

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

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-008-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-010-01.tar.bz2

AV-SMGR10.1-RHEL8.4-SSP-011-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-012-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-014-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-015-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-017-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-018-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-019-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-020-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-022-05.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-023-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-024-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-025-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-026-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-027-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-028-01.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #29 December 2024 release includes the following rpm updates:

binutils-2.30-125.el8_10.x86_64 bzip2-1.0.6-27.el8_10.x86_64 bzip2-libs-1.0.6-27.el8_10.x86_64 emacs-filesystem-26.1-12.el8_10.noarch expat-2.2.5-16.el8_10.x86_64 gmp-6.1.2-11.el8_6.x86_64 grub2-tools-efi-2.02-156.el8.x86_64 gtk-update-icon-cache-3.22.30-12.el8_10.x86_64 java-1.8.0-openjdk-1.8.0.432.b06-2.el8.x86_64 java-1.8.0-openjdk-devel-1.8.0.432.b06-2.el8.x86_64 java-1.8.0-openjdk-headless-1.8.0.432.b06-2.el8.x86_64 kernel-4.18.0-553.27.1.el8_10.x86_64 kernel-core-4.18.0-553.27.1.el8_10.x86_64 kernel-headers-4.18.0-553.27.1.el8_10.x86_64 kernel-modules-4.18.0-553.27.1.el8_10.x86_64 kernel-tools-4.18.0-553.27.1.el8_10.x86_64	kernel-tools-libs-4.18.0-553.27.1.el8_10.x86_64 krb5-libs-1.18.2-30.el8_10.x86_64 libtiff-4.0.9-33.el8_10.x86_64 linux-firmware-20240827-124.git3cff7109.el8_10.noarch nano-2.9.8-3.el8_10.x86_64 openssl-1.1.1k-14.el8_6.x86_64 openssl-libs-1.1.1k-14.el8_6.x86_64 platform-python-3.6.8-67.el8_10.x86_64 protobuf-c-1.3.0-8.el8_6.x86_64 python3-libs-3.6.8-67.el8_10.x86_64 python3-perf-4.18.0-553.27.1.el8_10.x86_64 tpm2-tss-2.3.2-5.el8_6.x86_64 tzdata-2024b-4.el8.noarch tzdata-java-2024b-4.el8.noarch xmlrpc-c-1.51.0-10.el8_10.x86_64 xmlrpc-c-client-1.51.0-10.el8_10.x86_64
---	---

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #29 December 2024 release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
SMGR-77381	openssl	RHSA-2024:7848 RHSA-2024:7846	CVE-2024-5535	Important
SMGR-77428	platform-python python3-libs	RHSA-2024:6975	CVE-2024-4032, CVE-2024-6923, CVE-2024-6232	Moderate
SMGR-77429	kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2024:8856 RHSA-2024:7000	CVE-2024-24857, CVE-2023-52492, CVE-2024-26851, CVE-2024-26924, CVE-2024-27017, CVE-2024-26976, CVE-2024-27062, CVE-2024-35839, CVE-2024-35898, CVE-2024-35939, CVE-2024-38608, CVE-2024-38586, CVE-2024-38541, CVE-2024-38540, CVE-2024-39503, CVE-2024-40924, CVE-2024-40961, CVE-2024-40983, CVE-2024-40984, CVE-2022-48773, CVE-2024-41009, CVE-2024-41042, CVE-2024-41066, CVE-2024-41092, CVE-2024-41093, CVE-2024-42070, CVE-2024-42079, CVE-2024-42244, CVE-2024-42284, CVE-2024-42292, CVE-2024-42301, CVE-2024-43854, CVE-2024-43880, CVE-2022-48936, CVE-2024-43889, CVE-2024-43892, CVE-2024-44935, CVE-2024-44989, CVE-2024-44990, CVE-2024-45018, CVE-2024-46826, CVE-2024-47668, CVE-2023-6040, CVE-2024-26595, CVE-2024-26600, CVE-2021-46984,	Important

			CVE-2023-52478, CVE-2023-52476, CVE-2023-52522, CVE-2021-47101, CVE-2021-47097, CVE-2023-52605, CVE-2024-26638, CVE-2024-26645, CVE-2024-26665, CVE-2024-26720, CVE-2024-26717, CVE-2024-26769, CVE-2024-26846, CVE-2024-26894, CVE-2024-26880, CVE-2024-26855, CVE-2024-26923, CVE-2024-26939, CVE-2024-27013, CVE-2024-27042, CVE-2024-35809, CVE-2023-52683, CVE-2024-35884, CVE-2024-35877, CVE-2024-35944, CVE-2024-35989, CVE-2021-47412, CVE-2021-47393, CVE-2021-47386, CVE-2021-47385, CVE-2021-47384, CVE-2021-47383, CVE-2021-47432, CVE-2021-47352, CVE-2021-47338, CVE-2021-47321, CVE-2021-47289, CVE-2021-47287, CVE-2023-52798, CVE-2023-52809, CVE-2023-52817, CVE-2023-52840, CVE-2023-52800, CVE-2021-47441, CVE-2021-47466, CVE-2021-47455, CVE-2021-47497, CVE-2021-47560, CVE-2021-47527, CVE-2024-36883, CVE-2024-36922, CVE-2024-36920, CVE-2024-36902, CVE-2024-36953, CVE-2024-36939, CVE-2024-36919, CVE-2024-36901, CVE-2021-47582, CVE-2021-47609,	
--	--	--	---	--

			CVE-2024-38619, CVE-2022-48754, CVE-2022-48760, CVE-2024-38581, CVE-2024-38579, CVE-2024-38570, CVE-2024-38559, CVE-2024-38558, CVE-2024-37356, CVE-2024-39471, CVE-2024-39499, CVE-2024-39501, CVE-2024-39506, CVE-2024-40904, CVE-2024-40911, CVE-2024-40912, CVE-2024-40929, CVE-2024-40931, CVE-2024-40941, CVE-2024-40954, CVE-2024-40958, CVE-2024-40959, CVE-2024-40960, CVE-2024-40972, CVE-2024-40977, CVE-2024-40978, CVE-2024-40988, CVE-2024-40989, CVE-2024-40995, CVE-2024-40997, CVE-2024-40998, CVE-2024-41005, CVE-2024-40901, CVE-2024-41007, CVE-2024-41008, CVE-2022-48804, CVE-2022-48836, CVE-2022-48866, CVE-2024-41090, CVE-2024-41091, CVE-2024-41012, CVE-2024-41013, CVE-2024-41014, CVE-2024-41023, CVE-2024-41035, CVE-2024-41038, CVE-2024-41039, CVE-2024-41040, CVE-2024-41041, CVE-2024-41044, CVE-2024-41055, CVE-2024-41056, CVE-2024-41060, CVE-2024-41064, CVE-2024-41065, CVE-2024-41071, CVE-2024-41076, CVE-2024-41097, CVE-2024-42084,	
--	--	--	---	--

			CVE-2024-42090, CVE-2024-42094, CVE-2024-42096, CVE-2024-42114, CVE-2024-42124, CVE-2024-42131, CVE-2024-42152, CVE-2024-42154, CVE-2024-42225, CVE-2024-42226, CVE-2024-42228, CVE-2024-42237, CVE-2024-42238, CVE-2024-42240, CVE-2024-42246, CVE-2024-42322, CVE-2024-43830, CVE-2024-43871	
SMGR-77430	java-1.8.0-openjdk java-1.8.0-openjdk-devel java-1.8.0-openjdk-headless	RHSA-2024:8117	CVE-2024-21210, CVE-2024-21208, CVE-2024-21217, CVE-2024-21235	Moderate
SMGR-77451	grub2	RHSA-2024:3184	CVE-2024-1048, CVE-2023-4692, CVE-2023-4693	Moderate
SMGR-77455	gtk3	RHSA-2024:6963	CVE-2024-6655	Moderate
SMGR-77457	nano	RHSA-2024:6986	CVE-2024-5742	Low
SMGR-77459	emacs	RHSA-2024:6987	CVE-2024-30203, CVE-2024-30205, CVE-2024-39331	Important
SMGR-77461	linux-firmware	RHSA-2024:7481	CVE-2023-20584, CVE-2023-31356	Important
SMGR-77463	tzdata	RHBA-2024:8805	N/A	Low
SMGR-77465	libtiff	RHSA-2024:8833	CVE-2024-7006	Moderate
SMGR-77468	xmlrpc-c	RHSA-2024:8859	CVE-2024-45491	Moderate
SMGR-77470	krb5	RHSA-2024:8860	CVE-2024-3596	Important
SMGR-77472	bzip2	RHSA-2024:8922	CVE-2019-12900	Low
SMGR-77474	expat	RHSA-2024:6989	CVE-2024-50602 CVE-2024-45490, CVE-2024-45491, CVE-2024-45492	Moderate
SMGR-77476	binutils	RHSA-2024:9689	CVE-2018-12699	Low

SMGR-77574	gmp	RHSA-2024:1102	CVE-2021-43618	Moderate
SMGR-77573	protobuf-c	RHSA-2024:0406	CVE-2022-48468	Moderate
SMGR-77572	tpm2-tss	RHSA-2024:4408	CVE-2023-22745	Moderate

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

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-008-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-010-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-011-02.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-012-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-014-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-015-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-017-03.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-018-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-019-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-020-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-022-05.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-023-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-024-02.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-025-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-026-03.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-027-01.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #28 October 2024 release includes the following rpm updates:

bubblewrap-0.4.0-2.el8_10.x86_64.rpm	
--------------------------------------	--

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #28 October 2024 release:

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

SMGR-77044	bubblewrap	RHSA-2024:6422	CVE-2024-42472	Important
------------	------------	----------------	----------------	-----------

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

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-008-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-010-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-011-02.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-012-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-014-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-015-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-017-03.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-018-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-019-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-020-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-022-05.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-023-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-024-02.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-025-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-026-03.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #27 September 2024 release includes the following rpm updates:

jose-10-2.el8_10.3.x86_64 libjose-10-2.el8_10.3.x86_64 wget-1.19.5-12.el8_10.x86_64 python3-urllib3-1.24.2-8.el8_10.noarch krb5-libs-1.18.2-29.el8_10.x86_64 bind-32:9.11.36-16.el8_10.2.x86_64 bind-export-libs-32:9.11.36-16.el8_10.2.x86_64 bind-libs-32:9.11.36-16.el8_10.2.x86_64 bind-libs-lite-32:9.11.36-16.el8_10.2.x86_64	bind-license-32:9.11.36-16.el8_10.2.noarch bind-utils-32:9.11.36-16.el8_10.2.x86_64 python3-bind-32:9.11.36-16.el8_10.2.noarch platform-python-setuptools-39.2.0-8.el8_10.noarch python3-setuptools-39.2.0-8.el8_10.noarch python3-setuptools-wheel-39.2.0-8.el8_10.noarch curl-7.61.1-34.el8_10.2.x86_64 libcurl-7.61.1-34.el8_10.2.x86_64
---	--

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #27 September 2024 release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
SMGR-76934	jose libjose	RHSA-2024:5294	CVE-2024-28176, CVE-2023-50967	Moderate
SMGR-76937	Wget	RHSA-2024:5299	CVE-2024-38428	Moderate
SMGR-76940	python3-urllib3	RHSA-2024:5309	CVE-2024-37891	Moderate
SMGR-76943	krb5-libs	RHSA-2024:5312	CVE-2024-37370, CVE-2024-37371	Moderate
SMGR-76946	bind bind-export-libs bind-libs bind-libs-lite bind-license bind-utils python3-bind	RHSA-2024:5524	CVE-2024-1737, CVE-2024-1975	Important
SMGR-76949	platform-python- setuptools python3-setuptools python3-setuptools- wheel	RHSA-2024:5530	CVE-2024-6345	Important
SMGR-76952	curl libcurl	RHSA-2024:5654	CVE-2024-2398	Moderate

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

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-008-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-010-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-011-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-012-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-014-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-015-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-017-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-018-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-019-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-020-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2

AV-SMGR10.1-RHEL8.4-SSP-022-05.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-023-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-024-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-025-01.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #26 release includes the following rpm updates:

c-ares-1.13.0-11.el8_10.x86_64 cups-libs-1:2.2.6-60.el8_10.x86_64 kernel-4.18.0-553.16.1.el8_10.x86_64 kernel-core-4.18.0-553.16.1.el8_10.x86_64 kernel-headers-4.18.0-553.16.1.el8_10.x86_64 kernel-modules-4.18.0-553.16.1.el8_10.x86_64 kernel-tools-4.18.0-553.16.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.16.1.el8_10.x86_64 less-530-3.el8_10.x86_64 libnghttp2-1.33.0-6.el8_10.1.x86_64 linux-firmware-20240610-122.git90df68d2.el8_10.noarch	openldap-2.4.46-19.el8_10.x86_64 python3-idna-2.5-7.el8_10.noarch python3-perf-4.18.0-553.8.1.el8_10.x86_64 xmlrpc-c-1.51.0-9.el8_10.x86_64 xmlrpc-c-client-1.51.0-9.el8_10.x86_64 java-1.8.0-openjdk-1:1.8.0.422.b05-2.el8.x86_64 java-1.8.0-openjdk-devel-1:1.8.0.422.b05-2.el8.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.422.b05-2.el8.x86_64 libndp-1.7-7.el8_10.x86_64 libtiff-4.0.9-32.el8_10.x86_64 python3-perf-4.18.0-553.16.1.el8_10.x86_64
--	--

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #26 release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
SMGR-76096 SMGR-76799	kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2024:4211 RHSA-2024:5101	CVE-2020-26555, CVE-2023-52881, CVE-2021-46972, CVE-2021-47073, CVE-2024-35890, CVE-2024-26584, CVE-2024-26583, CVE-2024-26585, CVE-2024-35789, CVE-2024-27410, CVE-2024-35838, CVE-2024-35845, CVE-2024-35855, CVE-2024-35854, CVE-2024-35853, CVE-2024-35852, CVE-2024-36007, CVE-2021-46909, CVE-2021-47069, CVE-2023-52615, CVE-2023-52626, CVE-2024-35835, CVE-2023-52667, CVE-2024-35959, CVE-2024-26656, CVE-2024-26801, CVE-2024-26982, CVE-2024-27397,	Important

			CVE-2023-52560, CVE-2024-26675, CVE-2024-26759, CVE-2024-26906, CVE-2023-52700, CVE-2024-26907, CVE-2024-35888, CVE-2023-52675, CVE-2023-52686, CVE-2023-5090, CVE-2023-52464, CVE-2024-26735, CVE-2024-26826, CVE-2024-26974, CVE-2023-52669, CVE-2023-52813, CVE-2024-35960, CVE-2024-35958, CVE-2021-47310, CVE-2024-26804, CVE-2021-47311, CVE-2024-26859, CVE-2021-47236, CVE-2023-52703, CVE-2024-36004, CVE-2023-52835, CVE-2023-52781, CVE-2023-52877, CVE-2021-47495, CVE-2023-52878, CVE-2021-47456, CVE-2021-47356, CVE-2021-47353, CVE-2023-52451, CVE-2023-52463, CVE-2021-46939, CVE-2023-52622, CVE-2024-26669, CVE-2024-26802, CVE-2024-26843, CVE-2024-26878, CVE-2024-36886, CVE-2023-52653, CVE-2024-21823, CVE-2023-52658, CVE-2024-35807, CVE-2024-35801, CVE-2024-35947, CVE-2024-35893, CVE-2024-35876, CVE-2023-52864, CVE-2023-52845, CVE-2023-28746, CVE-2023-52847, CVE-2021-47548, CVE-2024-36921, CVE-2024-26921, CVE-2021-47579, CVE-2024-36927,	
--	--	--	--	--

			CVE-2024-39276, CVE-2024-33621, CVE-2024-27010, CVE-2024-26960, CVE-2024-38596, CVE-2022-48743, CVE-2024-26733, CVE-2024-26586, CVE-2024-26698, CVE-2023-52619	
SMGR-76099	c-ares	RHSA-2024:4249	CVE-2024-25629	Low
SMGR-76796	libtiff	RHSA-2024:5079	CVE-2018-15209, CVE-2023-25433, CVE-2023-6228, CVE-2023-52356	Moderate
SMGR-76114	linux-firmware	RHSA-2024:4262	CVE-2023-31346	Moderate
SMGR-76102	libnghttp2	RHSA-2024:4252	CVE-2024-28182	Moderate
SMGR-76105	less	RHSA-2024:4256	CVE-2024-32487, CVE-2022-48624	Important
SMGR-76108	xmlrpc-c xmlrpc-c-client	RHSA-2024:4259	CVE-2023-52425	Moderate
SMGR-76111	python3-idna	RHSA-2024:4260	CVE-2024-3651	Moderate
SMGR-76117	openldap	RHSA-2024:4264	CVE-2023-2953	Low
SMGR-76120	cups-libs	RHSA-2024:4265	CVE-2024-35235	Moderate
SMGR-76793	libndp	RHSA-2024:4620	CVE-2024-5564	Important
SMGR-76790	java-1.8.0-openjdk java-1.8.0-openjdk-devel java-1.8.0-openjdk-headless	RHSA-2024:4563	CVE-2024-21147, CVE-2024-21131, CVE-2024-21138, CVE-2024-21140, CVE-2024-21145	Important

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

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-008-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-010-01.tar.bz2

AV-SMGR10.1-RHEL8.4-SSP-011-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-012-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-014-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-015-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-017-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-018-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-019-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-020-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-022-05.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-023-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-024-02.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #25 release includes the following rpm updates:

bind-32:9.11.36-14.el8_10.x86_64	kernel-tools-4.18.0-553.5.1.el8_10.x86_64
bind-export-libs-32:9.11.36-14.el8_10.x86_64	kernel-tools-4.18.0-553.el8_10.x86_64
bind-libs-32:9.11.36-14.el8_10.x86_64	kernel-tools-libs-4.18.0-553.5.1.el8_10.x86_64
bind-libs-lite-32:9.11.36-14.el8_10.x86_64	kernel-tools-libs-4.18.0-553.el8_10.x86_64
bind-license-32:9.11.36-14.el8_10.noarch	krb5-libs-1.18.2-27.el8_10.x86_64
bind-utils-32:9.11.36-14.el8_10.x86_64	libX11-1.6.8-8.el8.x86_64
dhcp-client-12:4.3.6-50.el8_10.x86_64	libX11-common-1.6.8-8.el8.noarch
dhcp-common-12:4.3.6-50.el8_10.noarch	libssh-0.9.6-14.el8.x86_64
dhcp-libs-12:4.3.6-50.el8_10.x86_64	libssh-config-0.9.6-14.el8.noarch
gdk-pixbuf2-2.36.12-6.el8_10.x86_64	libsss_idmap-2.9.4-3.el8_10.x86_64
gdk-pixbuf2-modules-2.36.12-6.el8_10.x86_64	libsss_nss_idmap-2.9.4-3.el8_10.x86_64
glibc-2.28-251.el8_10.i686	libtiff-4.0.9-31.el8.x86_64
glibc-2.28-251.el8_10.i686	libxml2-2.9.7-18.el8_10.i686
glibc-2.28-251.el8_10.i686	linux-firmware-20240111-121.gitb3132c18.el8.noarch
glibc-2.28-251.el8_10.x86_64	openssh-8.0p1-24.el8.x86_64
glibc-all-langpacks-2.28-251.el8_10.i686	openssh-askpass-8.0p1-24.el8.x86_64
glibc-all-langpacks-2.28-251.el8_10.x86_64	openssh-clients-8.0p1-24.el8.x86_64
glibc-common-2.28-251.el8_10.i686	openssh-server-8.0p1-24.el8.x86_64
glibc-common-2.28-251.el8_10.x86_64	pam-1.3.1-33.el8.x86_64
glibc-devel-2.28-251.el8_10.i686	platform-python-3.6.8-62.el8_10.x86_64
glibc-devel-2.28-251.el8_10.x86_64	python2-2.7.18-17.module+el8.10.0+20822+a15ec22d.x86_64
glibc-headers-2.28-251.el8_10.i686	python2-libs-2.7.18-17.module+el8.10.0+20822+a15ec22d.x86_64
glibc-headers-2.28-251.el8_10.x86_64	python2-pip-9.0.3-19.module+el8.9.0+19487+7dc18407.noarch
glibc-langpack-en-2.28-251.el8_10.i686	python2-pip-wheel-9.0.3-19.module+el8.9.0+19487+7dc18407.noarch
glibc-langpack-en-2.28-251.el8_10.x86_64	python2-setuptools-39.0.1-14.module+el8.10.0+20444+3bf7fee4.noarch
gmp-1:6.1.2-11.el8.x86_64	python2-setuptools-wheel-39.0.1-14.module+el8.10.0+20444+3bf7fee4.noarch
grub2-common-1:2.02-156.el8.noarch	python3-bind-32:9.11.36-14.el8_10.noarch
grub2-efi-x64-1:2.02-156.el8.x86_64	python3-libs-3.6.8-62.el8_10.x86_64
grub2-tools-1:2.02-156.el8.x86_64	python3-libxml2-2.9.7-18.el8_10.i686
grub2-tools-extra-1:2.02-156.el8.x86_64	python3-perf-4.18.0-553.5.1.el8_10.x86_64
grub2-tools-minimal-1:2.02-156.el8.x86_64	python3-perf-4.18.0-553.el8_10.x86_64
harfbuzz-1.7.5-4.el8.x86_64	squashfs-tools-4.3-21.el8.x86_64
kernel-4.18.0-553.5.1.el8_10.x86_64	sssd-client-2.9.4-3.el8_10.x86_64
kernel-4.18.0-553.el8_10.x86_64	systemd-239-82.el8.x86_64
kernel-core-4.18.0-553.5.1.el8_10.x86_64	
kernel-core-4.18.0-553.el8_10.x86_64	

kernel-headers-4.18.0-553.5.1.el8_10.x86_64 kernel-headers-4.18.0-553.el8_10.x86_64 kernel-modules-4.18.0-553.5.1.el8_10.x86_64 kernel-modules-4.18.0-553.el8_10.x86_64	systemd-libs-239-82.el8.i686 systemd-libs-239-82.el8.x86_64 systemd-pam-239-82.el8.x86_64 systemd-udev-239-82.el8.x86_64 traceroute-3:2.1.0-8.el8.x86_64
--	--

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #25 release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
SMGR-75855	libX11 libX11-common	RHSA-2024:2973	CVE-2023-43785 CVE-2023-43786 CVE-2023-43787	Moderate
SMGR-75858	harfbuzz	RHSA-2024:2980	CVE-2023-25193	Moderate
SMGR-75861	python2 python2-libs python2-pip python2-pip-wheel python2-setuptools python2-setuptools-wheel	RHSA-2024:2987	CVE-2022-40897 CVE-2022-48560 CVE-2022-48565 CVE-2023-43804 CVE-2024-22195	Moderate
SMGR-75864	libtiff	RHSA-2024:3059	CVE-2022-4645	Moderate
SMGR-75867 SMGR-75918	kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2024:3138 RHSA-2024:3618	CVE-2021-40153 CVE-2021-41072 CVE-2023-6240 CVE-2024-0340 CVE-2024-25744 CVE-2024-26593 CVE-2023-52445 CVE-2024-26603 CVE-2019-25162 CVE-2021-46934 CVE-2020-36777 CVE-2023-52477 CVE-2021-47055 CVE-2024-26615 CVE-2022-48627 CVE-2024-23307 CVE-2023-52565 CVE-2023-52578 CVE-2023-52528 CVE-2023-52520 CVE-2023-52513 CVE-2021-47118 CVE-2023-52610 CVE-2024-26643 CVE-2024-26642 CVE-2021-47153 CVE-2024-26659 CVE-2024-26664	Moderate

			CVE-2024-26779 CVE-2024-26744 CVE-2024-26743 CVE-2021-47185 CVE-2024-26901 CVE-2024-26872 CVE-2024-26919 CVE-2024-26964 CVE-2024-26934 CVE-2024-26933 CVE-2024-26993 CVE-2024-26973 CVE-2024-27059 CVE-2021-47013 CVE-2021-47171 CVE-2022-48669 CVE-2023-52439 CVE-2023-52594 CVE-2023-52595	
SMGR-75870	squashfs-tools	RHSA-2024:3139	CVE-2021-40153 CVE-2021-41072	Moderate
SMGR-75873	pam	RHSA-2024:3163	CVE-2024-22365	Moderate
SMGR-75876	openssh openssh-askpass openssh-clients openssh-server	RHSA-2024:3166	CVE-2020-15778	Moderate
SMGR-75879	linux-firmware	RHSA-2024:3178	CVE-2022-46329 CVE-2023-20592	Important
SMGR-75882	grub2-common grub2-efi-x64 grub2-tools grub2-tools-extra grub2-tools-minimal	RHSA-2024:3184	CVE-2024-1048 CVE-2023-4692 CVE-2023-4693	Moderate
SMGR-75885	systemd systemd-libs systemd-pam systemd-udev	RHSA-2024:3203	CVE-2023-7008	Moderate
SMGR-75888	traceroute	RHSA-2024:3211	CVE-2023-46316	Moderate
SMGR-75891	gmp	RHSA-2024:3214	CVE-2021-43618	Moderate
SMGR-75894	libssh libssh-config	RHSA-2024:3233	CVE-2023-6004 CVE-2023-6918	Low
SMGR-75897	krb5-libs	RHSA-2024:3268	CVE-2024-26458 CVE-2024-26461	Low
SMGR-75900 SMGR-75912	glibc glibc-all-langpacks glibc-common glibc-devel glibc-headers glibc-langpack-en	RHSA-2024:3269 RHSA-2024:3344	CVE-2024-2961 CVE-2024-33599 CVE-2024-33600 CVE-2024-33601 CVE-2024-33602	Important

SMGR-75903	libsss_idmap libsss_nss_idmap sssd-client	RHSA-2024:3270	CVE-2023-3758	Moderate
SMGR-75906	bind bind-export-libs bind-libs bind-libs-lite bind-license bind-utils python3-bind dhcp-client dhcp-common dhcp-libs	RHSA-2024:3271	CVE-2023-4408 CVE-2023-50387 CVE-2023-50868	Important
SMGR-75909	gdk-pixbuf2 gdk-pixbuf2-modules	RHSA-2024:3341	CVE-2022-48622	Moderate
SMGR-75915	platform-python python3-libs	RHSA-2024:3347	CVE-2023-6597 CVE-2024-0450	Important
SMGR-75921	libxml2 python3-libxml2	RHSA-2024:3626	CVE-2024-25062	Moderate

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

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-008-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-010-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-011-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-012-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-014-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-015-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-017-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-018-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-019-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-020-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-022-05.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-023-01.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #24 release includes the following rpm updates:

bind-32:9.11.36-11.el8 9.1.x86_64	gnutls-3.6.16-8.el8 9.3.x86_64.rpm
-----------------------------------	------------------------------------

bind-export-libs-32:9.11.36-11.el8_9.1.x86_64 bind-libs-32:9.11.36-11.el8_9.1.x86_64 bind-libs-lite-32:9.11.36-11.el8_9.1.x86_64 bind-license-32:9.11.36-11.el8_9.1.noarch bind-utils-32:9.11.36-11.el8_9.1.x86_64 curl-7.61.1-33.el8_9.5.x86_64 dhcp-client-12:4.3.6-49.el8_9.1.x86_64 dhcp-common-12:4.3.6-49.el8_9.1.noarch dhcp-libs-12:4.3.6-49.el8_9.1.x86_64.rpm expat-2.2.5-11.el8_9.1.x86_64.rpm glibc-2.28-236.el8_9.13.i686.rpm glibc-2.28-236.el8_9.13.x86_64.rpm glibc-all-langpacks-2.28-236.el8_9.13.x86_64.rpm glibc-common-2.28-236.el8_9.13.x86_64.rpm glibc-devel-2.28-236.el8_9.13.x86_64.rpm glibc-headers-2.28-236.el8_9.13.x86_64.rpm glibc-langpack-en-2.28-236.el8_9.13.x86_64.rpm	java-1.8.0-openjdk-1:1.8.0.412.b08-2.el8.x86_64.rpm java-1.8.0-openjdk-devel-1:1.8.0.412.b08-2.el8.x86_64.rpm java-1.8.0-openjdk-headless-1:1.8.0.412.b08-2.el8.x86_64.rpm kernel-4.18.0-513.24.1.el8_9.x86_64.rpm kernel-core-4.18.0-513.24.1.el8_9.x86_64.rpm kernel-headers-4.18.0-513.24.1.el8_9.x86_64.rpm kernel-modules-4.18.0-513.24.1.el8_9.x86_64.rpm kernel-tools-4.18.0-513.24.1.el8_9.x86_64.rpm kernel-tools-libs-4.18.0-513.24.1.el8_9.x86_64.rpm less-530-2.el8_9.x86_64.rpm libcurl-7.61.1-33.el8_9.5.x86_64.rpm python3-bind-32:9.11.36-11.el8_9.1.noarch.rpm python3-perf-4.18.0-513.24.1.el8_9.x86_64.rpm python3-unbound-1.16.2-5.el8_9.6.x86_64.rpm shim-x64-15.8-4.el8_9.x86_64.rpm unbound-libs-1.16.2-5.el8_9.6.x86_64.rpm
---	--

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #24 release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
SMGR-75536	curl bind-export-libs	RHSA-2024:1601	CVE-2023-46218 CVE-2023-28322 CVE-2023-38546	Moderate
SMGR-75539	kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2024:1607	CVE-2022-38096 CVE-2023-6931 CVE-2023-6546 ZDI-CAN-20527 CVE-2024-0565 CVE-2023-51042 CVE-2021-33631 CVE-2024-1086	Important
SMGR-75542	less	RHSA-2024:1610	CVE-2022-48624	Moderate
SMGR-75545	expat	RHSA-2024:1615	CVE-2023-52425	Moderate
SMGR-75548	python3-unbound unbound-libs	RHSA-2024:1751	CVE-2024-1488	Important
SMGR-75551	bind bind-export-libs bind-libs bind-libs-lite bind-license bind-utils python3-bind dhcp-client dhcp-common dhcp-libs	RHSA-2024:1782	CVE-2023-4408 CVE-2023-50387 CVE-2023-50868	Important
SMGR-75554	gnutls	RHSA-2024:1784	CVE-2024-28834	Moderate

SMGR-75557	java-1.8.0-8.0-openjdk java-1.8.0-openjdk-devel java-1.8.0-openjdk-headless	RHSA-2024:1818	CVE-2024-21011 CVE-2024-21068 CVE-2024-21085 CVE-2024-21094	Moderate
SMGR-75560	shim-x64	RHSA-2024:1902	CVE-2023-40546 CVE-2023-40547 CVE-2023-40548 CVE-2023-40549 CVE-2023-40550 CVE-2023-40551	Important
SMGR-75563	glibc glibc-all-langpacks glibc-common glibc-devel glibc-headers glibc-langpack-en	RHSA-2024:2722	CVE-2024-2961	Important

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

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-008-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-010-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-011-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-012-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-014-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-015-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-017-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-018-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-019-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-020-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-022-05.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #23 release includes the following rpm updates:

python3-unbound-1.16.2-5.el8_9.2.x86_64.rpm	unbound-libs-1.16.2-5.el8_9.2.x86_64.rpm
---	--

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #23 release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
SMGR-75125	python3-unbound	RHSA-2024:0965	CVE-2023-50387 CVE-2023-50868	Important

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

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-008-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-010-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-011-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-012-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-014-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-015-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-017-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-018-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-019-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-020-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-021-01.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #22 release includes the following rpm updates:

gnutls-3.6.16-8.el8_9.1.x86_64.rpm java-1.8.0-openjdk-1:1.8.0.402.b06-2.el8.x86_64.rpm java-1.8.0-openjdk-devel-1:1.8.0.402.b06-2.el8.x86_64.rpm java-1.8.0-openjdk-headless-1:1.8.0.402.b06-2.el8.x86_64.rpm kernel-4.18.0-513.18.1.el8_9.x86_64.rpm kernel-core-4.18.0-513.18.1.el8_9.x86_64.rpm kernel-headers-4.18.0-513.18.1.el8_9.x86_64.rpm kernel-modules-4.18.0-513.18.1.el8_9.x86_64.rpm kernel-tools-4.18.0-513.18.1.el8_9.x86_64.rpm kernel-tools-libs-4.18.0-513.18.1.el8_9.x86_64.rpm libmaxminddb-1.2.0-10.el8_9.1.x86_64.rpm libssh-0.9.6-13.el8_9.x86_64.rpm libssh-config-0.9.6-13.el8_9.noarch.rpm libxml2-2.9.7-18.el8_9.x86_64.rpm nss-3.90.0-6.el8_9.x86_64.rpm nss-softoken-3.90.0-6.el8_9.x86_64.rpm nss-softoken-freebl-3.90.0-6.el8_9.x86_64.rpm nss-sysinit-3.90.0-6.el8_9.x86_64.rpm nss-util-3.90.0-6.el8_9.x86_64.rpm	openssh-8.0p1-19.el8_9.2.x86_64.rpm openssh-askpass-8.0p1-19.el8_9.2.x86_64.rpm openssh-clients-8.0p1-19.el8_9.2.x86_64.rpm openssh-server-8.0p1-19.el8_9.2.x86_64.rpm openssl-1:1.1.1k-12.el8_9.x86_64.rpm openssl-libs-1:1.1.1k-12.el8_9.x86_64.rpm pixman-0.38.4-3.el8_9.x86_64.rpm platform-python-3.6.8-56.el8_9.3.x86_64.rpm python3-libs-3.6.8-56.el8_9.3.x86_64.rpm python3-libxml2-2.9.7-18.el8_9.x86_64.rpm python3-perf-4.18.0-513.11.1.el8_9.x86_64.rpm python3-urllib3-1.24.2-5.el8_9.2.noarch.rpm sqlite-3.26.0-19.el8_9.x86_64.rpm sqlite-libs-3.26.0-19.el8_9.x86_64.rpm sudo-1.9.5p2-1.el8_9.x86_64.rpm tcpdump-4.4.9.3-3.el8_9.1.x86_64.rpm oniguruma-6.8.2-2.1.el8_9.x86_64.rpm python3-perf-4.18.0-513.18.1.el8_9.x86_64mmmc.rpm tzdata-2023d-1.el8.noarch.rpm tzdata-2024a-1.el8.noarch.rpm
---	---

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #22 release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
SMGR-74905	openssl openssl-libs	RHSA-2023:7877	CVE-2023-3446 CVE-2023-3817 CVE-2023-5678	Low
SMGR-74908 SMGR-74956	nss nss-softokn nss-softokn-freebl nss-sysinit nss-util	RHSA-2024:0105 RHSA-2024:0786	CVE-2023-5388 CVE-2023-6135	Moderate
SMGR-74911 SMGR-75019	kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2024:0113 RHSA-2024:0897	CVE-2023-4622 CVE-2023-5633 CVE-2023-42753 CVE-2023-2162 CVE-2023-20569 CVE-2023-4623 CVE-2023-4921 CVE-2023-6817 CVE-2023-45871 CVE-2024-0646 CVE-2022-3545 CVE-2022-41858 CVE-2023-1073 CVE-2023-1838 CVE-2023-2166 CVE-2023-2176 CVE-2023-5717 CVE-2023-6356 CVE-2023-6535 CVE-2023-6536 CVE-2023-6606 CVE-2023-6610 CVE-2023-40283 CVE-2023-46813	Important
SMGR-74914 SMGR-74932	platform-python python3-libs	RHSA-2024:0114 RHSA-2024:0256	CVE-2022-48560 CVE-2022-48564 CVE-2023-27043	Moderate
SMGR-74917	python3-urllib3	RHSA-2024:0116	CVE-2023-43804 CVE-2023-45803	Moderate
SMGR-74920	libxml2 python3-libxml2	RHSA-2024:0119	CVE-2023-39615	Moderate
SMGR-74923	pixman	RHSA-2024:0131	CVE-2022-44638	Moderate
SMGR-74926 SMGR-74941	gnutls	RHSA-2024:0155 RHSA-2024:0627	CVE-2023-5981 CVE-2024-0553	Moderate
SMGR-74929	sqlite sqlite-libs	RHSA-2024:0253	CVE-2023-7104	Moderate

SMGR-74935	java-1.8.0-openjdk java-1.8.0-openjdk-devel java-1.8.0-openjdk-headless	RHSA-2024:0265	CVE-2024-20918 CVE-2024-20952 CVE-2024-20919 CVE-2024-20921, CVE-2024-20926 CVE-2024-20945	Important
SMGR-74938	openssh openssh-askpass openssh-clients openssh-server	RHSA-2024:0606	CVE-2023-48795 CVE-2023-51385	Moderate
SMGR-74944	libssh libssh-config	RHSA-2024:0628	CVE-2023-48795	Moderate
SMGR-74950	libmaxminddb	RHSA-2024:0768	CVE-2020-28241	Moderate
SMGR-74953	tcpdump	RHSA-2024:0769	CVE-2021-41043	Moderate
SMGR-74959	sudo	RHSA-2024:0811	CVE-2023-28487 CVE-2023-28486 CVE-2023-42465	Moderate
SMGR-74962 SMGR-74965	tzdata	RHBA-2024:0076 RHBA-2024:0762	N/A	Bugfix
SMGR-75016	oniguruma	RHSA-2024:0889	CVE-2019-13224 CVE-2019-16163 CVE-2019-19012 CVE-2019-19203 CVE-2019-19204	Moderate

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

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-008-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-010-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-011-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-012-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-014-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-015-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-017-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-018-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-019-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-020-01.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #21 release includes the following rpm updates:

avahi-libs-0.7-21.el8_9.x86_64.rpm kernel-4.18.0-513.9.1.el8_9.x86_64.rpm kernel-core-4.18.0-513.9.1.el8_9.x86_64.rpm kernel-headers-4.18.0-513.9.1.el8_9.x86_64.rpm	kernel-modules-4.18.0-513.9.1.el8_9.x86_64.rpm kernel-tools-4.18.0-513.9.1.el8_9.x86_64.rpm kernel-tools-libs-4.18.0-513.9.1.el8_9.x86_64.rpm python3-perf-4.18.0-513.9.1.el8_9.x86_64.rpm
---	---

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #21 release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-74437	avahi-libs	RHSA-2023:7836	CVE-2021-3468 CVE-2023-38469 CVE-2023-38470 CVE-2023-38471 CVE-2023-38472 CVE-2023-38473	Moderate	N/A	N/A
SMGR-74434	kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2023:7549	CVE-2023-2163 CVE-2023-3812 CVE-2023-5178 CVE-2022-45884 CVE-2022-45886 CVE-2022-45919 CVE-2023-1192	Important	N/A	N/A

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

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-008-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-010-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-011-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-012-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-014-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-015-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-017-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-018-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-019-01.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #20 release includes the following rpm updates:

avahi-libs-0.7-21.el8.x86_64.rpm bind-32:9.11.36-11.el8_9.x86_64.rpm bind-export-libs-32:9.11.36-11.el8_9.x86_64.rpm	open-vm-tools-12.2.5-3.el8_9.x86_64.rpm perl-HTTP-Tiny-0.074-2.el8.noarch.rpm platform-python-3.6.8-51.el8_8.2.x86_64.rpm
--	---

bind-libs-32:9.11.36-11.el8_9.x86_64.rpm bind-libs-lite-32:9.11.36-11.el8_9.x86_64.rpm bind-license-32:9.11.36-11.el8_9.noarch.rpm bind-utils-32:9.11.36-11.el8_9.x86_64.rpm binutils-2.30-119.el8_8.2.x86_64.rpm c-ares-1.13.0-8.el8.x86_64.rpm c-ares-1.13.0-9.el8_9.1.x86_64.rpm cups-libs-1:2.2.6-54.el8_9.x86_64.rpm emacsfilesystem-1:26.1-11.el8.noarch.rpm fwupd-1.7.8-2.el8.x86_64.rpm insights-client-3.2.2-1.el8_8.noarch.rpm kernel-4.18.0-513.5.1.el8_9.x86_64.rpm kernel-core-4.18.0-513.5.1.el8_9.x86_64.rpm kernel-headers-4.18.0-513.5.1.el8_9.x86_64.rpm kernel-modules-4.18.0-513.5.1.el8_9.x86_64.rpm kernel-tools-4.18.0-513.5.1.el8_9.x86_64.rpm kernel-tools-libs-4.18.0-513.5.1.el8_9.x86_64.rpm libX11-1.6.8-6.el8.x86_64.rpm libX11-common-1.6.8-6.el8.noarch.rpm libfastjson-0.99.9-2.el8.x86_64.rpm libpq-13.11-1.el8.x86_64.rpm linux-firmware-20230824-119.git0e048b06.el8_9.noarch.rpm	platform-python-3.6.8-56.el8_9.x86_64.rpm platform-python-pip-9.0.3-23.el8.noarch.rpm procps-ng-3.3.15-14.el8.x86_64.rpm protobuf-c-1.3.0-8.el8.x86_64.rpm python2-2.7.18-13.module+el8.8.0+20144+beed974d.2.x86_64.rpm python2-2.7.18-15.module+el8.9.0+20125+68111a8f.x86_64.rpm python2-libs-2.7.18-13.module+el8.8.0+20144+beed974d.2.x86_64.rpm python2-libs-2.7.18-15.module+el8.9.0+20125+68111a8f.x86_64.rpm python2-pip-9.0.3-19.module+el8.9.0+19487+7dc18407.noarch.rpm python2-pip-wheel-9.0.3-19.module+el8.9.0+19487+7dc18407.noarch.rpm python2-setuptools-39.0.1-13.module+el8.9.0+19487+7dc18407.noarch.rpm python2-setuptools-wheel-39.0.1-13.module+el8.9.0+19487+7dc18407.noarch.rpm python3-bind-32:9.11.36-11.el8_9.noarch.rpm python3-cryptography-3.2.1-6.el8.x86_64.rpm python3-libs-3.6.8-51.el8_8.2.x86_64.rpm python3-libs-3.6.8-56.el8_9.x86_64.rpm python3-perf-4.18.0-513.5.1.el8_9.x86_64.rpm python3-pip-9.0.3-23.el8.noarch.rpm python3-pip-wheel-9.0.3-23.el8.noarch.rpm shadow-utils-2:4.6-19.el8.x86_64.rpm tpm2-tss-2.3.2-5.el8.x86_64.rpm
--	--

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #20 release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-74304	python2 python2-libs python2-pip python2-pip-wheel	RHSA-2023:5994	CVE-2023-40217	Important	N/A	N/A
SMGR-74307	python3-libs platform-python	RHSA-2023:5997	CVE-2023-40217	Important	N/A	N/A
SMGR-74310	binutils	RHSA-2023:6236	CVE-2022-4285	Moderate	N/A	N/A
SMGR-74313	insights-client	RHSA-2023:6283	CVE-2023-3972	Important	N/A	N/A
SMGR-74316	protobuf-c	RHSA-2023:6944	CVE-2022-48468	Moderate	N/A	N/A
SMGR-74319	libfastjson	RHSA-2023:6976	CVE-2020-12762	Moderate	N/A	N/A
SMGR-74322	libpq	RHSA-2023:7016	CVE-2022-41862	Low	N/A	N/A
SMGR-74325	libX11 libX11-common	RHSA-2023:7029	CVE-2023-3138	Moderate	N/A	N/A
SMGR-74328	python2 python2-libs python2-pip python2-pip-wheel python2-setuptools python2-setuptools-wheel	RHSA-2023:7042	CVE-2023-32681	Moderate	N/A	N/A

SMGR-74331	kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2023:7077	CVE-2022-4744, CVE-2023-3609, CVE-2023-3611, CVE-2023-4128, CVE-2023-4206, CVE-2023-4207, CVE-2023-4208, CVE-2023-31436, CVE-2021-43975, CVE-2022-3594, CVE-2022-3640, CVE-2022-28388, CVE-2022-38457, CVE-2022-40133, CVE-2023-33951, CVE-2023-33952, CVE-2022-40982, CVE-2022-42895, CVE-2022-45869, CVE-2023-4155, CVE-2023-30456, CVE-2022-45887, CVE-2023-0458, CVE-2023-0590, CVE-2023-0597, CVE-2023-1073, CVE-2023-1074, CVE-2023-1079, CVE-2023-1118, CVE-2023-1206, CVE-2023-1252, CVE-2023-1382, CVE-2023-1989, CVE-2023-1998, CVE-2023-2513, CVE-2023-3161, CVE-2023-3268, CVE-2023-3772, CVE-2023-4132, CVE-2023-4732, CVE-2023-23455, CVE-2023-26545, CVE-2023-28328, CVE-2023-28772, CVE-2023-31084, CVE-2023-33203, CVE-2023-35823, CVE-2023-35824, CVE-2023-35825, CVE-2023-1075, CVE-2023-1855, CVE-2023-3141, CVE-2023-3212	Important	N/A	N/A
SMGR-74334	emacs-filesystem	RHSA-2023:7083	CVE-2022-48337 CVE-2022-48339	Moderate	N/A	N/A

SMGR-74337	python3-cryptography	RHSA-2023:7096	CVE-2023-23931	Moderate	N/A	N/A
SMGR-74340	linux-firmware	RHSA-2023:7109	CVE-2023-20569	Moderate	N/A	N/A
SMGR-74343	shadow-utils	RHSA-2023:7112	CVE-2023-4641	Low	N/A	N/A
SMGR-74346	c-ares	RHSA-2023:7116	CVE-2022-4904	Moderate	N/A	N/A
SMGR-74349	platform-python python3-libs	RHSA-2023:7151	CVE-2007-4559	Moderate	N/A	N/A
SMGR-74352	cups-libs	RHSA-2023:7165	CVE-2023-32324, CVE-2023-34241	Moderate	N/A	N/A
SMGR-74355	tpm2-tss	RHSA-2023:7166	CVE-2023-22745	Low	N/A	N/A
SMGR-74358	perl-HTTP-Tiny	RHSA-2023:7174	CVE-2023-31486	Moderate	N/A	N/A
SMGR-74361	platform-python-pip python3-pip python3-pip-wheel	RHSA-2023:7176	CVE-2007-4559	Moderate	N/A	N/A
SMGR-74364	bind bind-export-libs bind-libs bind-libs-lite bind-license bind-utils python3-bind	RHSA-2023:7177	CVE-2022-3094	Moderate	N/A	N/A
SMGR-74367	procps-ng	RHSA-2023:7187	CVE-2023-4016	Low	N/A	N/A
SMGR-74370	fwupd	RHSA-2023:7189	CVE-2022-3287	Moderate	N/A	N/A
SMGR-74373	avahi-libs	RHSA-2023:7190	CVE-2023-1981	Moderate	N/A	N/A
SMGR-74376	c-ares	RHSA-2023:7207	CVE-2020-22217, CVE-2023-31130	Moderate	N/A	N/A
SMGR-74379	open-vm-tools	RHSA-2023:7265	CVE-2023-34058, CVE-2023-34059	Important	N/A	N/A

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

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-008-01.tar.bz2

AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-010-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-011-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-012-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-014-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-015-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-017-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-018-01.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #19 release includes the following rpm updates:

bind-32:9.11.36-8.el8_8.2.x86_64.rpm bind-export-libs-32:9.11.36-8.el8_8.2.x86_64.rpm bind-libs-32:9.11.36-8.el8_8.2.x86_64.rpm bind-libs-lite-32:9.11.36-8.el8_8.2.x86_64.rpm bind-license-32:9.11.36-8.el8_8.2.noarch.rpm bind-utils-32:9.11.36-8.el8_8.2.x86_64.rpm glibc-2.28-225.el8_8.6.i686.rpm glibc-2.28-225.el8_8.6.x86_64.rpm glibc-all-langpacks-2.28-225.el8_8.6.x86_64.rpm glibc-common-2.28-225.el8_8.6.x86_64.rpm	glibc-devel-2.28-225.el8_8.6.x86_64.rpm glibc-headers-2.28-225.el8_8.6.x86_64.rpm glibc-langpack-en-2.28-225.el8_8.6.x86_64.rpm java-1.8.0-openjdk-1:1.8.0.392.b08-4.el8.x86_64.rpm java-1.8.0-openjdk-devel-1:1.8.0.392.b08-4.el8.x86_64.rpm java-1.8.0-openjdk-headless-1:1.8.0.392.b08-4.el8.x86_64.rpm libnhttp2-1.33.0-5.el8_8.x86_64.rpm libtiff-4.0.9-29.el8_8.x86_64.rpm python3-bind-32:9.11.36-8.el8_8.2.noarch.rpm
--	---

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #19 release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-73943	libtiff	RHSA-2023:5353	CVE-2023-0800 CVE-2023-0801 CVE-2023-0802 CVE-2023-0803 CVE-2023-0804	Moderate	ASA-2023-138	Medium
SMGR-73946	glibc glibc-all-langpacks glibc-common glibc-devel glibc-headers glibc-langpack-en	RHSA-2023:5455	CVE-2023-4527 CVE-2023-4806 CVE-2023-4813 CVE-2023-4911	Important	N/A	N/A
SMGR-73949	bind bind-export-libs bind-libs bind-libs-lite bind-license bind-utils python3-bind	RHSA-2023:5474	CVE-2023-3341	Important	ASA-2023-132	High

SMGR-73952	java-1.8.0-openjdk java-1.8.0-openjdk-devel java-1.8.0-openjdk-headless	RHSA-2023:5731	CVE-2022-40433 CVE-2023-22067 CVE-2023-22081	Moderate	N/A	N/A
SMGR-73955	libnhttp2	RHSA-2023:5837	CVE-2023-44487	Important	N/A	N/A

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

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-008-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-010-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-011-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-012-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-014-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-015-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-017-03.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #18 release includes the following rpm updates:

cups-libs-1:2.2.6-51.el8_8.1.x86_64.rpm dmidecode-1:3.3-4.el8_8.1.x86_64.rpm kernel-4.18.0-477.27.1.el8_8.x86_64.rpm kernel-core-4.18.0-477.27.1.el8_8.x86_64.rpm kernel-headers-4.18.0-477.27.1.el8_8.x86_64.rpm kernel-modules-4.18.0-477.27.1.el8_8.x86_64.rpm kernel-tools-4.18.0-477.27.1.el8_8.x86_64.rpm	kernel-tools-libs-4.18.0-477.27.1.el8_8.x86_64.rpm linux-firmware-20230404-117.git2e92a49f.el8_8.noarch.rpm ncurses-6.1-9.20180224.el8_8.1.x86_64.rpm ncurses-base-6.1-9.20180224.el8_8.1.noarch.rpm ncurses-libs-6.1-9.20180224.el8_8.1.x86_64.rpm open-vm-tools-12.1.5-2.el8_8.3.x86_64.rpm python3-perf-4.18.0-477.27.1.el8_8.x86_64.rpm
---	---

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #18 release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-73823	cups-libs	RHSA-2023:4864	CVE-2023-32360	Important	ASA-2023-116	Medium
SMGR-73826	kernel kernel-core kernel-headers kernel-modules	RHSA-2023:5244	CVE-2023-2002 CVE-2023-20593 CVE-2023-3090 CVE-2023-3390	Important	ASA-2023-119	High

	kernel-tools kernel-tools-libs python3-perf		CVE-2023-35001 CVE-2023-35788 CVE-2023-3776 CVE-2023-4004			
SMGR-73829	linux-firmware	RHSA-2023:5245	CVE-2023-20593	Moderate	N/A	N/A
SMGR-73832	ncurses ncurses-base ncurses-libs	RHSA-2023:5249	CVE-2023-29491	Moderate	N/A	N/A
SMGR-73817	dmidecode	RHSA-2023:5252	CVE-2023-30630	Moderate	ASA-2023-118	High
SMGR-73820	open-vm-tools	RHSA-2023:5312	CVE-2023-20900	Important	N/A	N/A

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

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-008-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-010-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-011-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-012-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-014-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-015-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-016-01.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #17 release includes the following rpm updates:

curl-7.61.1-30.el8_8.3.x86_64.rpm dbus-1:1.12.8-24.el8_8.1.x86_64.rpm dbus-common-1:1.12.8-24.el8_8.1.noarch.rpm dbus-daemon-1:1.12.8-24.el8_8.1.x86_64.rpm dbus-libs-1:1.12.8-24.el8_8.1.x86_64.rpm dbus-tools-1:1.12.8-24.el8_8.1.x86_64.rpm kernel-4.18.0-477.21.1.el8_8.x86_64.rpm kernel-core-4.18.0-477.21.1.el8_8.x86_64.rpm kernel-headers-4.18.0-477.21.1.el8_8.x86_64.rpm kernel-modules-4.18.0-477.21.1.el8_8.x86_64.rpm kernel-tools-4.18.0-477.21.1.el8_8.x86_64.rpm kernel-tools-libs-4.18.0-477.21.1.el8_8.x86_64.rpm libcap-2.48-5.el8_8.i686.rpm libcap-2.48-5.el8_8.x86_64.rpm	libcurl-7.61.1-30.el8_8.3.x86_64.rpm libxml2-2.9.7-16.el8_8.1.x86_64.rpm openssh-8.0p1-19.el8_8.x86_64.rpm openssh-askpass-8.0p1-19.el8_8.x86_64.rpm openssh-clients-8.0p1-19.el8_8.x86_64.rpm openssh-server-8.0p1-19.el8_8.x86_64.rpm python3-cloud-what-1.28.36-3.el8_8.x86_64.rpm python3-libxml2-2.9.7-16.el8_8.1.x86_64.rpm python3-perf-4.18.0-477.21.1.el8_8.x86_64.rpm python3-requests-2.20.0-3.el8_8.noarch.rpm python3-subscription-manager-rhsm-1.28.36-3.el8_8.x86_64.rpm python3-syspurpose-1.28.36-3.el8_8.x86_64.rpm subscription-manager-rhsm-certificates-1.28.36-3.el8_8.x86_64.rpm
---	---

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #17 release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-73651	openssh openssh-askpass openssh-clients openssh-server	RHSA-2023:4419	CVE-2023-38408	Important	N/A	N/A
SMGR-73654	dbus dbus-common dbus-daemon dbus-libs dbus-tools	RHSA-2023:4498	CVE-2023-34969	Moderate	ASA-2023-099	Medium
SMGR-73657	kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2023:4517	CVE-2022-42896 CVE-2023-1281 CVE-2023-1829 CVE-2023-2124 CVE-2023-2194 CVE-2023-2235	Important	ASA-2023-095	Important
SMGR-73660	python3-requests	RHSA-2023:4520	CVE-2023-32681	Moderate	N/A	N/A
SMGR-73663	curl libcurl	RHSA-2023:4523	CVE-2023-27536	Moderate	ASA-2023-096	Medium
SMGR-73666	libcap	RHSA-2023:4524	CVE-2023-2602 CVE-2023-2603	Moderate	N/A	N/A
SMGR-73669	libxml2 python3-libxml2	RHSA-2023:4529	CVE-2023-28484 CVE-2023-29469	Moderate	ASA-2023-097	Medium
SMGR-73672	python3-cloud-what python3-syspurpose python3-subscription-manager-rhsm subscription-manager-rhsm-certificate	RHSA-2023:4706	CVE-2023-3899	Important	N/A	N/A

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

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-008-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-010-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-011-02.tar.bz2

AV-SMGR10.1-RHEL8.4-SSP-012-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-014-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-015-01.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #16 release includes the following rpm updates:

bind-32:9.11.36-8.el8_8.1.x86_64.rpm bind-export-libs-32:9.11.36-8.el8_8.1.x86_64.rpm bind-libs-32:9.11.36-8.el8_8.1.x86_64.rpm bind-libs-lite-32:9.11.36-8.el8_8.1.x86_64.rpm bind-license-32:9.11.36-8.el8_8.1.noarch.rpm bind-utils-32:9.11.36-8.el8_8.1.x86_64.rpm java-1.8.0-openjdk-1:1.8.0.382.b05-2.el8.x86_64.rpm java-1.8.0-openjdk-devel-1:1.8.0.382.b05-2.el8.x86_64.rpm java-1.8.0-openjdk-headless-1:1.8.0.382.b05-2.el8.x86_64.rpm kernel-4.18.0-477.15.1.el8_8.x86_64.rpm kernel-core-4.18.0-477.15.1.el8_8.x86_64.rpm kernel-headers-4.18.0-477.15.1.el8_8.x86_64.rpm kernel-modules-4.18.0-477.15.1.el8_8.x86_64.rpm kernel-tools-4.18.0-477.15.1.el8_8.x86_64.rpm kernel-tools-libs-4.18.0-477.15.1.el8_8.x86_64.rpm libssh-0.9.6-10.el8_8.x86_64.rpm libssh-config-0.9.6-10.el8_8.noarch.rpm	libtiff-4.0.9-28.el8_8.x86_64.rpm open-vm-tools-12.1.5-2.el8_8.x86_64.rpm python2-2.7.18-13.module+el8.8.0+19042+06909d2c.1.x86_64.rpm python2-libs-2.7.18-13.module+el8.8.0+19042+06909d2c.1.x86_64.rpm python2-pip-9.0.3-19.module+el8.6.0+13001+ad200bd9.noarch.rpm python2-pip-wheel-9.0.3-19.module+el8.6.0+13001+ad200bd9.noarch.rpm python3-bind-32:9.11.36-8.el8_8.1.noarch.rpm python3-perf-4.18.0-477.15.1.el8_8.x86_64.rpm sqlite-3.26.0-18.el8_8.x86_64.rpm sqlite-libs-3.26.0-18.el8_8.x86_64.rpm systemd-239-74.el8_8.2.x86_64.rpm systemd-libs-239-74.el8_8.2.i686.rpm systemd-libs-239-74.el8_8.2.x86_64.rpm systemd-pam-239-74.el8_8.2.x86_64.rpm systemd-udev-239-74.el8_8.2.x86_64.rpm
--	---

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #16 release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-73331	python2 python2-libs python2-pip python2-pip-wheel	RHSA-2023:3780	CVE-2023-24329	Important	ASA-2023-072	High
SMGR-73334	libtiff	RHSA-2023:3827	CVE-2022-48281	Moderate	ASA-2023-070	Medium
SMGR-73337	system system-libs system-pam system-udev	RHSA-2023:3837	CVE-2023-26604	Moderate	ASA-2023-063	High
SMGR-73340	libssh libssh-config	RHSA-2023:3839	CVE-2023-1667 CVE-2023-2283	Moderate	ASA-2023-086	Medium
SMGR-73343	sqlite sqlite-libs	RHSA-2023:3840	CVE-2020-24736	Moderate	ASA-2023-061	Medium
SMGR-73346	kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2023:3847	CVE-2023-28466	Moderate	ASA-2023-068	High

SMGR-73349	open-vm-tools	RHSA-2023:3949	CVE-2023-20867	Low	ASA-2023-073	Low
SMGR-73352	bind bind-export-libs bind-libs bind-libs-elite bind-license bind-utils python3-bind	RHSA-2023:4102	CVE-2023-2828	Important	ASA-2023-089	High
SMGR-73355	java-1.8.0-openjdk java-1.8.0-openjdk-devel java-1.8.0-openjdk-headless	RHSA-2023:4176	CVE-2023-2828	Important	N/A	N/A

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

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-008-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-010-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-011-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-012-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-014-01.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #15 release includes the following rpm updates:

c-ares-1.13.0-6.el8_8.2.x86_64.rpm kernel-4.18.0-477.13.1.el8_8.x86_64.rpm kernel-core-4.18.0-477.13.1.el8_8.x86_64.rpm kernel-headers-4.18.0-477.13.1.el8_8.x86_64.rpm kernel-modules-4.18.0-477.13.1.el8_8.x86_64.rpm	kernel-tools-4.18.0-477.13.1.el8_8.x86_64.rpm kernel-tools-libs-4.18.0-477.13.1.el8_8.x86_64.rpm platform-python-3.6.8-51.el8_8.1.x86_64.rpm python3-libs-3.6.8-51.el8_8.1.x86_64.rpm python3-perf-4.18.0-477.13.1.el8_8.x86_64.rpm
---	---

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #15 release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-73209	kernel kernel-core kernel-headers kernel-modules	RHSA-2023:3349	CVE-2023-32233	Important	N/A	N/A

	kernel-tools kernel-tools-libs python3-perf					
SMGR-73212	c-ares	RHSA-2023:3584	CVE-2023-32067	Important	N/A	N/A
SMGR-73215	platform-python python3-libs	RHSA-2023:3591	CVE-2022-24329	Important	N/A	N/A

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

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-008-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-010-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-011-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-012-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-013-01.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #14 release includes the following rpm updates:

bind-32:9.11.36-8.el8.x86_64.rpm bind-export-libs-32:9.11.36-8.el8.x86_64.rpm bind-libs-32:9.11.36-8.el8.x86_64.rpm bind-libs-lite-32:9.11.36-8.el8.x86_64.rpm bind-license-32:9.11.36-8.el8.noarch.rpm bind-utils-32:9.11.36-8.el8.x86_64.rpm curl-7.61.1-30.el8.x86_64.rpm curl-7.61.1-30.el8_8.2.x86_64.rpm dhcp-client-12:4.3.6-49.el8.x86_64.rpm dhcp-common-12:4.3.6-49.el8.noarch.rpm dhcp-libs-12:4.3.6-49.el8.x86_64.rpm emacs-filesystem-1:26.1-10.el8_8.2.noarch.rpm emacs-filesystem-1:26.1-7.el8_7.1.noarch.rpm emacs-filesystem-1:26.1-9.el8.noarch.rpm java-1.8.0-openjdk-1:1.8.0.372.b07-1.el8_7.x86_64.rpm java-1.8.0-openjdk-devel-1:1.8.0.372.b07-1.el8_7.x86_64.rpm java-1.8.0-openjdk-headless-1:1.8.0.372.b07-1.el8_7.x86_64.rpm kernel-4.18.0-477.10.1.el8_8.x86_64.rpm kernel-core-4.18.0-477.10.1.el8_8.x86_64.rpm kernel-headers-4.18.0-477.10.1.el8_8.x86_64.rpm	kernel-modules-4.18.0-477.10.1.el8_8.x86_64.rpm kernel-tools-4.18.0-477.10.1.el8_8.x86_64.rpm kernel-tools-libs-4.18.0-477.10.1.el8_8.x86_64.rpm kpartx-0.8.4-37.el8.x86_64.rpm libarchive-3.3.3-5.el8.x86_64.rpm libcurl-7.61.1-30.el8.x86_64.rpm libcurl-7.61.1-30.el8_8.2.x86_64.rpm libtar-1.2.20-17.el8.x86_64.rpm libtiff-4.0.9-27.el8.x86_64.rpm python2-2.7.18-12.module+el8.8.0+17629+2cfc9d03.x86_64.rpm python2-libs-2.7.18-12.module+el8.8.0+17629+2cfc9d03.x86_64.rpm python2-pip-9.0.3-19.module+el8.6.0+13001+ad200bd9.noarch.rpm python2-pip-wheel-9.0.3-19.module+el8.6.0+13001+ad200bd9.noarch.rpm python3-bind-32:9.11.36-8.el8.noarch.rpm python3-perf-4.18.0-477.10.1.el8_8.x86_64.rpm python3-unbound-1.16.2-5.el8.x86_64.rpm unbound-libs-1.16.2-5.el8.x86_64.rpm
--	--

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #14 release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-72866	java-1.8.0-openjdk java-1.8.0-openjdk-devel java-1.8.0-openjdk-headless	RHSA-2023:1908	CVE-2023-21930 CVE-2023-21937 CVE-2023-21938 CVE-2023-21939 CVE-2023-21954 CVE-2023-21967 CVE-2023-21968	Important	ASA-2023-037	High
SMGR-72869	emacsfilesystem	RHSA-2023:1930	CVE-2023-28617	Important	ASA-2023-035	High
SMGR-72872	python3-unbound unbound-libs	RHSA-2023:2771	CVE-2022-3204	Moderate	N/A	N/A
SMGR-72875	python2 python2-libs python2-pip python2-pip-wheel	RHSA-2023:2860	CVE-2022-45061	Moderate	N/A	N/A
SMGR-72878	libtiff	RHSA-2023:2883	CVE-2022-3627 CVE-2022-3970	Moderate	N/A	N/A
SMGR-72881	libtar	RHSA-2023:2898	CVE-2021-33643 CVE-2021-33644 CVE-2021-33645 CVE-2021-3364	Moderate	ASA-2023-044	Critical
SMGR-72884	kpartx	RHSA-2023:2948	CVE-2022-41973	Moderate	N/A	N/A
SMGR-72887	kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2023:2951	CVE-2021-26341 CVE-2021-33655 CVE-2021-33656 CVE-2022-1462 CVE-2022-1679 CVE-2022-1789 CVE-2022-20141 CVE-2022-2196 CVE-2022-25265 CVE-2022-2663 CVE-2022-3028 CVE-2022-30594 CVE-2022-3239 CVE-2022-3522 CVE-2022-3524 CVE-2022-3564 CVE-2022-3566 CVE-2022-3567 CVE-2022-3619 CVE-2022-3623 CVE-2022-3625 CVE-2022-3628 CVE-2022-3707	Important	N/A	N/A

			CVE-2022-39188 CVE-2022-39189 CVE-2022-41218 CVE-2022-4129 CVE-2022-41674 CVE-2022-42703 CVE-2022-42720 CVE-2022-42721 CVE-2022-42722 CVE-2022-43750 CVE-2022-47929 CVE-2023-0394 CVE-2023-0461 CVE-2023-1195 CVE-2023-1582 CVE-2023-23454			
SMGR-72890	curl libcurl	RHSA-2023:2963	CVE-2022-35252 CVE-2022-43552	Low	N/A	N/A
SMGR-72893	dhcp-client dhcp-common dhcp-libs	RHSA-2023:3000	CVE-2022-2928 CVE-2022-2929	Moderate	N/A	N/A
SMGR-72896	bind bind-export-libs bind-libs bind-libs-lite bind-license bind-utils python3-bind	RHSA-2023:3002	CVE-2022-2795	Moderate	N/A	N/A
SMGR-72899	libarchive	RHSA-2023:3018	CVE-2022-36227	Low	ASA-2023-047	Medium
SMGR-72902	emacsfilesystem	RHSA-2023:3042	CVE-2022-45939	Moderate	ASA-2023-039	High
SMGR-72905	emacsfilesystem	RHSA-2023:3104	CVE-2023-2491	Important	ASA-2023-045	High
SMGR-72908	curl libcurl	RHSA-2023:3106	CVE-2023-27535	Moderate	ASA-2023-043	Medium

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

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-008-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-010-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-011-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-012-01.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #13 release includes the following rpm updates:

gnutls-3.6.16-6.el8_7.x86_64.rpm kernel-4.18.0-425.19.2.el8_7.x86_64.rpm kernel-core-4.18.0-425.19.2.el8_7.x86_64.rpm kernel-headers-4.18.0-425.19.2.el8_7.x86_64.rpm kernel-modules-4.18.0-425.19.2.el8_7.x86_64.rpm kernel-tools-4.18.0-425.19.2.el8_7.x86_64.rpm	kernel-tools-libs-4.18.0-425.19.2.el8_7.x86_64.rpm openssl-1:1.1.1k-9.el8_7.x86_64.rpm openssl-libs-1:1.1.1k-9.el8_7.x86_64.rpm python3-perf-4.18.0-425.19.2.el8_7.x86_64.rpm bugfix tzdata-2023b-1.el8.noarch.rpm bugfix tzdata-2023c-1.el8.noarch.rpm
--	--

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #13 release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-72763	openssl openssl-libs	RHSA-2023:1405	CVE-2022-4304 CVE-2022-4450 CVE-2022-0125 CVE-2022-0286	Important	ASA-2023-031	High
SMGR-72766	kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2023:1566	CVE-2022-4269 CVE-2022-4378 CVE-2022-0266 CVE-2022-0386	Important	N/A	N/A
SMGR-72769	gnutls	RHSA-2023:1569	CVE-2023-0361	Moderate	ASA-2023-033	High
SMGR-72772	tzdata-2023b	RHSA-2023:1491	N/A	BugFix	N/A	N/A
SMGR-72776	tzdata-2023c	RHSA-2023:1534	N/A	BugFix	N/A	N/A

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

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-008-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-010-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-011-02.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #12 release includes the following rpm updates:

curl-7.61.1-25.el8_7.3.x86_64.rpm libcurl-7.61.1-25.el8_7.3.x86_64.rpm nss-3.79.0-11.el8_7.x86_64.rpm nss-softokn-3.79.0-11.el8_7.x86_64.rpm	nss-softokn-freebl-3.79.0-11.el8_7.x86_64.rpm nss-sysinit-3.79.0-11.el8_7.x86_64.rpm nss-util-3.79.0-11.el8_7.x86_64.rpm
---	--

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #12 release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-72610	nss nss-softokn nss-softokn-freebl nss-sysinit nss-util	RHSA-2023:1252	CVE-2023-0767	Important	ASA-2023-028	High
SMGR-72607	curl libcurl	RHSA-2023:1140	CVE-2023-23916	Moderate	N/A	N/A
SMGR-72426	SSP installation log file access issue with user having administrative privileges.	N/A	N/A	N/A	Bugfix	N/A

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

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-008-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-010-01.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #11 release includes the following rpm updates:

dbus-1:1.12.8-23.el8_7.1.x86_64.rpm dbus-common-1:1.12.8-23.el8_7.1.noarch.rpm dbus-daemon-1:1.12.8-23.el8_7.1.x86_64.rpm dbus-lib-1:1.12.8-23.el8_7.1.x86_64.rpm dbus-tools-1:1.12.8-23.el8_7.1.x86_64.rpm expat-2.2.5-10.el8_7.1.x86_64.rpm	libksba-1.3.5-9.el8_7.x86_64.rpm libtasn1-4.13-4.el8_7.x86_64.rpm libtiff-4.0.9-26.el8_7.x86_64.rpm libxml2-2.9.7-15.el8_7.1.x86_64.rpm platform-python-3.6.8-48.el8_7.1.x86_64.rpm platform-python-setuptools-39.2.0-6.el8_7.1.noarch.rpm
--	---

grub2-common-1:2.02-142.el8_7.1.noarch.rpm grub2-efi-x64-1:2.02-142.el8_7.1.x86_64.rpm grub2-tools-1:2.02-142.el8_7.1.x86_64.rpm grub2-tools-extra-1:2.02-142.el8_7.1.x86_64.rpm grub2-tools-minimal-1:2.02-142.el8_7.1.x86_64.rpm java-1.8.0-openjdk-1:1.8.0.362.b09-2.el8_7.x86_64.rpm java-1.8.0-openjdk-devel-1:1.8.0.362.b09-2.el8_7.x86_64.rpm java-1.8.0-openjdk-headless-1:1.8.0.362.b09-2.el8_7.x86_64.rpm kernel-4.18.0-425.13.1.el8_7.x86_64.rpm kernel-core-4.18.0-425.13.1.el8_7.x86_64.rpm kernel-headers-4.18.0-425.13.1.el8_7.x86_64.rpm kernel-modules-4.18.0-425.13.1.el8_7.x86_64.rpm kernel-tools-4.18.0-425.13.1.el8_7.x86_64.rpm kernel-tools-libs-4.18.0-425.13.1.el8_7.x86_64.rpm	python3-libs-3.6.8-48.el8_7.1.x86_64.rpm python3-libxml2-2.9.7-15.el8_7.1.x86_64.rpm python3-perf-4.18.0-425.10.1.el8_7.x86_64.rpm python3-perf-4.18.0-425.13.1.el8_7.x86_64.rpm python3-setuptools-39.2.0-6.el8_7.1.noarch.rpm python3-setuptools-wheel-39.2.0-6.el8_7.1.noarch.rpm sqlite-libs-3.26.0-17.el8_7.x86_64.rpm sudo-1.8.29-8.el8_7.1.x86_64.rpm systemd-239-68.el8_7.4.x86_64.rpm systemd-libs-239-68.el8_7.4.i686.rpm systemd-libs-239-68.el8_7.4.x86_64.rpm systemd-pam-239-68.el8_7.4.x86_64.rpm systemd-udev-239-68.el8_7.4.x86_64.rpm tar 2:1.30-6.el8_7.1.x86_64.rpm
--	--

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #11 release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-72452	grub2-common grub2-efi-x64 grub2-tools grub2-tools-extra grub2-tools-minimal	RHSA-2023:0049	CVE-2022-2601 CVE-2022-3775	Moderate	ASA-2023-002	Medium
SMGR-72455	libtiff	RHSA-2023:0095	CVE-2022-2056 CVE-2022-2057 CVE-2022-2058 CVE-2022-2519 CVE-2022-2520 CVE-2022-2867 CVE-2022-2868 CVE-2022-2869 CVE-2022-2953	Moderate	ASA-2023-005	Medium
SMGR-72458	dbus dbus-common dbus-daemon dbus-libs dbus-tools	RHSA-2023:0096	CVE-2022-42010 CVE-2022-42011 CVE-2022-42012	Moderate	N/A	N/A
SMGR-72461 SMGR-72497	systemd systemd-libs systemd-pam systemd-udev	RHSA-2023:0100 RHSA-2023:0837	CVE-2022-3821 CVE-2022-4415	Moderate	ASA-2023-006	Medium
SMGR-72464 SMGR-72488	kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2023:0101 RHSA-2023:0832	CVE-2022-2964 CVE-2022-4139 CVE-2022-2873 CVE-2022-41222 CVE-2022-43945	Important	ASA-2023-004	High

SMGR-72467	expat	RHSA-2023:0103	CVE-2022-43680	Moderate	ASA-2023-008	High
SMGR-72470	sqlite-libs	RHSA-2023:0110	CVE-2022-35737	Moderate	ASA-2023-009	Medium
SMGR-72473	libtasn1	RHSA-2023:0116	CVE-2021-46848	Moderate	ASA-2023-019	Medium
SMGR-72476	libxml2 python3-libxml2	RHSA-2023:0173	CVE-2022-40303 CVE-2022-40304	Moderate	ASA-2023-007	High
SMGR-72479	java-1.8.0-openjdk java-1.8.0-openjdk-devel java-1.8.0-openjdk-headless	RHSA-2023:0208	CVE-2023-21830 CVE-2023-21843	Moderate	ASA-2023-016	Medium
SMGR-72482	Sudo	RHSA-2023:0284	CVE-2023-22809	Important	ASA-2023-010	High
SMGR-72485	libksba	RHSA-2023:0625	CVE-2022-47629	Important	ASA-2023-017	High
SMGR-72491	platform-python python3-libs	RHSA-2023:0833	CVE-2020-10735 CVE-2021-28861 CVE-2022-45061	Moderate	N/A	N/A
SMGR-72494	platform-python-setuptools python3-setuptools python3-setuptools-wheel	RHSA-2023:0835	CVE-2022-40897	Moderate	ASA-2023-023	Medium
SMGR-72500	tar	RHSA-2023:0842	CVE-2022-48303	Moderate	N/A	N/A

➤ **There was no System Manager February 2023 Security Service Pack update required.**

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

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-008-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-009-01.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #10 release includes the following rpm updates:

tzdata-2022g-1.el8.noarch.rpm	
-------------------------------	--

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #10 release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-72027	tzdata-2022g-1	RHSA-2022:8785	N/A	Bug Fix	N/A	N/A

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

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-008-01.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #9 release includes the following rpm updates:

bind-32:9.11.36-5.el8.x86_64 bind-export-libs-32:9.11.36-5.el8.x86_64 bind-libs-32:9.11.36-5.el8.x86_64 bind-libs-lite-32:9.11.36-5.el8.x86_64 bind-license-32:9.11.36-5.el8.noarch bind-utils-32:9.11.36-5.el8.x86_64 e2fsprogs-1.45.6-5.el8.x86_64 e2fsprogs-libs-1.45.6-5.el8.x86_64 freetype-2.9.1-9.el8.x86_64 fribidi-1.0.4-9.el8.x86_64 gdisk-1.0.3-11.el8.x86_64 glib2-2.56.4-159.el8.x86_64 kernel-4.18.0-425.3.1.el8.x86_64 kernel-core-4.18.0-425.3.1.el8.x86_64 kernel-headers-4.18.0-425.3.1.el8.x86_64 kernel-modules-4.18.0-425.3.1.el8.x86_64 kernel-tools-4.18.0-425.3.1.el8.x86_64 kernel-tools-libs-4.18.0-425.3.1.el8.x86_64 kpartx-0.8.4-28.el8_7.1.x86_64	krb5-libs-1.18.2-22.el8_7.x86_64 libcom_err-1.45.6-5.el8.x86_64 libss-1.45.6-5.el8.x86_64 libtiff-4.0.9-23.el8.x86_64 libxml2-2.9.7-15.el8.x86_64 python2-2.7.18-11.module+el8.7.0+15681+7a92afba.x86_64 python2-libs-2.7.18-11.module+el8.7.0+15681+7a92afba.x86_64 python2-pip-9.0.3-19.module+el8.6.0+13001+ad200bd9.noarch python2-pip-wheel-9.0.3-19.module+el8.6.0+13001+ad200bd9.noarch python3-bind-32:9.11.36-5.el8.noarch python3-libxml2-2.9.7-15.el8.x86_64 python3-perf-4.18.0-425.3.1.el8.x86_64 python3-unbound-1.16.2-2.el8.x86_64 rsync-3.1.3-19.el8.x86_64 unbound-libs-1.16.2-2.el8.x86_64 xmlrpc-c-1.51.0-8.el8.x86_64 xmlrpc-c-client-1.51.0-8.el8.x86_64 tzdata-2022f-1.el8.noarch
---	---

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #9 release:

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

SMGR-71782	fribidi	RHSA-2022:7514	CVE-2022-25308 CVE-2022-25309 CVE-2022-25310	Moderate	N/A	N/A
SMGR-71784	libtiff	RHSA-2022:7585	CVE-2022-0561 CVE-2022-0562 CVE-2022-0865 CVE-2022-0891 CVE-2022-0908 CVE-2022-0909 CVE-2022-0924 CVE-2022-1355 CVE-2022-22844	Moderate	ASA-2022-151	High
SMGR-71786	python2 python2-libs python2-pip python2-pip-wheel	RHSA-2022:7593	CVE-2015-20107	Moderate	ASA-2022-156	High
SMGR-71788	python3-unbound unbound-libs	RHSA-2022:7622	CVE-2022-30698 CVE-2022-30699	Moderate	ASA-2022-150	Medium
SMGR-71790	kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2022:7683	CVE-2020-36516 CVE-2020-36558 CVE-2021-30002 CVE-2021-3640 CVE-2022-0168 CVE-2022-0617 CVE-2022-0854 CVE-2022-1016 CVE-2022-1048 CVE-2022-1055 CVE-2022-1184 CVE-2022-1852 CVE-2022-20368 CVE-2022-2078 CVE-2022-21499 CVE-2022-23960 CVE-2022-24448 CVE-2022-2586 CVE-2022-26373 CVE-2022-2639 CVE-2022-27950 CVE-2022-28390 CVE-2022-28893 CVE-2022-2938 CVE-2022-29581 CVE-2022-36946	Moderate	ASA-2022-144	High
SMGR-71792	xmlrpc-c xmlrpc-c-client	RHSA-2022:7692	CVE-2021-46143 CVE-2022-22822 CVE-2022-22823 CVE-2022-22824 CVE-2022-22825 CVE-2022-22826 CVE-2022-22827	Moderate	ASA-2022-159	Critical

SMGR-71794	Gdisk	RHSA-2022:7700	CVE-2020-0256 CVE-2021-0308	Moderate	ASA-2022-142	Medium
SMGR-71796	glib2	RHSA-2022:7704	CVE-2022-22624 CVE-2022-22628 CVE-2022-22629 CVE-2022-22662 CVE-2022-26700 CVE-2022-26709 CVE-2022-26710 CVE-2022-26716 CVE-2022-26717 CVE-2022-26719 CVE-2022-30293	Moderate	ASA-2022-146	High
SMGR-71798	libxml2 python3-libxml2	RHSA-2022:7715	CVE-2016-3709	Moderate	ASA-2022-138	Medium
SMGR-71800	e2fsprogs e2fsprogs-libs libcom_err libss	RHSA-2022:7720	CVE-2022-1304	Moderate	ASA-2022-141	High
SMGR-71802	freetype	RHSA-2022:7745	CVE-2022-27404 CVE-2022-27405 CVE-2022-27406	Moderate	N/A	N/A
SMGR-71804	bind bind-export-libs bind-libs bind-libs-lite bind-license bind-utils python3-bind	RHSA-2022:7790	CVE-2021-25220	Moderate	ASA-2022-155	Medium
SMGR-71806	rsync	RHSA-2022:7793	CVE-2022-37434	Moderate	N/A	N/A
SMGR-71808	kpartx	RHSA-2022:7928	CVE-2022-3787	Important	ASA-2022-149	High
SMGR-71810	krb5-libs	RHSA-2022:8638	CVE-2022-42898	Important	N/A	N/A
SMGR-71812	tzdata-2022e-1 tzdata-2022f-1 tzdata-2022f-1	RHBA-2022:7824 RHBA-2022:7404 RHBA-2022:7884	N/A	Bug Fix	N/A	N/A

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

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2

AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2

AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2

AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2

AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2
AV-SMGR10.1-RHEL8.4-SSP-007-01.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #8 release includes the following rpm updates:

bind-32:9.11.36-3.el8_6.1.x86_64 bind-export-libs-32:9.11.36-3.el8_6.1.x86_64 bind-libs-32:9.11.36-3.el8_6.1.x86_64 bind-libs-lite-32:9.11.36-3.el8_6.1.x86_64 bind-license-32:9.11.36-3.el8_6.1.noarch bind-utils-32:9.11.36-3.el8_6.1.x86_64 python3-bind-32:9.11.36-3.el8_6.1.noarch expat-2.2.5-8.el8_6.3.x86_64 java-1.8.0-openjdk-1:1.8.0.352.b08-2.el8_6.x86_64 java-1.8.0-openjdk-devel-1:1.8.0.352.b08-2.el8_6.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.352.b08-2.el8_6.x86_64 libksba-1.3.5-8.el8_6.x86_64 gnutls-3.6.16-5.el8_6.x86_64	zlib-1.2.11-19.el8_6.x86_64 sqlite-3.26.0-16.el8_6.x86_64 sqlite-libs-3.26.0-16.el8_6.x86_64 kernel-4.18.0-372.32.1.el8_6.x86_64 kernel-core-4.18.0-372.32.1.el8_6.x86_64 kernel-headers-4.18.0-372.32.1.el8_6.x86_64 kernel-modules-4.18.0-372.32.1.el8_6.x86_64 kernel-tools-4.18.0-372.32.1.el8_6.x86_64 kernel-tools-libs-4.18.0-372.32.1.el8_6.x86_64 python3-perf-4.18.0-372.32.1.el8_6.x86_64 kpartx-0.8.4-22.el8_6.2.x86_64 tzdata-2022c-1.el8.noarch tzdata-2022d-1.el8.noarch tzdata-2022e-1.el8.noarch
---	--

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #8 release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-71500	bind bind-export-libs bind-libs bind-libs-lite bind-license bind-utils python3-bind	RHSA-2022:6778	CVE-2022-38177 CVE-2022-38178	Important	N/A	N/A
SMGR-71502	expat	RHSA-2022:6878	CVE-2022-40674	Important	N/A	N/A
SMGR-71504	java-1.8.0-openjdk java-1.8.0-openjdk-devel java-1.8.0-openjdk-headless	RHSA-2022:7006	CVE-2022-21619 CVE-2022-21624 CVE-2022-21626 CVE-2022-21628	Moderate	N/A	N/A
SMGR-71506	libksba	RHSA-2022:7089	CVE-2022-3515	Important	N/A	N/A
SMGR-71508	gnutls	RHSA-2022:7105	CVE-2015-2509	Moderate	N/A	N/A
SMGR-71510	zlib	RHSA-2022:7106	CVE-2022-37434	Moderate	ASA-2022-129	Critical
SMGR-71512	sqlite sqlite-libs	RHSA-2022:7108	CVE-2020-35525 CVE-2020-35527	Moderate	ASA-2022-130	High
SMGR-71514	kernel kernel-core kernel-headers	RHSA-2022: 7110	CVE-2022-0494 CVE-2022-1353 CVE-2022-23816	Important	ASA-2022-132	High

	kernel-modules kernel-tools kernel-tools-libs python3-perf		CVE-2022-23825 CVE-2022-2588 CVE-2022-29900 CVE-2022-29901			
SMGR-71516	kpartx	RHSA-2022:7192	CVE-2022-41974	Important	ASA-2022-128	High
SMGR-71518	tzdata-2022c-1 tzdata-2022d-1 tzdata-2022e-1	RHBA-2022:6138 RHBA-2022:6827 RHBA-2022:7067	N/A	Bug Fix	N/A	N/A

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

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2
 AV-SMGR10.1-RHEL8.4-SSP-006-01.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #7 release includes the following rpm updates:

url-7.61.1-22.el8_6.x86_64 gnupg2-2.2.20-3.el8_6.x86_64 gnupg2-smime-2.2.20-3.el8_6.x86_64 kernel-4.18.0-372.26.1.el8_6.x86_64 kernel-core-4.18.0-372.26.1.el8_6.x86_64 kernel-headers-4.18.0-372.26.1.el8_6.x86_64 kernel-modules-4.18.0-372.26.1.el8_6.x86_64 kernel-tools-4.18.0-372.26.1.el8_6.x86_64 kernel-tools-libs-4.18.0-372.26.1.el8_6.x86_64 libcurl-7.61.1-22.el8_6.x86_64 open-vm-tools-11.3.5-1.el8_6.x86_64	platform-python-3.6.8-47.el8_6.x86_64 python3-libs-3.6.8-47.el8_6.x86_64 python3-perf-4.18.0-372.26.1.el8_6.x86_64 rsync-3.1.3-14.el8_6.3.x86_64 systemd-239-58.el8_6.4.x86_64 systemd-libs-239-58.el8_6.4.x86_64 systemd-libs-239-58.el8_6.4.x86_64 systemd-pam-239-58.el8_6.4.x86_64 systemd-udev-239-58.el8_6.4.x86_64 tzdata-2022c-1.el8.noarch tzdata-java-2022c-1.el8.noarch
---	--

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #7 release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-71330	curl	RHSA-2022:6159	CVE-2022-32206 CVE-2022-32208	Moderate	N/A	N/A
SMGR-71332	rsync	RHSA-2022:6180	CVE-2022-29154	Important	ASA-2022-116	High
SMGR-71334	systemd systemd-libs systemd-pam	RHSA-2022:2526	CVE-2022-118	Important	ASA-2022-118	High

	systemd-udev					
SMGR-71336	pen-vm-tools	RHSA-2022:6357	CVE-2022-31676	Important	N/A	N/A
SMGR-71338	platform-python python3-libs	RHSA-2022:6457	CVE-2015-20107 CVE-2022-0391	Moderate	N/A	N/A
SMGR-71340	Kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2022: 6460	CVE-2022-21123 CVE-2022-21125 CVE-2022-21126	Moderate	N/A	N/A
SMGR-71342	gnupg2 gnupg2-smime	RHSA-2022:6463	CVE-2022-34903	Moderate	ASA-2022-121	Medium
SMGR-71404	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 #6 contains the fixes from the following previous patches:

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2

AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2

AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2

AV-SMGR10.1-RHEL8.4-SSP-005-02.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #6 release includes the following rpm updates:

pcre2-10.32-3.el8_6.i686 pcre2-10.32-3.el8_6.x86_64 vim-common-2:8.0.1763-19.el8_6.4.x86_64 vim-enhanced-2:8.0.1763-19.el8_6.4.x86_64 vim-filessystem-2:8.0.1763-19.el8_6.4.noarch vim-minimal-2:8.0.1763-19.el8_6.4.x86_64 openssl-1:1.1.1k-7.el8_6.x86_64 openssl-libs-1:1.1.1k-7.el8_6.x86_64	kernel-4.18.0-372.19.1.el8_6.x86_64 kernel-core-4.18.0-372.19.1.el8_6.x86_64 kernel-headers-4.18.0-372.19.1.el8_6.x86_64 kernel-modules-4.18.0-372.19.1.el8_6.x86_64 kernel-tools-4.18.0-372.19.1.el8_6.x86_64 kernel-tools-libs-4.18.0-372.19.1.el8_6.x86_64 python3-perf-4.18.0-372.19.1.el8_6.x86_64
---	---

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #6 release:

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

SMGR-71023	pcr2	RHSA-2022: 5809	CVE-022-1586	Moderate	ASA-2022-112	High
SMGR-71025	vim-common vim-enhanced vim-filesystem vim-minimal	RHSA-2022:5813	CVE-2022-1785 CVE-2022-1897 CVE-2022-1927	Moderate	ASA-2022-110	Critical
SMGR-71027	openssl openssl-libs	RHSA-2022:5818	CVE-2022-1292 CVE-2022-2068 CVE-2022-2097	Moderate	ASA-2022-111	Medium
SMGR-71029	Kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2022:5819	CVE-2020-1012 CVE-2022-32250	Important	N/A	N/A

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

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2

AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2

AV-SMGR10.1-RHEL8.4-SSP-004-01.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #5 release includes the following rpm updates:

libcrypt-1.8.5-7.el8_6.i686	vim-common-2:8.0.1763-19.el8_6.2.x86_64
libcrypt-1.8.5-7.el8_6.x86_64	vim-enhanced-2:8.0.1763-19.el8_6.2.x86_64
curl-7.61.1-22.el8_6.3.x86_64	vim-filesystem-2:8.0.1763-19.el8_6.2.noarch
libcurl-7.61.1-22.el8_6.3.x86_64	vim-minimal-2:8.0.1763-19.el8_6.2.x86_64
expat-2.2.5-8.el8_6.2.x86_64	kernel-4.18.0-372.16.1.el8_6.x86_64
kernel-4.18.0-372.13.1.el8_6.x86_64	kernel-core-4.18.0-372.16.1.el8_6.x86_64
kernel-core-4.18.0-372.13.1.el8_6.x86_64	kernel-headers-4.18.0-372.16.1.el8_6.x86_64
kernel-headers-4.18.0-372.13.1.el8_6.x86_64	kernel-modules-4.18.0-372.16.1.el8_6.x86_64
kernel-modules-4.18.0-372.13.1.el8_6.x86_64	kernel-tools-4.18.0-372.16.1.el8_6.x86_64
kernel-tools-4.18.0-372.13.1.el8_6.x86_64	kernel-tools-libs-4.18.0-372.16.1.el8_6.x86_64
kernel-tools-libs-4.18.0-372.13.1.el8_6.x86_64	python3-perf-4.18.0-372.16.1.el8_6.x86_64
python3-perf-4.18.0-372.13.1.el8_6.x86_64	java-1.8.0-openjdk-1:1.8.0.342.b07-2.el8_6.x86_64
libxml2-2.9.7-13.el8_6.1.x86_64	java-1.8.0-openjdk-devel-1:1.8.0.342.b07-2.el8_6.x86_64
python3-libxml2-2.9.7-13.el8_6.1.x86_64	java-1.8.0-openjdk-headless-1:1.8.0.342.b07-2.el8_6.x86_64

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #5 release:

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

SMGR-70658	libcrypt	RHSA-2022:5311	CVE-2021-40528	Moderate	ASA-2022-103	Medium
SMGR-70660	curl libcurl	RHSA-2022:5313	CVE-2022-22576 CVE-2022-27774 CVE-2022-27776 CVE-2022-27782	Moderate	N/A	N/A
SMGR-70662	expat	RHSA-2022:5314	CVE-2022-25313 CVE-2022-25314	Moderate	ASA-2022-102	High
SMGR-70664	kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2022:5316	CVE-2020-28915 CVE-2022-27666	Important	ASA-2022-101	High
SMGR-70666	libxml2 python3-libxml2	RHSA-2022:5317	CVE-2022-29824	Moderate	ASA-2022-100	High
SMGR-70668	vim-common vim-enhanced vim-filesystem vim-minimal	RHSA-2022:5319	CVE-2022-1621 CVE-2022-1629	Moderate	ASA-2022-104	High
SMGR-70670	kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2022:5564	CVE-2022-1729	Important	ASA-2022-109	Medium
SMGR-70672	java-1.8.0-openjdk java-1.8.0-openjdk-devel java-1.8.0-openjdk-headless	RHSA-2022:5696	CVE-2022-21540 CVE-2022-21541 CVE-2022-34169	Important	ASA-2022-107	High

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

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2

AV-SMGR10.1-RHEL8.4-SSP-003-03.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #4 release includes the following rpm updates:

xz-5.2.4-4.el8_6.x86_64 xz-libs-5.2.4-4.el8_6.i686 xz-libs-5.2.4-4.el8_6.x86_64 cups-libs-1:2.2.6-45.el8_6.2.x86_64 grub2-common-1:2.02-123.el8_6.noarch grub2-efi-x64-1:2.02-123.el8_6.x86_64	grub2-tools-1:2.02-123.el8_6.x86_64 grub2-tools-extra-1:2.02-123.el8_6.x86_64 grub2-tools-minimal-1:2.02-123.el8_6.x86_64 mokutil-1:0.3.0-11.el8_6.1.x86_64 shim-x64-15.6-1.el8.x86_64
---	--

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #4 release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-70290	xz xz-libs	RHSA-2022:4991	CVE-2022-1271	Important	ASA-2022-080	High
SMGR-70292	cups-libs	RHSA-2022:5056	CVE-2022-26691	Important	ASA-2022-091	High
SMGR-70294	grub2-common grub2-efi-x64 grub2-tools grub2-tools-extra grub2-tools-minimal mokutil shim-x64	RHSA-2022:5095	CVE-2021-3695 CVE-2021-3696 CVE-2021-3697 CVE-2022-28733 CVE-2022-28734 CVE-2022-28735 CVE-2022-28736 CVE-2022-28737	Important	ASA-2022-098	High

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

AV-SMGR10.1-RHEL8.4-SSP-002-01.tar.bz2

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

System Manager 10.1 Security Service Pack SSP #3 release includes the following rpm updates:

bind-32:9.11.36-3.el8.x86_64	libudisks2-2.9.0-9.el8.x86_64
bind-export-libs-32:9.11.36-3.el8.x86_64	openssh-8.0p1-13.el8.x86_64
bind-libs-32:9.11.36-3.el8.x86_64	openssh-askpass-8.0p1-13.el8.x86_64
bind-libs-lite-32:9.11.36-3.el8.x86_64	openssh-clients-8.0p1-13.el8.x86_64
bind-license-32:9.11.36-3.el8.noarch	openssh-server-8.0p1-13.el8.x86_64
bind-utils-32:9.11.36-3.el8.x86_64	pixman-0.38.4-2.el8.x86_64
cairo-1.15.12-6.el8.x86_64	platform-python-3.6.8-45.el8.x86_64
c-ares-1.13.0-6.el8.x86_64	polkit-0.115-13.el8_5.2.x86_64
cpio-2.12-11.el8.x86_64	polkit-libs-0.115-13.el8_5.2.x86_64
grub2-common-1:2.02-123.el8.noarch	python2-2.7.18-10.module+el8.6.0+14191+7fdd52cd.x86_64
grub2-efi-x64-1:2.02-123.el8.x86_64	python2-libs-2.7.18-10.module+el8.6.0+14191+7fdd52cd.x86_64
grub2-tools-1:2.02-123.el8.x86_64	python2-pip-9.0.3-19.module+el8.6.0+13001+ad200bd9.noarch
grub2-tools-extra-1:2.02-123.el8.x86_64	python2-pip-wheel-9.0.3-19.module+el8.6.0+13001+ad200bd9.noarch
grub2-tools-minimal-1:2.02-123.el8.x86_64	python3-bind-32:9.11.36-3.el8.noarch
gzip-1.9-13.el8_5.x86_64	python3-libs-3.6.8-45.el8.x86_64
java-1.8.0-openjdk-1:1.8.0.332.b09-1.el8_5.x86_64	python3-lxml-4.2.3-4.el8.x86_64
java-1.8.0-openjdk-devel-1:1.8.0.332.b09-1.el8_5.x86_64	python3-perf-4.18.0-348.23.1.el8_5.x86_64
java-1.8.0-openjdk-headless-1:1.8.0.332.b09-1.el8_5.x86_64	python3-perf-4.18.0-372.9.1.el8.x86_64
kernel-4.18.0-348.23.1.el8_5.x86_64	rsync-3.1.3-14.el8_6.2.x86_64
kernel-4.18.0-372.9.1.el8.x86_64	rsyslog-8.2102.0-7.el8_6.1.x86_64
kernel-core-4.18.0-348.23.1.el8_5.x86_64	rsyslog-gnutls-8.2102.0-7.el8_6.1.x86_64
kernel-core-4.18.0-372.9.1.el8.x86_64	udisks2-2.9.0-9.el8.x86_64
kernel-headers-4.18.0-348.23.1.el8_5.x86_64	vim-common-2:8.0.1763-16.el8_5.13.x86_64
kernel-headers-4.18.0-372.9.1.el8.x86_64	vim-enhanced-2:8.0.1763-16.el8_5.13.x86_64
kernel-modules-4.18.0-348.23.1.el8_5.x86_64	vim-filesystem-2:8.0.1763-16.el8_5.13.noarch
kernel-modules-4.18.0-372.9.1.el8.x86_64	vim-minimal-2:8.0.1763-16.el8_5.13.x86_64
kernel-tools-4.18.0-348.23.1.el8_5.x86_64	xmlrpc-c-1.51.0-5.el8_5.1.x86_64
kernel-tools-4.18.0-372.9.1.el8.x86_64	xmlrpc-c-client-1.51.0-5.el8_5.1.x86_64
kernel-tools-libs-4.18.0-348.23.1.el8_5.x86_64	zlib-1.2.11-18.el8_5.x86_64
kernel-tools-libs-4.18.0-372.9.1.el8.x86_64	
libpq-13.5-1.el8.x86_64	
libssh-0.9.6-3.el8.x86_64	
libssh-config-0.9.6-3.el8.noarch	
libtiff-4.0.9-21.el8.x86_64	

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #3 release:

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

SMGR-69800	java-1.8.0-openjdk java-1.8.0-openjdk-devel java-1.8.0-openjdk-headless	RHSA-2022:1491	CVE-2022-21426 CVE-2022-21434 CVE-2022-21443 CVE-2022-21476 CVE-2022-21496	Important	N/A	N/A
SMGR-69802	gzip	RHSA-2022:1537	CVE-2022-1271	Important	ASA-2022-041	High
SMGR-69804	polkit polkit-libs	RHSA-2022:1546	CVE-2021-4115	Moderate	ASA-2022-040	Medium
SMGR-69806	kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2022:1550	CVE-2021-4028 CVE-2022-25636	Important	N/A	N/A
SMGR-69808	vim-common vim-enhanced vim-filesystem vim-minimal	RHSA-2022:1552	CVE-2022-1154	Moderate	ASA-2022-042	Critical
SMGR-69810	zlib	RHSA-2022:1642	CVE-2018-25032	Important	ASA-2022-044	High
SMGR-69812	xmlrpc-c xmlrpc-c-client	RHSA-2022:1643	CVE-2022-25235	Important	ASA-2022-068	Critical
SMGR-69814	Libtiff	RHSA-2022:1810	CVE-2020-19131	Moderate	ASA-2022-050	High
SMGR-69816	libudisks2 udisks2	RHSA-2022:1820	CVE-2021-3802	Low	ASA-2022-048	Low
SMGR-69818	python2 python2-libs python2-pip python2-wheel	RHSA-2022:1821	CVE-2021-3733 CVE-2021-3737 CVE-2021-4189 CVE-2021-43818 CVE-2022-0391	Moderate	ASA-2022-059	High
SMGR-69820	libpq	RHSA-2022:1891	CVE-2021-23222	Low	ASA-2022-060	Low
SMGR-69822	python3-lxml	RHSA-2022:1932	CVE-2021-43818	Moderate	ASA-2022-071	High
SMGR-69824	cairo pixman	RHSA-2022:196	CVE-2020-35492	Moderate	ASA-2022-052	High
SMGR-69826	platform-python python3-libs	RHSA-2022:1986	CVE-2021-3737 CVE-2021-4189	Moderate	ASA-2022-049	Medium
SMGR-69830	cpio	RHSA-2022:1991	CVE-2021-38185	Moderate	ASA-2022-054	High
SMGR-69832	openssh openssh-askpass openssh-clients openssh-server	RHSA-2022:2013	CVE-2021-41617	Moderate	ASA-2022-056	High
SMGR-69834	libssh libssh-config	RHSA-2022:2031	CVE-2021-3634	Low	ASA-2022-05	Medium

SMGR-69836	c-ares	RHSA-2022:2043	CVE-2021-3672	Moderate	N/A	N/A
SMGR-69838	bind bind-export-libs bind-libs bind-libs-lite bind-license bind-utils python3-bind	RHSA-2022:2092	CVE-2021-25219	Moderate	ASA-2022-069	Medium
SMGR-69840	grub2-common grub2-efi-x64 grub2-tools grub2-tools-extra grub2-tools-minimal	RHSA-2022:2110	CVE-2021-3981	Low	ASA-2022-051	Low
SMGR-69842	rsync	RHSA-2022:2201	CVE-2018-25032	Important	ASA-2022-063	High
SMGR-69894	rsyslog rsyslog-gnutils	RHSA-2022:4799	CVE-2022-24903	Important	ASA-2022-078	High
SMGR-69828	kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2022:1988	CVE-2020-0404 CVE-2020-13974 CVE-2020-27820 CVE-2020-4788 CVE-2021-0941 CVE-2021-20322 CVE-2021-21781 CVE-2021-26401 CVE-2021-29154 CVE-2021-3612 CVE-2021-3669 CVE-2021-37159 CVE-2021-3743 CVE-2021-3744 CVE-2021-3752 CVE-2021-3759 CVE-2021-3764 CVE-2021-3772 CVE-2021-3773 CVE-2021-4002 CVE-2021-4037 CVE-2021-4083 CVE-2021-4157 CVE-2021-41864 CVE-2021-4197 CVE-2021-4203 CVE-2021-42739 CVE-2021-43056 CVE-2021-43389 CVE-2021-43976 CVE-2021-44733 CVE-2021-45485 CVE-2021-45486 CVE-2022-0001 CVE-2022-0002 CVE-2022-0286 CVE-2022-0322 CVE-2022-1011	Important	ASA-2022-055	Critical

System Manager 10.1 Security Service Pack SSP #2 release includes the following rpm updates:

kernel-4.18.0-348.20.1.el8_5.x86_64 kernel-core-4.18.0-348.20.1.el8_5.x86_64 kernel-headers-4.18.0-348.20.1.el8_5.x86_64 kernel-modules-4.18.0-348.20.1.el8_5.x86_64 kernel-tools-4.18.0-348.20.1.el8_5.x86_64 kernel-tools-libs-4.18.0-348.20.1.el8_5.x86_64 python3-perf-4.18.0-348.20.1.el8_5.x86_64 libarchive-3.3.3-3.el8_5.x86_64 vim-common-2:8.0.1763-16.el8_5.12.x86_64 vim-enhanced-2:8.0.1763-16.el8_5.12.x86_64 vim-filesystem-2:8.0.1763-16.el8_5.12.noarch vim-minimal-2:8.0.1763-16.el8_5.12.x86_64	glibc-2.28-164.el8_5.3.i686 glibc-2.28-164.el8_5.3.x86_64 glibc-all-langpacks-2.28-164.el8_5.3.x86_64 glibc-common-2.28-164.el8_5.3.x86_64 glibc-devel-2.28-164.el8_5.3.x86_64 glibc-headers-2.28-164.el8_5.3.x86_64 glibc-langpack-en-2.28-164.el8_5.3.x86_64 libxml2-2.9.7-12.el8_5.x86_64 python3-libxml2-2.9.7-12.el8_5.x86_64 expat-2.2.5-4.el8_5.3.x86_64 openssl-1:1.1.1k-6.el8_5.x86_64 openssl-libs-1:1.1.1k-6.el8_5.x86_64
---	---

Security vulnerabilities resolved in System Manager 10.1 Security Service Pack SSP #2 release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-69502	kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2022:0825	CVE-2021-0920 CVE-2021-4154 CVE-2022-0330 CVE-2022-0435 CVE-2022-0492 CVE-2022-0516 CVE-2022-0847 CVE-2022-22942	Important	ASA-2022-028	High
SMGR-69504	libarchive	RHSA-2022:0892	CVE-2021-23177 CVE-2021-31566	Moderate	NA	NA
SMGR-69506	vim-common vim-enhanced vim-filesystem vim-minimal	RHSA-2022:0894	CVE-2022-0261 CVE-2022-0318 CVE-2022-0359 CVE-2022-0361 CVE-2022-0392 CVE-2022-0413	Moderate	ASA-2022-030	High
SMGR-69508	glibc glibc-all-langpacks glibc-common glibc-devel glibc-headers glibc-langpack-en	RHSA-2022:0896	CVE-2021-3999 CVE-2022-23218 CVE-2022-23219	Moderate	ASA-2022-074	High
SMGR-69510	libxml2 python3-libxml2	RHSA-2022:0899	CVE-2022-23308	Moderate	ASA-2022-033	High
SMGR-69512	expat	RHSA-2022:0951	CVE-2021-45960 CVE-2021-46143 CVE-2022-22822 CVE-2022-22823 CVE-2022-22824 CVE-2022-22825 CVE-2022-22826	Important	ASA-2022-031	Critical

			CVE-2022-22827 CVE-2022-23852 CVE-2022-25235 CVE-2022-25236 CVE-2022-25315			
SMGR-69514	openssl openssl-lib	RHSA-2022:1065	CVE-2022-0778	Important	ASA-2022-036	High

System Manager 10.1.0.1 (10.1.0.0 Service Pack 1) release includes the following rpm updates:

aide-0.16-14.el8_5.1.x86_64 cryptsetup-2.3.3-4.el8_5.1.x86_64 cryptsetup-libs-2.3.3-4.el8_5.1.x86_64 cyrus-sasl-2.1.27-6.el8_5.x86_64 cyrus-sasl-lib-2.1.27-6.el8_5.x86_64 glibc-2.28-164.el8.i686 java-1.8.0-openjdk-1:1.8.0.322.b06-2.el8_5.x86_64 java-1.8.0-openjdk-devel-1:1.8.0.322.b06-2.el8_5.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.322.b06-2.el8_5.x86_64 kernel-4.18.0-348.12.2.el8_5.x86_64 kernel-4.18.0-348.7.1.el8_5.x86_64 kernel-core-4.18.0-348.12.2.el8_5.x86_64 kernel-core-4.18.0-348.7.1.el8_5.x86_64 kernel-headers-4.18.0-348.12.2.el8_5.x86_64 kernel-headers-4.18.0-348.7.1.el8_5.x86_64 kernel-modules-4.18.0-348.12.2.el8_5.x86_64 kernel-modules-4.18.0-348.7.1.el8_5.x86_64 kernel-tools-4.18.0-348.12.2.el8_5.x86_64 kernel-tools-4.18.0-348.7.1.el8_5.x86_64 kernel-tools-libs-4.18.0-348.12.2.el8_5.x86_64 kernel-tools-libs-4.18.0-348.7.1.el8_5.x86_64 libgcc-8.5.0-3.el8.i686 libgcc-8.5.0-4.el8_5.i686	libstdc++-8.5.0-3.el8.i686 libstdc++-8.5.0-4.el8_5.i686 nss-3.67.0-7.el8_5.x86_64 nss-softokn-3.67.0-7.el8_5.x86_64 nss-softokn-freebl-3.67.0-7.el8_5.x86_64 nss-sysinit-3.67.0-7.el8_5.x86_64 nss-util-3.67.0-7.el8_5.x86_64 openssl-1:1.1.1k-5.el8_5.x86_64 openssl-libs-1:1.1.1k-5.el8_5.x86_64 polkit-0.115-13.el8_5.1.x86_64 polkit-libs-0.115-13.el8_5.1.x86_64 python3-perf-4.18.0-348.12.2.el8_5.x86_64 python3-perf-4.18.0-348.7.1.el8_5.x86_64 python3-rpm-4.14.3-19.el8_5.2.x86_64 rpm-4.14.3-19.el8_5.2.x86_64 rpm-build-libs-4.14.3-19.el8_5.2.x86_64 rpm-libs-4.14.3-19.el8_5.2.x86_64 rpm-plugin-selinux-4.14.3-19.el8_5.2.x86_64 rpm-plugin-systemd-inhibit-4.14.3-19.el8_5.2.x86_64 vim-common-2:8.0.1763-16.el8_5.4.x86_64 vim-enhanced-2:8.0.1763-16.el8_5.4.x86_64 vim-filesystem-2:8.0.1763-16.el8_5.4.noarch vim-minimal-2:8.0.1763-16.el8_5.4.x86_64
---	---

Security vulnerabilities resolved in System Manager 10.1.0.1 (10.1.0.0 Service Pack 1) release:

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
SMGR-69443	aide	RHSA-2022:0441	CVE-2021-45417	Important	ASA-2022-021	High
SMGR-69441	cryptsetup cryptsetup-libs	RHSA-2022:0370	CVE-2021-4122	Moderate	ASA-2022-019	Medium
SMGR-69445	cyrus-sasl cyrus-sasl-lib	RHSA-2022:0658	N/A	Important	N/A	N/A
SMGR-69419	glibc	RHSA-2021:4358	CVE-2021-35942 CVE-2021-27645 CVE-2021-33574	Moderate	ASA-2021-172	Critical

SMGR-69435	java-1.8.0-openjdk java-1.8.0-openjdk-dlevel java-1.8.0-openjdk-headless	RHSA-2022:0307	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-2022-008	Medium
SMGR-69431	kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs	RHSA-2022:0188	CVE-2021-4155 CVE-2022-0185	Important	ASA-2022-006	High
SMGR-69429	kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs	RHSA-2021:5227	CVE-2021-20321	Moderate	ASA-2021-187	Medium
SMGR-69421	libgcc libstdc++	RHSA-2021:4386	CVE-2018-20673	Low	ASA-2021-170	Medium
SMGR-69423	libgcc libstdc++	RHSA-2021:4587	CVE-2021-42574	Moderate	ASA-2021-164	High
SMGR-69425	nss nss-softokn nss-softokn-freebl nss-sysinit nss-util	RHSA-2021:4903	CVE-2021-43527	Critical	ASA-2021-181	High
SMGR-69427	openssl openssl-libs	RHSA-2021:5226	CVE-2021-3712	Moderate	ASA-2022-002	High
SMGR-69433	polkit polkit-libs	RHSA-2022:0267	CVE-2021-4034	Important	ASA-2022-007	High
SMGR-69431	python3-perf	RHSA-2022:0188	CVE-2021-4155 CVE-2022-0185	Important	ASA-2022-006	High
SMGR-69429	python3-perf	RHSA-2021:5227	CVE-2021-20321	Moderate	ASA-2021-187	Medium
SMGR-69439	python3 rpm rpm-build-libs rpm-libs rpm-plugin-selinux rpm-plugin-systemd-inhabit	RHSA-2022:0368	CVE-2021-3521	Moderate	ASA-2022-016	Medium
SMGR-69437	vim-common vim-enhanced vim-filesystem vim-minimal	RHSA-2022:0366	CVE-2021-3872 CVE-2021-3984 CVE-2021-4019 CVE-2021-4192 CVE-2021-4193	Moderate	ASA-2022-015	High

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](#).