Product Correction Notice (PCN)

Issue Date:	**18-April-2022**
Supplement Date:	**22-April-2024**
Expiration Date:	**NA**
PCN Number:	**2136S**

SECTION 1 - CUSTOMER NOTICE

Products affected by this PCN:

Avaya Aura® Session Manager 10.1 vAppliance running on Avaya provided servers: Avaya Solutions 130 R5.x (Dell® PowerEdge R640), Solutions Platform S8300E R5.1; and vAppliance running on customer provided VMware® certified hardware.
Reference the Avaya Aura® Platform Offer Definition for details.

Description:

CRITICAL: The Security Service Pack installation framework for Session Manager has changed in Release 10.1.x. It is imperative that the instructions in this PCN be reviewed for complete steps prior to installation of Security Service Packs on a Session Manager 10.1.x system.

22 April 2024 - Supplement 22 of this PCN introduces **Avaya Aura Session Manager 10.1 Security Service Pack #23**

- **(AV-SM10.1-RHEL8.4-SSP-023-01.tar.bz2; PLDS ID SM000000301).**
- Session Manager 10.1 SSP #23 is applicable to Session Manager/Branch Session Manager 10.1.0.1 or later.
- SM Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 10.1.0.1 or later Service Pack/Feature Pack does NOT contain any Red Hat security updates. SSP #23 must be installed** after applying the Service Pack to ensure robust security protection. Reference **PCN2135S** for additional details on the Session Manager 10.1.x Service Pack.
- SSP installation will fail unless Service Pack 10.1.0.1 or later is installed first.
- If SSP #3 is installed, SSP #23 must be applied as soon as possible to address the issues noted in **PSN020574u** and before applying any additional Service Packs
- 10.1 SSPs will not work on the 10.2 release and there will be different SSPs for both 10.1 and 10.2.

18 March 2024 - Supplement 21 of this PCN introduces **Avaya Aura Session Manager 10.1 Security Service Pack #22**

- **(AV-SM10.1-RHEL8.4-SSP-022-01.tar.bz2; PLDS ID SM000000299).**
- Session Manager 10.1 SSP #22 is applicable to Session Manager/Branch Session Manager 10.1.0.1 or later.
- SM Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 10.1.0.1 or later Service Pack/Feature Pack does NOT contain any Red Hat security updates. SSP #22 must be installed** after applying the Service Pack to ensure robust security protection. Reference **PCN2135S** for additional details on the Session Manager 10.1.x Service Pack.
- SSP installation will fail unless Service Pack 10.1.0.1 or later is installed first.
- If SSP #3 is installed, SSP #22 must be applied as soon as possible to address the issues noted in **PSN020574u** and before applying any additional Service Packs
- 10.1 SSPs will not work on the 10.2 release and there will be different SSPs for both 10.1 and

10.2.

16 January 2024 - Supplement 20 of this PCN introduces **Avaya Aura Session Manager 10.1 Security Service Pack #21**

- **(AV-SM10.1-RHEL8.4-SSP-021-01.tar.bz2; PLDS ID SM000000296).**
- Session Manager 10.1 SSP #21 is applicable to Session Manager/Branch Session Manager 10.1.0.1 or later.
- SM Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 10.1.0.1 or later Service Pack/Feature Pack does NOT contain any Red Hat security updates. SSP #21 must be installed** after applying the Service Pack to ensure robust security protection. Reference **PCN2135S** for additional details on the Session Manager 10.1.x Service Pack.
- SSP installation will fail unless Service Pack 10.1.0.1 or later is installed first.
- If SSP #3 is installed, SSP #21 must be applied as soon as possible to address the issues noted in **PSN020574u** and before applying any additional Service Packs
- 10.1 SSPs will not work on the 10.2 release and there will be different SSPs for both 10.1 and 10.2.

18-December-2023- Supplement 19 of this PCN introduces **Avaya Aura Session Manager 10.1 Security Service Pack #20**

- **(AV-SM10.1-RHEL8.4-SSP-020-01.tar.bz2; PLDS ID SM000000291).**
- Session Manager 10.1 SSP #20 is applicable to Session Manager/Branch Session Manager 10.1.0.1 or later.
- SM Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 10.1.0.1 or later Service Pack/Feature Pack does NOT contain any Red Hat security updates. SSP #20 must be installed** after applying the Service Pack to ensure robust security protection. Reference **PCN2135S** for additional details on the Session Manager 10.1.x Service Pack.
- SSP installation will fail unless Service Pack 10.1.0.1 or later is installed first.
- If SSP #3 is installed, SSP #20 must be applied as soon as possible to address the issues noted in **PSN020574u** and before applying any additional Service Packs
- 10.1 SSPs will not work on the 10.2 release and there will be different SSPs for both 10.1 and 10.2.

20-November-2023- Supplement 18 of this PCN introduces **Avaya Aura Session Manager 10.1 Security Service Pack #19**

- **(AV-SM10.1-RHEL8.4-SSP-019-01.tar.bz2; PLDS ID SM000000288).**
- Session Manager 10.1 SSP #19 is applicable to Session Manager/Branch Session Manager 10.1.0.1 or later.
- SM Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 10.1.0.1 or later Service Pack/Feature Pack does NOT contain any Red Hat security updates. SSP #19 must be installed** after applying the Service Pack to ensure robust security protection. Reference **PCN2135S** for additional details on the Session Manager 10.1.x Service Pack.
- SSP installation will fail unless Service Pack 10.1.0.1 or later is installed first.
- If SSP #3 is installed, SSP #19 must be applied as soon as possible to address the issues noted in **PSN020574u** and before applying any additional Service Packs

16-October-2023- Supplement 17 of this PCN introduces **Avaya Aura Session Manager 10.1 Security Service Pack #18**

- **(AV-SM10.1-RHEL8.4-SSP-018-01.tar.bz2; PLDS ID SM000000287).**
- Session Manager 10.1 SSP #18 is applicable to Session Manager/Branch Session Manager 10.1.0.1 or later.
- SM Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 10.1.0.1 or later Service Pack/Feature Pack does NOT contain any Red Hat security updates. SSP #18 must be installed** after applying the Service Pack to ensure robust security protection. Reference **PCN2135S** for additional details on the Session Manager 10.1.x Service Pack.
- SSP installation will fail unless Service Pack 10.1.0.1 or later is installed first.
- If SSP #3 is installed, SSP #18 must be applied as soon as possible to address the issues noted in **PSN020574u** and before applying any additional Service Packs.

18-September-2023- Supplement 16 of this PCN introduces **Avaya Aura Session Manager 10.1 Security Service Pack #17**

- **(AV-SM10.1-RHEL8.4-SSP-017-01.tar.bz2; PLDS ID SM000000284).**
- Session Manager 10.1 SSP #17 is applicable to Session Manager/Branch Session Manager 10.1.0.1 or later.
- SM Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 10.1.0.1 or later Service Pack/Feature Pack does NOT contain any Red Hat security updates. SSP #17 must be installed** after applying the Service Pack to ensure robust security protection. Reference **PCN2135S** for additional details on the Session Manager 10.1.x Service Pack.
- SSP installation will fail unless Service Pack 10.1.0.1 or later is installed first.
- If SSP #3 is installed, SSP #17 must be applied as soon as possible to address the issues noted in **PSN020574u** and before applying any additional Service Packs.

28-August-2023- Supplement 15 of this PCN introduces **Avaya Aura Session Manager 10.1 Security Service Pack #16**

- **(AV-SM10.1-RHEL8.4-SSP-016-02.tar.bz2; PLDS ID SM000000279).**
- Session Manager 10.1 SSP #16 is applicable to Session Manager/Branch Session Manager 10.1.0.1 or later.
- SM Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 10.1.0.1 or later Service Pack/Feature Pack does NOT contain any Red Hat security updates. SSP #16 must be installed** after applying the Service Pack to ensure robust security protection. Reference **PCN2135S** for additional details on the Session Manager 10.1.x Service Pack.
- SSP installation will fail unless Service Pack 10.1.0.1 or later is installed first.
- If SSP #3 is installed, SSP #16 must be applied as soon as possible to address the issues noted in **PSN020574u** and before applying any additional Service Packs.

17-July-2023- Supplement 14 of this PCN introduces **Avaya Aura Session Manager 10.1 Security Service Pack #15**

- **(AV-SM10.1-RHEL8.4-SSP-015-02.tar.bz2; PLDS ID SM000000276).**
- Session Manager 10.1 SSP #15 is applicable to Session Manager/Branch Session Manager 10.1.0.1 or later.

- SM Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 10.1.0.1 or later Service Pack/Feature Pack does NOT contain any Red Hat security updates. SSP #15 must be installed** after applying the Service Pack to ensure robust security protection. Reference **PCN2135S** for additional details on the Session Manager 10.1.x Service Pack.
- SSP installation will fail unless Service Pack 10.1.0.1 or later is installed first.
- If SSP #3 is installed, SSP #15 must be applied as soon as possible to address the issues noted in **PSN020574u** and before applying any additional Service Packs.

20-June-2023- Supplement 13 of this PCN introduces **Avaya Aura Session Manager 10.1 Security Service Pack #14**

- **(AV-SM10.1-RHEL8.4-SSP-014-01.tar.bz2; PLDS ID SM000000272).**
- Session Manager 10.1 SSP #14 is applicable to Session Manager/Branch Session Manager 10.1.0.1 or later.
- SM Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 10.1.0.1 or later Service Pack/Feature Pack does NOT contain any Red Hat security updates. SSP #14 must be installed** after applying the Service Pack to ensure robust security protection. Reference **PCN2135S** for additional details on the Session Manager 10.1.x Service Pack.
- SSP installation will fail unless Service Pack 10.1.0.1 or later is installed first.
- If SSP #3 is installed, SSP #14 must be applied as soon as possible to address the issues noted in **PSN020574u** and before applying any additional Service Packs.

22-May-2023- Supplement 12 of this PCN introduces **Avaya Aura Session Manager 10.1 Security Service Pack #13**

- **(AV-SM10.1-RHEL8.4-SSP-013-01.tar.bz2; PLDS ID SM000000268).**
- Session Manager 10.1 SSP #13 is applicable to Session Manager/Branch Session Manager 10.1.0.1 or later.
- SM Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 10.1.0.1 or later Service Pack/Feature Pack does NOT contain any Red Hat security updates. SSP #13 must be installed** after applying the Service Pack to ensure robust security protection. Reference **PCN2135S** for additional details on the Session Manager 10.1.x Service Pack.
- SSP installation will fail unless Service Pack 10.1.0.1 or later is installed first.
- If SSP #3 is installed, SSP #13 must be applied as soon as possible to address the issues noted in **PSN020574u** and before applying any additional Service Packs.

17-April-2023- Supplement 11 of this PCN introduces **Avaya Aura Session Manager 10.1 Security Service Pack #12**

- **(AV-SM10.1-RHEL8.4-SSP-012-01.tar.bz2; PLDS ID SM000000265).**
- Session Manager 10.1 SSP #12 is applicable to Session Manager/Branch Session Manager 10.1.0.1 or later.
- SM Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 10.1.0.1 or later Service Pack/Feature Pack does NOT contain any Red Hat security updates. SSP #12 must be installed** after applying the Service Pack to ensure robust security protection. Reference **PCN2135S** for additional details on the Session Manager 10.1.x Service Pack.
- SSP installation will fail unless Service Pack 10.1.0.1 or later is installed first.

- If SSP #3 is installed, SSP #12 must be applied as soon as possible to address the issues noted in **PSN020574u** and before applying any additional Service Packs.

20-March-2023- Supplement 10 of this PCN introduces **Avaya Aura Session Manager 10.1 Security Service Pack #11**

- **(AV-SM10.1-RHEL8.4-SSP-011-01.tar.bz2; PLDS ID SM000000261).**
- Session Manager 10.1 SSP #11 is applicable to Session Manager/Branch Session Manager 10.1.0.1 or later.
- SM Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 10.1.0.1 or later Service Pack/Feature Pack does NOT contain any Red Hat security updates. SSP #11 must be installed** after applying the Service Pack to ensure robust security protection. Reference **PCN2135S** for additional details on the Session Manager 10.1.x Service Pack.
- SSP installation will fail unless Service Pack 10.1.0.1 or later is installed first.
- If SSP #3 is installed, SSP #11 must be applied as soon as possible to address the issues noted in **PSN020574u** and before applying any additional Service Packs.
- 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.

23-January-2023- Supplement 9 of this PCN introduces **Avaya Aura Session Manager 10.1 Security Service Pack #10**

- **(AV-SM10.1-RHEL8.4-SSP-010-01.tar.bz2; PLDS ID SM000000253).**
- Session Manager 10.1 SSP #10 is applicable to Session Manager/Branch Session Manager 10.1.0.1 and 10.1.0.2
- SM Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 10.1.0.1 or 10.1.0.2 Service Pack does NOT contain any Red Hat security updates. SSP #10 must be installed** after applying the Service Pack to ensure robust security protection. Reference **PCN2135S** for additional details on the Session Manager 10.1.x Service Pack.
- SSP installation will fail unless Service Pack 10.1.0.1 or 10.1.0.2 is installed first.
- If SSP #3 is installed, SSP #10 must be applied as soon as possible to address the issues noted in **PSN020574u** and before applying any additional Service Packs.

19-December-2022- Supplement 8 of this PCN introduces **Avaya Aura Session Manager 10.1 Security Service Pack #9**

- **(AV-SM10.1-RHEL8.4-SSP-009-01.tar.bz2; PLDS ID SM000000251).**
- Session Manager 10.1 SSP #9 is applicable to Session Manager/Branch Session Manager 10.1.0.1 and 10.1.0.2
- SM Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 10.1.0.1 or 10.1.0.2 Service Pack does NOT contain any Red Hat security updates. SSP #9 must be installed** after applying the Service Pack to ensure robust security protection. Reference **PCN2135S** for additional details on the Session Manager 10.1.x Service Pack.
- SSP installation will fail unless Service Pack 10.1.0.1 or 10.1.0.2 is installed first.
- If SSP #3 is installed, SSP #9 must be applied as soon as possible to address the issues noted in **PSN020574u** and before applying any additional Service Packs.

28-November-2022- Supplement 7 of this PCN introduces **Avaya Aura Session Manager 10.1 Security Service Pack #8**

- **(AV-SM10.1-RHEL8.4-SSP-008-01.tar.bz2; PLDS ID SM000000248).**
- Session Manager 10.1 SSP #8 is applicable to Session Manager/Branch Session Manager 10.1.0.1 and 10.1.0.2
- SM Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 10.1.0.1 or 10.1.0.2 Service Pack does NOT contain any Red Hat security updates. SSP #8 must be installed** after applying the Service Pack to ensure robust security protection. Reference **PCN2135S** for additional details on the Session Manager 10.1.x Service Pack.
- SSP installation will fail unless Service Pack 10.1.0.1 or 10.1.0.2 is installed first.
- If SSP #3 is installed, SSP #8 must be applied as soon as possible to address the issues noted in **PSN020574u** and before applying any additional Service Packs.

17-October-2022- Supplement 6 of this PCN introduces **Avaya Aura Session Manager 10.1 Security Service Pack #7**

- **(AV-SM10.1-RHEL8.4-SSP-007-01.tar.bz2; PLDS ID SM000000245).**
- Session Manager 10.1 SSP #7 is applicable to Session Manager/Branch Session Manager 10.1.0.1 and 10.1.0.2
- SM Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 10.1.0.1 or 10.1.0.2 Service Pack does NOT contain any Red Hat security updates. SSP #7 must be installed** after applying the Service Pack to ensure robust security protection. Reference **PCN2135S** for additional details on the Session Manager 10.1.x Service Pack.
- SSP installation will fail unless Service Pack 10.1.0.1 or 10.1.0.2 is installed first.
- If SSP #3 is installed, SSP #7 must be applied as soon as possible to address the issues noted in **PSN020574u** and before applying any additional Service Packs.

26-September-2022- Supplement 5 of this PCN introduces **Avaya Aura Session Manager 10.1 Security Service Pack #6**

- **(AV-SM10.1-RHEL8.4-SSP-006-01.tar.bz2; PLDS ID SM000000240).**
- Session Manager 10.1 SSP #6 is applicable to Session Manager/Branch Session Manager 10.1.0.1 and 10.1.0.2
- SM Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 10.1.0.1 or 10.1.0.2 Service Pack does NOT contain any Red Hat security updates. SSP #6 must be installed** after applying the Service Pack to ensure robust security protection. Reference **PCN2135S** for additional details on the Session Manager 10.1.x Service Pack.
- SSP installation will fail unless Service Pack 10.1.0.1 or 10.1.0.2 is installed first.
- If SSP #3 is installed and SSP #4 or #5 was not installed, SSP #6 must be applied as soon as possible to address the issues noted in **PSN020574u** and before applying any additional Service Packs.

16-August-2022- Supplement 4 of this PCN introduces **Avaya Aura Session Manager 10.1 Security**

Service Pack #5

- **(AV-SM10.1-RHEL8.4-SSP-005-02.tar.bz2; PLDS ID SM000000239).**
- This Security Service Pack is only applicable to SM 10.1.0.1.
- Session Manager 10.1 SSP #5 is applicable to Session Manager/Branch Session Manager 10.1.0.1.
- SM Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 10.1.0.1 Service Pack does NOT contain any Red Hat security updates. SSP #5 must be installed** after applying the 10.1.0.1 Service Pack to ensure robust security protection. Reference **PCN2135S** for additional details on the Session Manager 10.1.0.1 Service Pack.
- SSP installation will fail unless Service Pack 10.1.0.1 is installed first.
- If SSP #3 is installed and SSP #4 was not installed, SSP #5 must be applied as soon as possible to address the issues noted in **PSN020574u** and before applying any additional Service Packs.

22-July-2022- Supplement 3 of this PCN introduces **Avaya Aura Session Manager 10.1 Security Service Pack #4**

- **(AV-SM10.1-RHEL8.4-SSP-004-03.tar.bz2; PLDS ID SM000000237).**
- This Security Service Pack is only applicable to SM 10.1.0.1.
- Session Manager 10.1 SSP #4 is applicable to Session Manager/Branch Session Manager 10.1.0.1.
- SM Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 10.1.0.1 Service Pack does NOT contain any Red Hat security updates. SSP #4 must be installed** after applying the 10.1.0.1 Service Pack to ensure robust security protection. Reference **PCN2135S** for additional details on the Session Manager 10.1.0.1 Service Pack.
- SSP installation will fail unless Service Pack 10.1.0.1 is installed first.
- If SSP #3 is already installed, SSP #4 **must** be applied as soon as possible to address the issues noted in **PSN020574u** and before applying any additional Service Packs.

06-July-2022- Supplement 2-1

- **ALERT!! : SSP #3, which includes OpenJDK updates, results in Cassandra/User Data Storage issues. For now, this SSP is disabled from the support site. Reference PSN020574u for additional details.**

21-June-2022- Supplement 2 of this PCN introduces an **Avaya Aura Session Manager 10.1 Security Service Pack #3**

- **~~(AV-SM10.1-RHEL8.4-SSP-003-02.tar.bz2; PLDS ID SM000000234).~~**
- This Security Service Pack is only applicable to SM 10.1.0.1.
- Session Manager 10.1 SSP #3 is applicable to Session Manager/Branch Session Manager 10.1.0.1.
- SM Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 10.1.0.1 Service Pack does NOT contain any Red Hat security updates. SSP #3 must be installed** after applying the 10.1.0.1 Service Pack to ensure robust security protection. Reference **PCN2135S** for additional details on the Session Manager 10.1.0.1 Service Pack.
- SSP installation will fail unless Service Pack 10.1.0.1 is installed first.

- Reference the “***Finding the installation instructions***” section of this PCN for detailed installation instructions.
- *Disabled – see Supplement 2-1 above.*

16-May-2022- Supplement 1 of this PCN introduces an **Avaya Aura Session Manager 10.1 Security Service Pack #2**

- **(AV-SM10.1-RHEL8.4-SSP-002-01.tar.bz2;   PLDS ID SM000000232).**
- This Security Service Pack is only applicable to SM 10.1.0.1.
- Session Manager 10.1 SSP #2 is applicable to Session Manager/Branch Session Manager 10.1.0.1.
- SM Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 10.1.0.1 Service Pack does NOT contain any Red Hat security updates. SSP #2 must be installed** after applying the 10.1.0.1 Service Pack to ensure robust security protection. Reference **PCN2135S** for additional details on the Session Manager 10.1.0.1 Service Pack.
- SSP installation will fail unless Service Pack 10.1.0.1 is installed first.
- Reference the “***Finding the installation instructions***” section of this PCN for detailed installation instructions.

18-April-2022– This PCN introduces **Avaya Aura Session Manager 10.1 Security Service Pack #1**

- **(AV-SM10.1-RHEL8.4-SSP-001-01.tar.bz2;   PLDS ID SM000000229).**
- This Security Service Pack is only applicable to SM 10.1.0.1.
- Session Manager 10.1 SSP #1 is applicable to Session Manager/Branch Session Manager 10.1.0.1
- SM Security Service Packs should NOT be applied on the Software Only Offer.
- **Critical Note: Session Manager 10.1.0.1 Service Pack does NOT contain any Red Hat security updates. SSP #1 must be installed** after applying the 10.1.0.1 Service Pack to ensure robust security protection. Reference **PCN2135S** for additional details on the Session Manager 10.1.0.1 Service Pack.
- SSP installation will fail unless Service Pack 10.1.0.1 is installed first.
- Reference the “***Finding the installation instructions***” section of this PCN for detailed installation instructions.

Level of Risk/Severity **Class 1=High** **Class 2=Medium** **Class 3=Low**	Class 2
Is it required that this PCN be applied to my system?	This PCN is required for Session Manager 10.1.x. It is not applicable to the Software Only offer. **SSP #23 must be installed** after applying the 10.1.0.1 or later Service Pack to ensure robust security protection.
The risk if this PCN	The system will be exposed to the security vulnerabilities referenced in Section 1B.

is not installed:

Is this PCN for US customers, non-US customers, or both?

This applies to both US and non-US customers.

Does applying this PCN disrupt my service during installation?

This security service Pack will disrupt service in that it requires a system reboot to take effect. Since Session Manager runs in an active-active environment, when multiple Session Manager instances are in a network, the servers should be updated one at a time to minimize any service impact. If only one Session Manager server is in the configuration, service will be impacted during the upgrade time, and should be planned for accordingly.

Installation of this PCN is required by:

Customer and/or (Avaya Remote or On-Site Services) and/or Avaya Authorized Business Partner.

Release notes and workarounds are located:

The **Security Service Pack** resolves vulnerabilities described by Avaya Security Advisories (ASA) referenced in section 1B – Security information.
NOTE: The Avaya Security Advisory (ASA) process is being reworked to provide more timely updates. As that process is finalized, this PCN will be updated to reflect the new process and associated ASA information

The ASAs referenced in section 1B can be viewed by performing the following steps in a browser:

1. Go to http://support.avaya.com then enter your **Username** and **Password** and **LOG IN.**
2. Mouse over Search at the top of the page.
3. Type the ASA number of interest into the search field and Enter.
4. Click on the Security Advisory document link to read the Avaya Security Advisory.

You can also access the ASAs by performing the following steps from a browser:

1. Go to http://support.avaya.com then enter your **Username** and **Password** and **LOG IN.**
2. Scroll to the bottom of the page and click **Community -> Avaya Security**.
3. Click on the link for the year the security advisory was published, which is part of the ASA number.
4. Page through the advisory numbers to find the link of interest.

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

The **Avaya Aura® Session Manager Release 10.1 Release Notes** can be obtained by performing the following steps from a browser:
1. Go to http://support.avaya.com
2. Search for the document titled "**Avaya Aura® 10.1.x.x Release Notes**".

What materials are required to implement this PCN (If PCN can be customer installed):

This PCN is being issued as a customer installable PCN. The specified Session Manager files are required. To obtain the update files refer to the **How do I order this PCN** section of this PCN.

If unfamiliar with installing Session Manager security updates, the installation instructions are required. To obtain the installation instructions please refer to the **Finding the installation instructions** section of this PCN

How do I order this PCN (If PCN can be customer installed):

Software can be downloaded directly from support.avaya.com. No order is required.
The Security Service Pack can be downloaded by performing the following steps from a browser:

1. Go to http://support.avaya.com then enter your **Username** and **Password** and click **LOG IN.**
2. Mouse over **Search Product** at the top of the page.
3. Begin to type **Session Manager** and when Avaya Aura® Session Manager appears as a selection below, select it.
4. Select 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® Session Manager 10.1.x Security Service Pack.**
7. Scroll down the page to find the download link for the required Security Service Pack. This link will take you to the PLDS system with the **Download pub ID** already entered.
8. Select the **Download** link in PLDS to begin the download.

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

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

PLDS Hints:

1. In the PLDS **View Downloads** section under the **Suggested Downloads** tab, select **Session Manager** in the **Product Line** search field to display frequently downloaded Session Manager software, including recent Service Packs and other software updates.
2. All Session Manager 10.1.x software downloads are available on PLDS. In the PLDS **View Downloads** section under the **Search by Download** tab, select **Session Manager** in the **Application** search field and **10.1** in the **Version** search field to display all available Session 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):

CRITICAL: The Security Service Pack installation framework for SM has changed in Release 10.1.x. It is imperative that the instructions in this PCN be reviewed for complete steps prior to installation of Security Service Packs on an SM 10.1.x system.
With this release Avaya introduces a common version on RedHat Enterprise Linux (RHEL 8.4) to its Avaya Aura platform. Common versions of RPMs are supported and consumed by the components. This results in a change to how security updates are provided for SM.
Important Security Service Pack Installation Notes:

1. The SSP update process will utilize the new Common framework that provides a new "*av-update-os*" command and new "*av-version*" command that will show the SSP version currently running on SM.
2. The SSP can be activated/applied using command line only.
3. Installing Session Manager Security Service Pack through Solution Deployment Manager (SDM) is not supported.
4. SSPs should NOT be installed on Session Manager 10.1.x Software Only deployments.
5. Security Service Packs are cumulative for the release they apply to. The current Security Service Pack for a release will include the fixes from all previous Security Service Packs for that release.

Installation using CLI

6. Ensure that a maintenance window has been obtained.
7. Ensure that **SM Service Pack #1** (10.1.0.1) or later service pack is installed.
8. Download the Security Service Pack binary from PLDS and copy it in the customer account home directory. (e.g. /home/cust) on SM.
9. Take a VM snapshot and Session Manager application backup prior to making changes.
10. Place the SM in **Deny New Service**.
    a. On the home page of the System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
    c. Click **Service State**.
    d. From the drop-down list box, select **Deny New Service.**
    e. Before updating on the confirmation page, click **Confirm.** On the **Session Manager Dashboard** page, wait until **Active Call Count** is zero. Refresh the screen to update the count.
11. Login to the SM CLI utilizing customer account, root or sroot credentials. Other services logins (init, inads, craft) do not have permissions to install the SSP.
12. Change directory to where the SSP was copied (e.g. /home/cust).
13. Ensure the MD5sum matches what is provided in the PLDS Download ID description.
14. Execute the following command to install the SSP. Note that there is NO prompt to ask if you want to proceed. Output of the installation is written to a log file under /var/log/avaya with the name of the SSP and the date/timestamp. Following example is for SSP #18.

    # av-update-os /home/cust/AV-SM10.1-RHEL8.4-SSP-023-01.tar.bz2

    Syntax for SSP file name

    AV-<product name><mainline release version>-RHEL<number>-SSP-<SSP #>-<build #>.tar.bz2

    AV: stands for Avaya
    <product name>: this will define the product for which the SSP is targeted
    <Mainline release version>: this is mainline release version for the product eg: 10.1
    RHEL <number>: base RHEL being used in our application, e.g., 8.4
    SSP-<SSP #>: this is a 3-digit number that defines the SSP version
    <build #>: this is a 2-digit number that defines the build number of the SSP

15. Confirmation of successful update will be shown, and the system will go for automatic reboot.
16. After reboot, on the home page of System Manager Web Console, Under **Elements**, click **Session Manager.** For the SM, verify that all tests are passing, entity links are up, data replication, and user data storage (core SMs only).

17. Remove the VM snapshot.
18. Place the SM in **Accept New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
    c. From the drop-down list box, select **Accept New Service**
    d. Before updating on the confirmation page, click **Confirm.** On the **Session Manager Dashboard** page, wait until **Active Call Count** is zero. Refresh the screen to update the count.

SECTION 1A – SOFTWARE FEATURE PACK INFORMATION

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

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

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

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

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

```
ID                     Version        Status    Summary
---------------------- -------------- --------- --------------------------------
AV-SM-RHEL8-SSP-023    01             installed Security Service Pack #23
```

The Command Line Interface (CLI) can also be utilized to run the command "*av-version*" on the server.

```
[root@]# av-version
-------------------------------------
OS_VERSION: Red Hat Enterprise Linux release 8.4 (Ootpa)
AV_SSP_VERSION : 023
AV_BUILD_NUMBER : 01
```

What you should do if the Software installation fails?

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

How to remove the Software if malfunction of your system

The **Upgrading Avaya Aura® Session Manager** document and **Upgrading and Migrating Avaya Aura® Applications to 10.1** contains instructions on how to upgrade Session Manager release 10.1.X and later systems to release 10.1.0.1, and can be obtained by performing the following steps from a browser:

occurs:	1. Go to http://support.avaya.com 2. Click on **Documents** in the top menu bar 3. In the Enter Your Product Here box, enter “**Session Manager**”, select release “**10.1.x”** in the pull-down list, and select the **“Installation, Upgrades & Config”** checkbox in the Content Type box on the left. Then click the “**ENTER**” button to display a list of documents. 4. Search for the document titled “**Upgrading Avaya Aura® Session Manager”** & **“Upgrading and Migrating Avaya Aura® Applications to 10.1”** **Contact Avaya Services for assistance if the system is not operating properly after the upgrade to this release. Alternatively, a rollback can be performed by re-installing all software on the Session Manager server per the server replacement procedures in the Maintenance and Troubleshooting guide.**

SECTION 1B – SECURITY INFORMATION

Security Notes	In keeping with NIST guidelines and industry best practices, Avaya is rotating the security keys associated with remote maintenance access through the Access Security Gateway.
Are there any Security risks involved?	Issues described by the 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 SM release.
Avaya Security Vulnerability Classification:	***The Avaya Security Advisory (ASA) process is being reworked to provide more timely updates. As that process is finalized, this PCN will be updated to reflect the new process and associated ASA information.***

SM 10.1 Security Service Pack #23 includes the following rpm updates:

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-modules-4.18.0-513.18.1.el8_9.x86_64.rpm oniguruma-6.8.2-2.1.el8_9.x86_64.rpm	perf-4.18.0-513.18.1.el8_9.x86_64.rpm 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 SM 10.1 Security Service Pack #23

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-92851	python3-unbound unbound-libs	RHSA-2024:0965	CVE-2023-50387 CVE-2023-50868	Important	None	None

ASM-92849	kernel kernel-core kernel-modules perf	RHSA-2024:0897	CVE-2022-3545 CVE-2022-41858 CVE-2023-1073 CVE-2023-1838 CVE-2023-2166 CVE-2023-2176 CVE-2023-4623 CVE-2023-4921 CVE-2023-5717 CVE-2023-6356 CVE-2023-6535 CVE-2023-6536 CVE-2023-6606 CVE-2023-6610 CVE-2023-6817 CVE-2023-40283 CVE-2023-45871 CVE-2023-46813 CVE-2024-0646	Important	None	None
ASM-92850	oniguruma	RHSA-2024:0889	CVE-2019-13224 CVE-2019-16163 CVE-2019-19012 CVE-2019-19203 CVE-2019-19204	Moderate	None	None

SM 10.1 Security Service Pack #22 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-4.18.0-513.11.1.el8_9.x86_64.rpm
kernel-core-4.18.0-513.11.1.el8_9.x86_64.rpm
kernel-modules-4.18.0-513.11.1.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-softokn-3.90.0-6.el8_9.x86_64.rpm
nss-softokn-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-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
perf-4.18.0-513.11.1.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-rpm-4.14.3-28.el8_9.x86_64.rpm
python3-urllib3-1.24.2-5.el8_9.2.noarch.rpm
rpm-4.14.3-28.el8_9.x86_64.rpm
rpm-build-libs-4.14.3-28.el8_9.x86_64.rpm
rpm-libs-4.14.3-28.el8_9.x86_64.rpm
rpm-plugin-selinux-4.14.3-28.el8_9.x86_64.rpm
rpm-plugin-systemd-inhibit-4.14.3-28.el8_9.x86_64.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

Security vulnerabilities resolved in SM 10.1 Security Service Pack #22

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
ASM-92801	sudo	RHSA-2024:0811	CVE-2023-28486 CVE-2023-28487 CVE-2023-42465	Moderate
ASM-92798	nss nss-softokn nss-softokn-freebl nss-sysinit nss-util	RHSA-2024:0786	CVE-2023-6135	Moderate
ASM-92796	libmaxminddb	RHSA-2024:0768	CVE-2020-28241	Moderate
ASM-92800	python3-rpm rpm rpm-build-libs rpm-libs rpm-plugin-selinux rpm-plugin-systemd-inhibit	RHSA-2024:0647	CVE-2021-35937 CVE-2021-35938 CVE-2021-35939	Moderate
ASM-92797	Libssh libssh-config	RHSA-2024:0628	CVE-2023-48795	Moderate
ASM-92795	gnutls	RHSA-2024:0627	CVE-2024-0553	Moderate
ASM-92799	openssh openssh-clients openssh-server	RHSA-2024:0606	CVE-2023-48795 CVE-2023-51385	Moderate
ASM-92715	java-1.8.0-openjdk java-1.8.0-openjdk-devel java-1.8.0-openjdk-headless	RHSA-2024:0265	CVE-2024-20918 CVE-2024-20919 CVE-2024-20921 CVE-2024-20926 CVE-2024-20945	Important

			CVE-2024-20952	
ASM-92722	platform-python python3-libs	RHSA-2024:0256	CVE-2023-27043	Moderate
ASM-92725	sqlite sqlite-libs	RHSA-2024:0253	CVE-2023-7104	Moderate
ASM-92714	gnutls	RHSA-2024:0155	CVE-2023-5981	Moderate
ASM-92720	pixman	RHSA-2024:0131	CVE-2022-44638	Moderate
ASM-92717	libxml2	RHSA-2024:0119	CVE-2023-39615	Moderate
ASM-92724	python3-urllib3	RHSA-2024:0116	CVE-2023-43804 CVE-2023-45803	Moderate
ASM-92721	platform-python python3-libs	RHSA-2024:0114	CVE-2022-48560 CVE-2022-48564	Moderate
ASM-92716	kernel kernel-core kernel-modules perf	RHSA-2024:0113	CVE-2023-2162 CVE-2023-4622 CVE-2023-5633 CVE-2023-20569 CVE-2023-42753	Important

ASM-92718	nss nss-softokn nss-softokn-freebl nss-sysinit nss-util	RHSA-2024:0105	CVE-2023-5388	Moderate
ASM-92719	openssl openssl-libs	RHSA-2023:7877	CVE-2023-3446 CVE-2023-3817 CVE-2023-5678	Low

SM 10.1 Security Service Pack #21 includes the following rpm updates:

avahi-libs-0.7-21.el8_9.1.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-modules-4.18.0-513.9.1.el8_9.x86_64.rpm perf-4.18.0-513.9.1.el8_9.x86_64.rpm

Security vulnerabilities resolved in SM 10.1 Security Service Pack #21

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-92643	avahi-libs	RHSA-2023:7836	CVE-2021-3468 CVE-2023-38469 CVE-2023-38470 CVE-2023-38471 CVE-2023-38472 CVE-2023-38473	Moderate	None	None
ASM-92644	Kernel kernel-core kernel-modules perf	RHSA-2023:7549	CVE-2022-45884 CVE-2022-45886 CVE-2022-45919 CVE-2023-1192 CVE-2023-2163 CVE-2023-3812 CVE-2023-5178	Important	None	None

SM 10.1 Security Service Pack #20 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 bind-libs-32:9.11.36-11.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 python2-2.7.18-15.module+el8.9.0+20125+68111a8f.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 c-ares-1.13.0-9.el8_9.1.x86_64.rpm cups-libs-1:2.2.6-54.el8_9.x86_64.rpm fwupd-1.7.8-2.el8.x86_64.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-modules-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 open-vm-tools-12.2.5-3.el8_9.1.x86_64.rpm perf-4.18.0-513.5.1.el8_9.x86_64.rpm perl-HTTP-Tiny-0.074-2.el8.noarch.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-libs-3.6.8-56.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 sysstat-11.7.3-11.el8.x86_64.rpm tpm2-tss-2.3.2-5.el8.x86_64.rpm wireshark-cli-1:2.6.2-17.el8.x86_64.rpm

Security vulnerabilities resolved in SM 10.1 Security Service Pack #20

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-92554	open-vm-tools	RHSA-2023:7265	CVE-2023-34058 CVE-2023-34059	Important	None	None
ASM-92546	c-ares	RHSA-2023:7207	CVE-2020-22217 CVE-2023-31130	Moderate	None	None
ASM-92567	avahi-libs	RHSA-2023:7190	CVE-2023-1981	Moderate	None	None
ASM-92548	fwupd	RHSA-2023:7189	CVE-2022-3287	Moderate	None	None
ASM-92559	procps-ng	RHSA-2023:7187	CVE-2023-4016	Low	None	None
ASM-92544	bind bind-export-libs bind-libs bind-libs-lite bind-license bind-utils python3-bind	RHSA-2023:7177	CVE-2022-3094	Moderate	None	None
ASM-92558	platform-python-pip python3-pip	RHSA-2023:7176	CVE-2007-4559	Moderate	None	None

	python3-pip-wheel					
ASM-92555	perl-HTTP-Tiny	RHSA-2023:7174	CVE-2023-31486	Moderate	None	None
ASM-92565	tpm2-tss	RHSA-2023:7166	CVE-2023-22745	Low	None	None
ASM-92547	cups-libs	RHSA-2023:7165	CVE-2023-32324 CVE-2023-34241	Moderate	None	None
ASM-92557	platform-python python3-libs	RHSA-2023:7151	CVE-2007-4559	Moderate	None	None
ASM-92545	c-ares	RHSA-2023:7116	CVE-2022-4904	Moderate	None	None
ASM-92563	shadow-utils	RHSA-2023:7112	CVE-2023-4641	Low	None	None
ASM-92553	linux-firmware	RHSA-2023:7109	CVE-2023-20569	Moderate	None	None
ASM-92549	kernel kernel-core kernel-modules perf	RHSA-2023:7077	CVE-2021-43975 CVE-2022-3594 CVE-2022-3640 CVE-2022-4744 CVE-2022-28388 CVE-2022-38457 CVE-2022-40133 CVE-2022-40982 CVE-2022-42895 CVE-2022-45869 CVE-2022-45887 CVE-2023-0458 CVE-2023-0590 CVE-2023-0597 CVE-2023-1073 CVE-2023-1074 CVE-2023-1075 CVE-2023-1079 CVE-2023-1118 CVE-2023-1206 CVE-2023-1252 CVE-2023-1382 CVE-2023-1855 CVE-2023-1989 CVE-2023-1998 CVE-2023-2513 CVE-2023-3141 CVE-2023-3161 CVE-2023-3212 CVE-2023-3268	Important	None	None

			CVE-2023-3609 CVE-2023-3611 CVE-2023-3772 CVE-2023-4128 CVE-2023-4132 CVE-2023-4155 CVE-2023-4206 CVE-2023-4207 CVE-2023-4208 CVE-2023-4732 CVE-2023-23455 CVE-2023-26545 CVE-2023-28328 CVE-2023-28772 CVE-2023-30456 CVE-2023-31084 CVE-2023-31436 CVE-2023-33203 CVE-2023-33951 CVE-2023-33952 CVE-2023-35823 CVE-2023-35824 CVE-2023-35825			
ASM-92562	python2 python2-libs python2-pip python2-pip-wheel python2-setuptools python2-setuptools-wheel	RHSA-2023:7042	CVE-2023-32681	Moderate	None	None
ASM-92550	libX11 libX11-common	RHSA-2023:7029	CVE-2023-3138	Moderate	None	None
ASM-92552	libpq	RHSA-2023:7016	CVE-2022-41862	Low	None	None
ASM-92566	wireshark-cli	RHSA-2023:7015	CVE-2023-0666 CVE-2023-2856 CVE-2023-2858 CVE-2023-2952	Moderate	None	None
ASM-92564	sysstat	RHSA-2023:7010	CVE-2023-33204	Moderate	None	None
ASM-92551	libfastjson	RHSA-2023:6976	CVE-2020-12762	Moderate	None	None
ASM-92560	protobuf-c	RHSA-2023:6944	CVE-2022-48468	Moderate	None	None
ASM-92556	platform-python python3-libs	RHSA-2023:5997	CVE-2023-40217	Important	None	None

ASM-92561	python2 python2-libs python2-pip python2-pip-wheel	RHSA-2023:5994	CVE-2023-40217	Important	None	None

SM 10.1 Security Service Pack #19 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-common-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
libnghttp2-1.33.0-5.el8_8.x86_64.rpm
libtiff-4.0.9-29.el8_8.x86_64.rpm
libwebp-1.0.0-8.el8_8.1.x86_64.rpm
open-vm-tools-12.1.5-2.el8_8.3.x86_64.rpm
python3-bind-32:9.11.36-8.el8_8.2.noarch.rpm

Security vulnerabilities resolved in SM 10.1 Security Service Pack #19

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-92409	libnghttp2	RHSA-2023:5837	CVE-2023-44487	Important	None	None
ASM-92408	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	None	None
ASM-92306	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
ASM-92407	glibc glibc glibc-common glibc-langpack-en	RHSA-2023:5455	CVE-2023-4527 CVE-2023-4806 CVE-2023-4813 CVE-2023-4911	Important	None	None

ASM-92339	libtiff	RHSA-2023:5353	CVE-2023-0800 CVE-2023-0801 CVE-2023-0802 CVE-2023-0803 CVE-2023-0804	Moderate	ASA-2023-138	Medium
ASM-92260	open-vm-tools	RHSA-2023:5312	CVE-2023-20900	Important	ASA-2023-122	High
ASM-92332	libwebp	RHSA-2023:5309	CVE-2023-4863	Important	ASA-2023-134	Critical

SM 10.1 Security Service Pack #18 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-modules-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 perf-4.18.0-477.27.1.el8_8.x86_64.rpm

Security vulnerabilities resolved in SM 10.1 Security Service Pack #18

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-92113	dmidecode	RHSA-2023:5252	CVE-2023-30630	Moderate	ASA-2020-095	High
ASM-92171	ncurses ncurses-base ncurses-libs	RHSA-2023:5249	CVE-2023-29491	Moderate	None	None
ASM-92170	linux-firmware	RHSA-2023:5245	CVE-2023-20593	Moderate	None	None

ASM-92115	kernel kernel-core kernel-modules perf	RHSA-2023:5244	CVE-2023-2002 CVE-2023-3090 CVE-2023-3390 CVE-2023-3776 CVE-2023-4004 CVE-2023-20593 CVE-2023-35001 CVE-2023-35788	Important	ASA-2023-119	High
ASM-92095	cups-libs	RHSA-2023:4864	CVE-2023-32360	Important	ASA-2023-116	Medium

SM 10.1 Security Service Pack #17 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-modules-4.18.0-477.21.1.el8_8.x86_64.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-clients-8.0p1-19.el8_8.x86_64.rpm
openssh-server-8.0p1-19.el8_8.x86_64.rpm
perf-4.18.0-477.21.1.el8_8.x86_64.rpm
python3-requests-2.20.0-3.el8_8.noarch.rpm

Security vulnerabilities resolved in SM 10.1 Security Service Pack #17

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-91836	libxml2	RHSA-2023:4529	CVE-2023-28484 CVE-2023-29469	Moderate	ASA-2021-189	Medium

ASM-92076	libcap	RHSA-2023:4524	CVE-2023-2602 CVE-2023-2603	Moderate	ASA-2020-199	Medium
ASM-91828	curl libcurl	RHSA-2023:4523	CVE-2023-27536 CVE-2023-28321	Moderate	ASA-2021-189	Medium
ASM-92075	python3-requests	RHSA-2023:4520	CVE-2023-32681	Moderate	ASA-2020-199	Medium
ASM-91829	kernel kernel-core kernel-modules perf	RHSA-2023:4517	CVE-2022-42896 CVE-2023-1281 CVE-2023-1829 CVE-2023-2124 CVE-2023-2194 CVE-2023-2235	Important	ASA-2021-189	High
ASM-91846	dbus dbus-common dbus-daemon dbus-libs dbus-tools	RHSA-2023:4498	CVE-2023-34969	Moderate	ASA-2021-189	Medium
ASM-91954	openssh openssh-clients openssh-server	RHSA-2023:4419	CVE-2023-38408	Important	ASA-2020-199	Critical

SM 10.1 Security Service Pack #16 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
python3-bind-32:9.11.36-8.el8_8.1.noarch.rpm

Security vulnerabilities resolved in SM 10.1 Security Service Pack #16

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-91648	java-1.8.0-openjdk java-1.8.0-openjdk-devel java-1.8.0-openjdk-headless	RHSA-2023:4176	CVE-2023-22045 CVE-2023-22049	Moderate	None	None
ASM-91640	Bind bind-export-libs bind-libs bind-libs-lite bind-license bind-utils python3-bind	RHSA-2023:4102	CVE-2023-2828	Important	ASA-2023-089	High

SM 10.1 Security Service Pack #15 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
c-ares-1.13.0-6.el8_8.2.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
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-modules-4.18.0-477.15.1.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_8.2.x86_64.rpm
libssh-0.9.6-10.el8_8.x86_64.rpm
systemd-udev-239-74.el8_8.2.x86_64.rpm
unbound-libs-1.16.2-5.el8.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
perf-4.18.0-477.15.1.el8_8.x86_64.rpm
platform-python-3.6.8-51.el8_8.1.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.noarch.rpm
python3-libs-3.6.8-51.el8_8.1.x86_64.rpm
python3-unbound-1.16.2-5.el8.x86_64.rpm
sqlite-3.26.0-18.el8_8.x86_64.rpm
sqlite-libs-3.26.0-18.el8_8.x86_64.rpm
sysstat-11.7.3-9.el8.x86_64.rpm
systemd-239-74.el8_8.2.x86_64.rpm
systemd-libs-239-74.el8_8.2.x86_64.rpm
systemd-pam-239-74.el8_8.2.x86_64.rpm

Security vulnerabilities resolved in SM 10.1 Security Service Pack #15

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-91414	open-vm-tools	RHSA-2023:3949	CVE-2023-20867	Low	ASA-2021-189	Low
ASM-91416	Kernel kernel-core kernel-modules perf	RHSA-2023:3847	CVE-2023-28466	Moderate	ASA-2021-189	High
ASM-91407	sqlite sqlite-libs	RHSA-2023:3840	CVE-2020-24736	Moderate	ASA-2021-189	Medium
ASM-91425	Libssh libssh-config	RHSA-2023:3839	CVE-2023-1667 CVE-2023-2283	Moderate	None	None
ASM-91427	system systemd-libs systemd-pam systemd-udev	RHSA-2023:3837	CVE-2023-26604	Moderate	None	None
ASM-91415	libtiff	RHSA-2023:3827	CVE-2022-48281	Moderate	ASA-2023-070	Medium
ASM-91413	python2 python2-libs python2-pip	RHSA-2023:3780	CVE-2023-24329	Important	ASA-2021-189	High

	python2-pip-wheel					
ASM-91426	platform-python python3-libs	RHSA-2023:3591	CVE-2023-24329	Important	None	None
ASM-91390	c-ares	RHSA-2023:3584	CVE-2023-32067	Important	ASA-2023-056	High
ASM-91384	kernel kernel-core kernel-modules perf	RHSA-2023:3349	CVE-2023-32233	Important	None	None
ASM-91139	curl libcurl	RHSA-2023:3106	CVE-2023-27535	Moderate	ASA-2021-189	Medium
ASM-91145	libarchive	RHSA-2023:3018	CVE-2022-36227	Low	ASA-2021-189	Medium
ASM-91380	bind bind-export-libs bind-libs bind-libs-lite bind-license bind-utils python3-bind	RHSA-2023:3002	CVE-2022-2795	Moderate	None	None
ASM-91382	dhcp-client dhcp-common dhcp-libs	RHSA-2023:3000	CVE-2022-2928 CVE-2022-2929	Moderate	None	None
ASM-91381	libcurl	RHSA-2023:2963	CVE-2022-35252 CVE-2022-43552	Low	ASA-2021-189	Medium
ASM-91383	kernel kernel-core kernel-modules perf	RHSA-2023:2951	CVE-2021-26341 CVE-2021-33655 CVE-2021-33656 CVE-2022-1462 CVE-2022-1679 CVE-2022-1789 CVE-2022-2196 CVE-2022-2663 CVE-2022-3028 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 CVE-2022-4129 CVE-2022-20141 CVE-2022-25265	Important	None	None

			CVE-2022-30594 CVE-2022-39188 CVE-2022-39189 CVE-2022-41218 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			
ASM-91385	kpartx	RHSA-2023:2948	CVE-2022-41973	Moderate	ASA-2021-189	High
ASM-91386	libtiff	RHSA-2023:2883	CVE-2022-3627 CVE-2022-3970	Moderate	None	None
ASM-91387	python2 python2-libs python2-pip python2-pip-wheel	RHSA-2023:2860	CVE-2022-45061	Moderate	None	None
ASM-91133	sysstat	RHSA-2023:2800	CVE-2022-39377	Moderate	ASA-2023-041	High
ASM-91388	python3-unbound unbound-libs	RHSA-2023:2771	CVE-2022-3204	Moderate	ASA-2021-189	High

SM 10.1 Security Service Pack #14 includes the following rpm updates:

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
libwebp-1.0.0-8.el8_7.x86_64.rpm

Security vulnerabilities resolved in SM 10.1 Security Service Pack #14

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-91126	libwebp	RHSA-2023:2076	CVE-2023-1999	Important	None	None

ASM-91090	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

SM 10.1 Security Service Pack #13 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-modules-4.18.0-425.19.2.el8_7.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-util-3.79.0-11.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 perf-4.18.0-425.19.2.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 tzdata-2023c-1.el8.noarch.rpm

Security vulnerabilities resolved in SM 10.1 Security Service Pack #13

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-90850	gnutls	RHSA-2023:1569	CVE-2023-0361	Moderate	ASA-2021-189	High
ASM-90984	kernel kernel-core kernel-modules perf	RHSA-2023:1566	CVE-2022-4269 CVE-2022-4378 CVE-2023-0266 CVE-2023-0386	Important	None	None
ASM-90792	openssl openssl-libs	RHSA-2023:1405	CVE-2022-4304 CVE-2022-4450 CVE-2023-0215 CVE-2023-0286	Important	ASA-2021-189	High
ASM-90724	nss nss-softokn nss-softokn-freebl nss-sysinit nss-util	RHSA-2023:1252	CVE-2023-0767	Important	ASA-2021-189	High
ASM-90808	tzdata	RHBA-2023:1534	NA	Bugfix	NA	NA

SM 10.1 Security Service Pack #12 includes the following rpm updates:

curl-7.61.1-25.el8_7.3.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-modules-4.18.0-425.13.1.el8_7.x86_64.rpm libcurl-7.61.1-25.el8_7.3.x86_64.rpm perf-4.18.0-425.13.1.el8_7.x86_64.rpm platform-python-setuptools-39.2.0-6.el8_7.1.noarch.rpm python3-libs-3.6.8-48.el8_7.1.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 systemd-239-68.el8_7.4.x86_64.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 SM 10.1 Security Service Pack #12

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-90694	curl libcurl	RHSA-2023:1140	CVE-2023-23916	Moderate	None	None
ASM-90580	tar	RHSA-2023:0842	CVE-2022-48303	Moderate	ASA-2021-189	Low
ASM-90695	systemd systemd-libs systemd-pam systemd-udev	RHSA-2023:0837	CVE-2022-4415	Moderate	None	None
ASM-90556	platform-python-setuptools python3-setuptools python3-setuptools-wheel	RHSA-2023:0835	CVE-2022-40897	Moderate	ASA-2021-189	Medium
ASM-90696	platform-python python3-libs	RHSA-2023:0833	CVE-2020-10735 CVE-2021-28861 CVE-2022-45061	Moderate	None	None
ASM-90697	Kernel kernel-core kernel-modules perf	RHSA-2023:0832	CVE-2022-2873 CVE-2022-41222 CVE-2022-43945	Important	None	None

SM 10.1 Security Service Pack #11 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-libs-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 grub2-common-1:2.02-142.el8_7.1.noarch.rpm	kernel-4.18.0-425.10.1.el8_7.x86_64.rpm kernel-core-4.18.0-425.10.1.el8_7.x86_64.rpm kernel-modules-4.18.0-425.10.1.el8_7.x86_64.rpm libXpm-3.5.12-9.el8_7.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

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	libxml2-2.9.7-15.el8_7.1.x86_64.rpm perf-4.18.0-425.10.1.el8_7.x86_64.rpm sqlite-3.26.0-17.el8_7.x86_64.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_7.1.x86_64.rpm systemd-libs-239-68.el8_7.1.x86_64.rpm systemd-pam-239-68.el8_7.1.x86_64.rpm systemd-udev-239-68.el8_7.1.x86_64.rpm

Security vulnerabilities resolved in SM 10.1 Security Service Pack #11

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-90506	libksba	RHSA-2023:0625	CVE-2022-47629	Important	ASA-2021-189	High
ASM-90532	libXpm	RHSA-2023:0379	CVE-2022-4883 CVE-2022-44617 CVE-2022-46285	Important	ASA-2023-020	High
ASM-90408	sudo	RHSA-2023:0284	CVE-2023-22809	Important	ASA-2022-018	High
ASM-90444	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-2021-189	Medium
ASM-90366	libxml2	RHSA-2023:0173	CVE-2022-40303 CVE-2022-40304	Moderate	ASA-2022-018	High
ASM-90533	libtasn1	RHSA-2023:0116	CVE-2021-46848	Moderate	ASA-2023-019	Medium
ASM-90364	sqlite sqlite-libs	RHSA-2023:0110	CVE-2022-35737	Moderate	ASA-2023-009	Medium
ASM-90365	expat	RHSA-2023:0103	CVE-2022-43680	Moderate	ASA-2022-018	Low
ASM-90313	kernel kernel-core kernel-modules perf	RHSA-2023:0101	CVE-2022-2964 CVE-2022-4139	Important	ASA-2023-004	High
ASM-90367	systemd systemd-libs systemd-pam systemd-udev	RHSA-2023:0100	CVE-2022-3821	Moderate	ASA-2023-006	Medium
ASM-90531	dbus dbus-common	RHSA-2023:0096	CVE-2022-42010 CVE-2022-42011	Moderate	None	None

	dbus-daemon dbus-libs dbus-tools		CVE-2022-42012			
ASM-90368	libtiff	RHSA-2023:0095	CVE-2022-2056 CVE-2022-2057 CVE-2022-2058 CVE-2022-2519 CVE-2022-2520 CVE-2022-2521 CVE-2022-2867 CVE-2022-2868 CVE-2022-2869 CVE-2022-2953	Moderate	ASA-2023-005	Medium
ASM-90299	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

- **There was no Session Manager February 2023 Security Service Pack update required.**

SM 10.1 Security Service Pack #10 includes the following rpm updates:

krb5-libs-1.18.2-22.el8_7.x86_64.rpm tzdata-2022g-1.el8	tzdata-java-2022g-1.el8

Security vulnerabilities resolved in SM 10.1 Security Service Pack #10

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-90255	krb5-libs	RHSA-2022:8638	CVE-2022-42898	Important	ASA-2022-175	High
ASM-90222	tzdata tzdata-java	RHBA-2022:8785	N/A	Bugfix	N/A	N/A

SM 10.1 Security Service Pack #9 includes the following rpm updates:

bind-32:9.11.36-5.el8.x86_64.rpm bind-export-libs-32:9.11.36-5.el8.x86_64.rpm	libtiff-4.0.9-23.el8.x86_64.rpm ibxml2-2.9.7-15.el8.x86_64.rpm

bind-libs-32:9.11.36-5.el8.x86_64.rpm bind-libs-lite-32:9.11.36-5.el8.x86_64.rpm bind-license-32:9.11.36-5.el8.noarch.rpm bind-utils-32:9.11.36-5.el8.x86_64.rpm e2fsprogs-1.45.6-5.el8.x86_64.rpm e2fsprogs-libs-1.45.6-5.el8.x86_64.rpm freetype-2.9.1-9.el8.x86_64.rpm fribidi-1.0.4-9.el8.x86_64.rpm gdisk-1.0.3-11.el8.x86_64.rpm glib2-2.56.4-159.el8.x86_64.rpm gnutls-3.6.16-5.el8_6.x86_64.rpm kernel-4.18.0-425.3.1.el8.x86_64.rpm kernel-core-4.18.0-425.3.1.el8.x86_64.rpm kernel-modules-4.18.0-425.3.1.el8.x86_64.rpm kpartx-0.8.4-28.el8_7.1.x86_64.rpm libcom_err-1.45.6-5.el8.x86_64.rpm libss-1.45.6-5.el8.x86_64.rpm	perf-4.18.0-425.3.1.el8.x86_64.rpm python2-2.7.18-11.module+el8.7.0+15681+7a92afba.x86_64.rpm python2-libs-2.7.18-11.module+el8.7.0+15681+7a92afba.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-32:9.11.36-5.el8.noarch.rpm python3-unbound-1.16.2-2.el8.x86_64.rpm qt5-srpm-macros-5.15.3-1.el8.noarch.rpm sqlite-3.26.0-16.el8_6.x86_64.rpm sqlite-libs-3.26.0-16.el8_6.x86_64.rpm tzdata-2022f-1.el8 tzdata-java-2022f-1.el8 unbound-libs-1.16.2-2.el8.x86_64.rpm zlib-1.2.11-19.el8_6.i686.rpm

Security vulnerabilities resolved in SM 10.1 Security Service Pack #9

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-90101	kpartx	RHSA-2022:7928	CVE-2022-3787	Important	ASA-2022-149	High
ASM-90141	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
ASM-90144	freetype	RHSA-2022:7745	CVE-2022-27404 CVE-2022-27405 CVE-2022-27406	Moderate	None	None
ASM-90035	e2fsprogs e2fsprogs-libs libcom_err libss	RHSA-2022:7720	CVE-2022-1304	Moderate	ASA-2022-141	High
ASM-90036	libxml2	RHSA-2022:7715	CVE-2016-3709	Moderate	ASA-2022-138	Medium
ASM-90040	glib2	RHSA-2022:7704	CVE-2022-22624	Moderate	ASA-2022-146	High

			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			
ASM-90038	gdisk	RHSA-2022:7700	CVE-2020-0256 CVE-2021-0308	Moderate	ASA-2022-142	Medium
ASM-90037	kernel kernel-core kernel-modules perf	RHSA-2022:7683	CVE-2020-36516 CVE-2020-36558 CVE-2021-3640 CVE-2021-30002 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-2022-2078 CVE-2022-2586 CVE-2022-2639 CVE-2022-2938 CVE-2022-20368 CVE-2022-21499 CVE-2022-23960 CVE-2022-24448 CVE-2022-26373 CVE-2022-27950 CVE-2022-28390 CVE-2022-28893 CVE-2022-29581 CVE-2022-36946	Moderate	ASA-2022-144	High
ASM-90143	python3-unbound	RHSA-2022:7622	CVE-2022-30698	Moderate	ASA-2022-150	Medium

	unbound-libs		CVE-2022-30699			
ASM-90140	python2 python2-libs python2-pip python2-pip-wheel	RHSA-2022:7593	CVE-2015-20107	Moderate	ASA-2022-156	High
ASM-90142	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
ASM-90145	fribidi	RHSA-2022:7514	CVE-2022-25308 CVE-2022-25309 CVE-2022-25310	Moderate	None	None
ASM-90146	qt5-srpm-macros	RHSA-2022:7482	CVE-2022-25255	Moderate	None	None
ASM-90003	kpartx	RHSA-2022:7192	CVE-2022-41974	Important	ASA-2022-128	High
ASM-90004	kernel kernel-core kernel-modules perf	RHSA-2022:7110	CVE-2022-0494 CVE-2022-1353 CVE-2022-2588 CVE-2022-23816 CVE-2022-23825 CVE-2022-29900 CVE-2022-29901	Important	ASA-2022-132	High
ASM-90001	sqlite sqlite-libs	RHSA-2022:7108	CVE-2020-35525 CVE-2020-35527	Moderate	ASA-2022-130	High
ASM-90002	zlib	RHSA-2022:7106	CVE-2022-37434	Moderate	ASA-2022-129	Critical
ASM-90139	gnutls	RHSA-2022:7105	CVE-2022-2509	Moderate	ASA-2022-158	High
ASM-90041	tzdata tzdata-java	RHBA-2022:7404	N/A	Bug Fix	N/A	N/A

SM 10.1 Security Service Pack #8 includes the following rpm updates:

bind-32:9.11.36-3.el8_6.1.x86_64.rpm	java-1.8.0-openjdk-devel-1:1.8.0.352.b08-2.el8_6.x86_64.rpm
bind-export-libs-32:9.11.36-3.el8_6.1.x86_64.rpm	java-1.8.0-openjdk-headless-1:1.8.0.352.b08-2.el8_6.x86_64.rpm
bind-libs-32:9.11.36-3.el8_6.1.x86_64.rpm	libksba-1.3.5-8.el8_6.x86_64.rpm

bind-libs-lite-32:9.11.36-3.el8_6.1.x86_64.rpm bind-license-32:9.11.36-3.el8_6.1.noarch.rpm bind-utils-32:9.11.36-3.el8_6.1.x86_64.rpm expat-2.2.5-8.el8_6.3.x86_64.rpm java-1.8.0-openjdk-1:1.8.0.352.b08-2.el8_6.x86_64.rpm	python3-bind-32:9.11.36-3.el8_6.1.noarch.rpm tzdata-2022e-1.el8 tzdata-java-2022e-1.el8

Security vulnerabilities resolved in SM 10.1 Security Service Pack #8

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-89982	libksba	RHSA-2022:7089	CVE-2022-3515	Important	None	None
ASM-89981	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	Important	None	None
ASM-89980	expat	RHSA-2022:6878	CVE-2022-40674	Important	None	None
ASM-89979	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	ASA-2022-134	Low
ASM-89964	tzdata tzdata-java	RHBA-2022:7067	N/A	Bug Fix	N/A	N/A

SM 10.1 Security Service Pack #7 includes the following rpm updates:

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

Security vulnerabilities resolved in SM 10.1 Security Service Pack #7

Fix id	Updated Package	RHSA Number	Common	RHSA	ASA Number	ASA

			Vulnerability and Exposure (CVE) ID	Severity		Overall Severity
ASM-89839	gnupg2 gnupg2-smime	RHSA-2022:6463	CVE-2022-34903	Moderate	ASA-2022-121	Medium
ASM-89840	kernel kernel-core kernel-modules perf	RHSA-2022:6460	CVE-2022-21123 CVE-2022-21125 CVE-2022-21166	Moderate	None	None
ASM-89838	platform-python python3-libs	RHSA-2022:6457	CVE-2015-20107 CVE-2022-0391	Moderate	None	None
ASM-89841	open-vm-tools	RHSA-2022:6357	CVE-2022-31676	Important	None	None
ASM-89837	curl libcurl	RHSA-2022:6159	CVE-2022-32206 CVE-2022-32208	Moderate	None	None
ASM-89934	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

SM 10.1 Security Service Pack #6 includes the following rpm updates:

kernel-4.18.0-372.19.1.el8_6.x86_64.rpm	pcre2-10.32-3.el8_6.x86_64.rpm
kernel-core-4.18.0-372.19.1.el8_6.x86_64.rpm	perf-4.18.0-372.19.1.el8_6.x86_64.rpm
kernel-modules-4.18.0-372.19.1.el8_6.x86_64.rpm	vim-common-2:8.0.1763-19.el8_6.4.x86_64.rpm
openssl-1:1.1.1k-7.el8_6.x86_64.rpm	vim-filesystem-2:8.0.1763-19.el8_6.4.noarch.rpm
openssl-libs-1:1.1.1k-7.el8_6.x86_64.rpm	vim-minimal-2:8.0.1763-19.el8_6.4.x86_64.rpm

Security vulnerabilities resolved in SM 10.1 Security Service Pack #6

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-89715	kernel kernel-core kernel-modules perf	RHSA-2022:5819	CVE-2022-1012 CVE-2022-32250	Important	ASA-2022-120	High
ASM-89635	openssl openssl-libs	RHSA-2022:5818	CVE-2022-1292 CVE-2022-2068 CVE-2022-2097	Moderate	ASA-2022-111	Medium
ASM-89636	vim-common vim-filesystem	RHSA-2022:5813	CVE-2022-1785 CVE-2022-1897	Moderate	ASA-2022-110	Critical

	vim-minimal		CVE-2022-1927			
ASM-89634	pcre2	RHSA-2022:5809	CVE-2022-1586	Moderate	ASA-2022-112	High

Note: Supplement 4 of PCN2135S covers postgres security update. (CVE-2021-23214 and CVE-2021-23222)

SM 10.1 Security Service Pack #5 includes the following rpm updates:

java-1.8.0-openjdk-1:1.8.0.342.b07-2.el8_6.x86_64.rpm
java-1.8.0-openjdk-devel-1:1.8.0.342.b07-2.el8_6.x86_64.rpm
java-1.8.0-openjdk-headless-1:1.8.0.342.b07-2.el8_6.x86_64.rpm
kernel-4.18.0-372.16.1.el8_6.x86_64.rpm
kernel-core-4.18.0-372.16.1.el8_6.x86_64.rpm
kernel-modules-4.18.0-372.16.1.el8_6.x86_64.rpm
perf-4.18.0-372.16.1.el8_6.x86_64.rpm

Security vulnerabilities resolved in SM 10.1 Security Service Pack #5

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-89566	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
ASM-89567	kernel kernel-core kernel-modules perf	RHSA-2022:5564	CVE-2022-1729	Important	ASA-2022-109	Medium

SM 10.1 Security Service Pack #4 includes the following rpm updates:

cups-libs-1:2.2.6-45.el8_6.2.x86_64.rpm
curl-7.61.1-22.el8_6.3.x86_64.rpm
expat-2.2.5-8.el8_6.2.x86_64.rpm
grub2-common-1:2.02-123.el8_6.8.noarch.rpm
grub2-efi-x64-1:2.02-123.el8_6.8.x86_64.rpm
grub2-tools-1:2.02-123.el8_6.8.x86_64.rpm
grub2-tools-extra-1:2.02-123.el8_6.8.x86_64.rpm
grub2-tools-minimal-1:2.02-123.el8_6.8.x86_64.rpm
kernel-4.18.0-372.13.1.el8_6.x86_64.rpm
kernel-core-4.18.0-372.13.1.el8_6.x86_64.rpm
kernel-modules-4.18.0-372.13.1.el8_6.x86_64.rpm
libcurl-7.61.1-22.el8_6.3.x86_64.rpm
libgcrypt-1.8.5-7.el8_6.x86_64.rpm
libxml2-2.9.7-13.el8_6.1.x86_64.rpm
mokutil-1:0.3.0-11.el8_6.1.x86_64.rpm
perf-4.18.0-372.13.1.el8_6.x86_64.rpm
rsyslog-8.2102.0-7.el8_6.1.x86_64.rpm
rsyslog-gnutls-8.2102.0-7.el8_6.1.x86_64.rpm
shim-x64-15.6-1.el8.x86_64.rpm
vim-common-2:8.0.1763-19.el8_6.2.x86_64.rpm
vim-filesystem-2:8.0.1763-19.el8_6.2.noarch.rpm
vim-minimal-2:8.0.1763-19.el8_6.2.x86_64.rpm
xz-5.2.4-4.el8_6.x86_64.rpm
xz-libs-5.2.4-4.el8_6.x86_64.rpm

Security vulnerabilities resolved in SM 10.1 Security Service Pack #4

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-89392	vim-common vim-filesystem vim-minimal	RHSA-2022:5319	CVE-2022-1621 CVE-2022-1629	Moderate	ASA-2022-104	High
ASM-89389	libxml2	RHSA-2022:5317	CVE-2022-29824	Moderate	ASA-2022-100	High
ASM-89388	kernel kernel-core kernel-modules perf	RHSA-2022:5316	CVE-2020-28915 CVE-2022-27666	Important	ASA-2022-101	High
ASM-89391	curl libcurl	RHSA-2022:5313	CVE-2022-22576 CVE-2022-27774 CVE-2022-27776 CVE-2022-27782	Moderate	None	NA
ASM-89390	libgcrypt	RHSA-2022:5311	CVE-2021-40528	Moderate	ASA-2022-103	Medium
ASM-89358	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
ASM-89357	cups-libs	RHSA-2022:5056	CVE-2022-26691	Important	ASA-2022-091	High
ASM-89257	xz xz-libs	RHSA-2022:4991	CVE-2022-1271	Important	ASA-2022-080	High
ASM-89233	rsyslog rsyslog-gnutls	RHSA-2022:4799	CVE-2022-24903	Important	ASA-2022-078	High

SM 10.1 Security Service Pack #3 includes the following rpm updates:

bind-32:9.11.36-3.el8.x86_64.rpm bind-export-libs-32:9.11.36-3.el8.x86_64.rpm bind-libs-32:9.11.36-3.el8.x86_64.rpm bind-libs-lite-32:9.11.36-3.el8.x86_64.rpm	libssh-config-0.9.6-3.el8.noarch.rpm libtiff-4.0.9-21.el8.x86_64.rpm libudisks2-2.9.0-9.el8.x86_64.rpm openssh-8.0p1-13.el8.x86_64.rpm

bind-license-32:9.11.36-3.el8.noarch.rpm
bind-utils-32:9.11.36-3.el8.x86_64.rpm
c-ares-1.13.0-6.el8.x86_64.rpm
cairo-1.15.12-6.el8.x86_64.rpm
cpio-2.12-11.el8.x86_64.rpm
grub2-common-1:2.02-123.el8.noarch.rpm
grub2-efi-x64-1:2.02-123.el8.x86_64.rpm
grub2-tools-1:2.02-123.el8.x86_64.rpm
grub2-tools-extra-1:2.02-123.el8.x86_64.rpm
grub2-tools-minimal-1:2.02-123.el8.x86_64.rpm
gzip-1.9-13.el8_5.x86_64.rpm
java-1.8.0-openjdk-1:1.8.0.332.b09-1.el8_5.x86_64.rpm
java-1.8.0-openjdk-devel-1:1.8.0.332.b09-1.el8_5.x86_64.rpm
java-1.8.0-openjdk-headless-1:1.8.0.332.b09-1.el8_5.x86_64.rpm
kernel-4.18.0-372.9.1.el8.x86_64.rpm
kernel-core-4.18.0-372.9.1.el8.x86_64.rpm
kernel-modules-4.18.0-372.9.1.el8.x86_64.rpm
libpq-13.5-1.el8.x86_64.rpm
libssh-0.9.6-3.el8.x86_64.rpm

openssh-clients-8.0p1-13.el8.x86_64.rpm
openssh-server-8.0p1-13.el8.x86_64.rpm
perf-4.18.0-372.9.1.el8.x86_64.rpm
pixman-0.38.4-2.el8.x86_64.rpm
platform-python-3.6.8-45.el8.x86_64.rpm
polkit-0.115-13.el8_5.2.x86_64.rpm
polkit-libs-0.115-13.el8_5.2.x86_64.rpm
python2-2.7.18-10.module+el8.6.0+14191+7fdd52cd.x86_64.rpm
python2-libs-2.7.18-10.module+el8.6.0+14191+7fdd52cd.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-32:9.11.36-3.el8.noarch.rpm
python3-libs-3.6.8-45.el8.x86_64.rpm
python3-lxml-4.2.3-4.el8.x86_64.rpm
udisks2-2.9.0-9.el8.x86_64.rpm
vim-common-2:8.0.1763-16.el8_5.13.x86_64.rpm
vim-filesystem-2:8.0.1763-16.el8_5.13.noarch.rpm
vim-minimal-2:8.0.1763-16.el8_5.13.x86_64.rpm
zlib-1.2.11-18.el8_5.i686.rpm

Security vulnerabilities resolved in SM 10.1 Security Service Pack #3

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-89035	grub2-common grub2-efi-x64 grub2-tools grub2-tools-extra grub2-tools-minimal	RHSA-2022:2110	CVE-2021-3981	Low	ASA-2022-051	Low
ASM-89059	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
ASM-89131	c-ares	RHSA-2022:2043	CVE-2021-3672	Moderate	None	NA
ASM-89040	libssh libssh-config	RHSA-2022:2031	CVE-2021-3634	Low	ASA-2022-057	Medium
ASM-89039	openssh openssh-clients openssh-server	RHSA-2022:2013	CVE-2021-41617	Moderate	ASA-2022-056	High
ASM-89037	cpio	RHSA-2022:1991	CVE-2021-38185	Moderate	ASA-2022-054	High

ASM-89038	kernel kernel-core kernel-modules perf	RHSA-2022:1988	CVE-2020-0404 CVE-2020-4788 CVE-2020-13974 CVE-2020-27820 CVE-2021-0941 CVE-2021-3612 CVE-2021-3669 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-2021-4197 CVE-2021-4203 CVE-2021-20322 CVE-2021-21781 CVE-2021-26401 CVE-2021-29154 CVE-2021-37159 CVE-2021-41864 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
ASM-89033	platform-python python3-libs	RHSA-2022:1986	CVE-2021-3737 CVE-2021-4189	Moderate	ASA-2022-049	Medium
ASM-89036	cairo pixman	RHSA-2022:1961	CVE-2020-35492	Moderate	ASA-2022-052	High
ASM-89058	python3-lxml	RHSA-2022:1932	CVE-2021-43818	Moderate	ASA-2022-071	High
ASM-89042	libpq	RHSA-2022:1891	CVE-2021-23222	Low	ASA-2022-060	Low
ASM-89041	python2 python2-libs python2-pip python2-pip-wheel	RHSA-2022:1821	CVE-2021-3733 CVE-2021-3737 CVE-2021-4189 CVE-2021-43818 CVE-2022-0391	Moderate: python27	ASA-2022-059	High
ASM-89032	libudisks2 udisks2	RHSA-2022:1820	CVE-2021-3802	Low	ASA-2022-048	Low
ASM-89034	libtiff	RHSA-2022:1810	CVE-2020-19131	Moderate	ASA-2022-050	High
ASM-88850	zlib	RHSA-2022:1642	CVE-2018-25032	Important	ASA-2022-044	High
ASM-88837	vim-common	RHSA-2022:1552	CVE-2022-1154	Moderate	ASA-2022-042	Critical

	vim-filesystem vim-minimal					
ASM-89129	kernel kernel-core kernel-modules perf	RHSA-2022:1550	CVE-2021-4028 CVE-2022-25636	Important	None	NA
ASM-88836	polkit polkit-libs	RHSA-2022:1546	CVE-2021-4115	Moderate	ASA-2022-040	Medium
ASM-88838	gzip	RHSA-2022:1537	CVE-2022-1271	Important	ASA-2022-041	High
ASM-89130	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	None	NA

SM 10.1 Security Service Pack #2 includes the following rpm updates:

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

Security vulnerabilities resolved in SM 10.1 Security Service Pack #2

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-88548	openssl openssl-libs	RHSA-2022:1065	CVE-2022-0778	Important	ASA-2022-036	High
ASM-88478	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 CVE-2022-22827 CVE-2022-23852 CVE-2022-25235 CVE-2022-25236 CVE-2022-25315	Important	ASA-2022-031	Critical
ASM-88484	libxml2	RHSA-2022:0899	CVE-2022-23308	Moderate	ASA-2022-033	High
ASM-88809	glibc glibc-common glibc-langpack-en	RHSA-2022:0896	CVE-2021-3999 CVE-2022-23218 CVE-2022-23219	Moderate	ASA-2022-074	High
ASM-88470	vim-common vim-filesystem vim-minimal	RHSA-2022:0894	CVE-2022-0261 CVE-2022-0318 CVE-2022-0359 CVE-2022-0361	Moderate	ASA-2022-030	Low

			CVE-2022-0392 CVE-2022-0413			
ASM-88808	libarchive	RHSA-2022:0892	CVE-2021-23177 CVE-2021-31566	Moderate	None	NA
ASM-88466	kernel kernel-core kernel-modules 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

SM 10.1 Security Service Pack #1 includes the following rpm updates:

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

Security vulnerabilities resolved in SM 10.1 Security Service Pack #1

Fix id	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
ASM-88437	cyrus-sasl-lib	RHSA-2022:0658	CVE-2022-24407	Important	ASA-2022-027	Critical
ASM-88104	aide	RHSA-2022:0441	CVE-2021-45417	Important	ASA-2022-021	High
ASM-88073	cryptsetup cryptsetup-libs	RHSA-2022:0370	CVE-2021-4122	Moderate	ASA-2022-019	Low
ASM-88065	python3-rpm rpm rpm-build-libs rpm-libs rpm-plugin-selinux rpm-plugin-systemd-inhibit	RHSA-2022:0368	CVE-2021-3521	Moderate	ASA-2022-016	Medium
ASM-88066	vim-common vim-filesystem	RHSA-2022:0366	CVE-2021-3872 CVE-2021-3984	Moderate	ASA-2022-015	High

	vim-minimal		CVE-2021-4019 CVE-2021-4192 CVE-2021-4193			
ASM-88059	java-1.8.0-openjdk java-1.8.0-openjdk-devel 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
ASM-88028	polkit polkit-libs	RHSA-2022:0267	CVE-2021-4034	Important	ASA-2022-007	High
ASM-88029	kernel kernel-core kernel-modules perf	RHSA-2022:0188	CVE-2021-4155 CVE-2022-0185	Important	ASA-2022-006	High
ASM-87829	kernel kernel-core kernel-modules perf	RHSA-2021:5227	CVE-2021-20321	Moderate	ASA-2021-187	Medium
ASM-87856	openssl openssl-libs	RHSA-2021:5226	CVE-2021-3712	Moderate	ASA-2022-002	High
ASM-87855	nss nss-softokn nss-softokn-freebl nss-sysinit nss-util	RHSA-2021:4903	CVE-2021-43527	Critical	ASA-2021-190	Critical
ASM-87854	kernel kernel-core kernel-modules perf	RHSA-2021:4647	CVE-2021-20317 CVE-2021-43267	Important	ASA-2021-178	High

Mitigation: Not Applicable

SECTION 1C – ENTITLEMENTS AND CONTACTS

Material Coverage Entitlements: There is no incremental charge for the material in this PCN. The software updates are available on support.avaya.com and from plds.avaya.com.

Avaya Customer Service Coverage Entitlements: Avaya is issuing this PCN as installable by the customer. If the customer requests Avaya to install this PCN, it is considered a billable event as outlined in Section 4 (*Software Updates and Product Correction Notices*) of the Avaya Service Agreement Supplement (Full Maintenance Coverage) unless the customer has purchased an Avaya Services enhanced offer such as the Avaya Services Product Correction Support offer.

Additionally, Avaya on-site support is not included. If on-site support is requested, Avaya will bill the customer current Per Incident charges unless the customer has purchased an Avaya Services enhanced offer such as the Avaya Services Product Correction Support offer.

Customers under the following Avaya coverage: -Full Coverage Service Contract* -On-site Hardware Maintenance Contract*	
Remote Installation	Current Per Incident Rates Apply
Remote or On-site Services Labor	Current Per Incident Rates Apply

- Service contracts that include both labor and parts support – 24x7, 8x5.

Customers under the following Avaya coverage: -Warranty -Software Support -Software Support Plus Upgrades -Remote Only -Parts Plus Remote -Remote Hardware Support -Remote Hardware Support w/ Advance Parts Replacement	
Help-Line Assistance	Per Terms of Services Contract or coverage
Remote or On-site Services Labor	Per Terms of Services Contract or coverage

Avaya Product Correction Notice Support Offer
The Avaya Product Correction Support Offer provides out-of-hours support for remote and on-site technician installable PCNs, and Avaya installation for all Avaya issued PCNs that are classified as “Customer-Installable”. Refer to the PCN Offer or contact your Avaya Account Representative for complete details.

Avaya Authorized Partner Service Coverage Entitlements:

Avaya Authorized Partner
Avaya Authorized Partners are responsible for the implementation of this PCN on behalf of their customers.

Who to contact for more information:

If you require further information or assistance please contact your Authorized Service Provider, or visit support.avaya.com. There you can access more product information, chat with an Agent, or open an online Service Request. Support is provided per your warranty or service contract terms unless otherwise specified in the Avaya support Terms of Use.