

Product Correction Notice (PCN)

Issue Date: 15-July-2019
 Supplement Date: 8-May-2023
 Expiration Date: NA
 PCN Number: 2107S

SECTION 1 - CUSTOMER NOTICE

Products affected by this PCN: Avaya Aura® Communication Manager 8.1 Simplex vAppliance and Duplex vAppliance running on Avaya Aura® Appliance Virtualization Platform (AVP) on Avaya provided servers, VMware® vSphere® ESXi infrastructures on VMware® certified hardware, Simplex and Duplex vAppliance running on Amazon Web Services (AWS) and Simplex and Duplex vAppliance running on Kernel-based Virtual Machine (KVM).

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

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

8 May 2023 – Supplement 29 of this PCN introduces **Security Service Pack #30** (PLAT-rhel7.6-0300.tar; **PLDS ID** CM000001600) and **Kernel Service Pack #30** (KERNEL-3.10.0-1160.88.1.el7.tar; **PLDS ID** CM000001601). Since there was no KSP in the previous supplements, to align SSP and KSP numbering, the KSP jumps from KSP#27 to KSP#30. KSP#28 and KSP#29 were never built.

- A pre-activation patch is required if CM was upgraded in a specific scenario utilizing Avaya Aura® System Manager Solution Deployment Manager (SDM). Please see **PSN020355u** for details.
- Security and Kernel Service Packs should NOT be applied on the Software Only offer.

21 February 2023 – Supplement 28 of this PCN introduces **Security Service Pack #29** (PLAT-rhel7.6-0290.tar; **PLDS ID** CM000001598) This release of Security Updates did not require a new Kernel Service Pack. **Kernel Service Pack #27** should continue to be used.

- A pre-activation patch is required if CM was upgraded in a specific scenario utilizing Avaya Aura® System Manager Solution Deployment Manager (SDM). Please see **PSN020355u** for details.
- Security and Kernel Service Packs should NOT be applied on the Software Only offer.

9 January 2023 – Supplement 27 of this PCN introduces **Security Service Pack #28** (PLAT-rhel7.6-0280.tar; **PLDS ID** CM000001596) This release of Security Updates did not require a new Kernel Service Pack. **Kernel Service Pack #27** should continue to be used.

- A pre-activation patch is required if CM was upgraded in a specific scenario utilizing Avaya Aura® System Manager Solution Deployment Manager (SDM). Please see **PSN020355u** for details.

- Security and Kernel Service Packs should NOT be applied on the Software Only offer.

13 December 2022 – Supplement 26 of this PCN introduces **Security Service Pack #27** (PLAT-rhel7.6-0270.tar; **PLDS ID** CM000001594) and **Kernel Service Pack #27** (KERNEL-3.10.0-1160.80.1.el7.tar; **PLDS ID** CM000001595). Since there was no KSP in the previous supplements, to align SSP and KSP numbering, the KSP jumps from KSP#24 to KSP#27. KSP#25 and KSP#26 were never built.

- A pre-activation patch is required if CM was upgraded in a specific scenario utilizing Avaya Aura® System Manager Solution Deployment Manager (SDM). Please see **PSN020355u** for details.
- Security and Kernel Service Packs should NOT be applied on the Software Only offer.

14 November 2022 – Supplement 25 of this PCN introduces **Security Service Pack #26** (PLAT-rhel7.6-0260.tar; **PLDS ID** CM000001593). This release of Security Updates did not require a new Kernel Service Pack. **Kernel Service Pack #24** should continue to be used.

- A pre-activation patch is required if CM was upgraded in a specific scenario utilizing Avaya Aura® System Manager Solution Deployment Manager (SDM). Please see **PSN020355u** for details.
- Security and Kernel Service Packs should NOT be applied on the Software Only offer.

24 October 2022 – Supplement 24 of this PCN introduces **Security Service Pack #25** (PLAT-rhel7.6-0250.tar; **PLDS ID** CM000001592). This release of Security Updates did not require a new Kernel Service Pack. **Kernel Service Pack #24** should continue to be used.

- A pre-activation patch is required if CM was upgraded in a specific scenario utilizing Avaya Aura® System Manager Solution Deployment Manager (SDM). Please see **PSN020355u** for details.
- Security and Kernel Service Packs should NOT be applied on the Software Only offer.

12 September 2022 – Supplement 23 of this PCN introduces **Security Service Pack #24** (PLAT-rhel7.6-0240.tar; **PLDS ID** CM000001589) and **Kernel Service Pack #24** (KERNEL-3.10.0-1160.76.1.el7.tar; **PLDS ID** CM000001590) for Avaya Aura® Communication Manager 8.1.x (R018x.00.0.890.0).

- A pre-activation patch is required if CM was upgraded in a specific scenario utilizing Avaya Aura® System Manager Solution Deployment Manager (SDM). Please see **PSN020355u** for details.
- Security and Kernel Service Packs should NOT be applied on the Software Only offer.

8 August 2022 – Supplement 22 of this PCN introduces **Security Service Pack #23** (PLAT-rhel7.6-0230.tar; **PLDS ID** CM000001586) and **Kernel Service Pack #23** (KERNEL-3.10.0-1160.71.1.el7.tar; **PLDS ID** CM000001587) for Avaya Aura® Communication Manager 8.1.x (R018x.00.0.890.0). Since there was no KSP in the previous two supplements, to align SSP and KSP numbering, the KSP jumps from KSP#20 to KSP#23. KSP#21 and KSP#22 were never built.

- A pre-activation patch is required if CM was upgraded in a specific scenario utilizing Avaya Aura® System Manager Solution Deployment Manager (SDM). Please see **PSN020355u** for details.
- Security and Kernel Service Packs should NOT be applied on the Software Only offer.

18 July 2022 – Supplement 21 of this PCN introduces **Security Service Pack #22** (PLAT-rhel7.6-0220.tar; **PLDS ID** CM000001585) for Avaya Aura® Communication Manager 8.1.x (R018x.00.0.890.0). This release of Security Updates did not require a new Kernel Service Pack. **Kernel Service Pack #20** should continue to be used.

- A pre-activation patch is required if CM was upgraded in a specific scenario utilizing Avaya Aura® System Manager Solution Deployment Manager (SDM). Please see **PSN020355u** for details.
- Security and Kernel Service Packs should NOT be applied on the Software Only offer.

13 June 2022 – Supplement 20 of this PCN introduces **Security Service Pack #21** (PLAT-rhel7.6-0210.tar; **PLDS ID** CM000001583) for Avaya Aura® Communication Manager 8.1.x (R018x.00.0.890.0). This release of Security Updates did not require a new Kernel Service Pack. **Kernel Service Pack #20** should continue to be used.

- A pre-activation patch is required if CM was upgraded in a specific scenario utilizing Avaya Aura® System Manager Solution Deployment Manager (SDM). Please see **PSN020355u** for details.
- Security and Kernel Service Packs should NOT be applied on the Software Only offer.

09 May 2022 – Supplement 19 of this PCN introduces **Security Service Pack #20** (PLAT-rhel7.6-0200.tar; **PLDS ID** CM000001581) and **Kernel Service Pack #20** (KERNEL-3.10.0-1160.62.1.el7.tar; **PLDS ID** CM000001582) for Avaya Aura® Communication Manager 8.1.x (R018x.00.0.890.0).

- A pre-activation patch is required if CM was upgraded in a specific scenario utilizing Avaya Aura® System Manager Solution Deployment Manager (SDM). Please see **PSN020355u** for details.
- Security and Kernel Service Packs should NOT be applied on the Software Only offer.

11 Apr 2022 – Supplement 18 of this PCN introduces **Security Service Pack #19** (PLAT-rhel7.6-0190.tar; **PLDS ID** CM000001579) and **Kernel Service Pack #19** (KERNEL-3.10.0-1160.59.1.el7.tar; **PLDS ID** CM000001580) for Avaya Aura® Communication Manager 8.1.x (R018x.00.0.890.0).

- A pre-activation patch is required if CM was upgraded in a specific scenario utilizing Avaya Aura® System Manager Solution Deployment Manager (SDM). Please see **PSN020355u** for details.
- Security and Kernel Service Packs should NOT be applied on the Software Only offer.

14 Mar 2022 – Supplement 17 of this PCN introduces **Security Service Pack #18** (PLAT-rhel7.6-0180.tar; **PLDS ID** CM000001577) and **Kernel Service Pack #18** (KERNEL-3.10.0-1160.53.1.el7.tar; **PLDS ID** CM000001578) for Avaya Aura® Communication Manager 8.1.x (R018x.00.0.890.0). Since there was no KSP in the previous supplement, to align SSP and KSP numbering, the KSP jumps from KSP#16 to KSP#18. KSP#17 was never built.

- A pre-activation patch is required if CM was upgraded in a specific scenario utilizing Avaya Aura® System Manager Solution Deployment Manager (SDM). Please see **PSN020355u** for details.
- Security and Kernel Service Packs should NOT be applied on the Software Only offer.

22 Feb 2022 – Supplement 16 of this PCN introduces **Security Service Pack #17** (PLAT-rhel7.6-0170.tar; **PLDS ID** CM000001576). This release of Security Updates did not require a new Kernel Service Pack. **Kernel Service Pack #16** should continue to be used.

- A pre-activation patch is required if CM was upgraded in a specific scenario utilizing Avaya Aura® System Manager Solution Deployment Manager (SDM). Please see **PSN020355u** for details.
- Security and Kernel Service Packs should NOT be applied on the Software Only offer.

10 Jan 2022 – Supplement 15 of this PCN introduces **Security Service Pack #16** (PLAT-rhel7.6-

0160.tar; **PLDS ID** CM000001573) and **Kernel Service Pack #16** (KERNEL-3.10.0-1160.49.1.el7.tar; **PLDS ID** CM000001574) for Avaya Aura® Communication Manager 8.1.x (R018x.00.0.890.0).

- A pre-activation patch is required if CM was upgraded in a specific scenario utilizing Avaya Aura® System Manager Solution Deployment Manager (SDM). Please see **PSN020355u** for details.
- Security and Kernel Service Packs should NOT be applied on the Software Only offer.

20 Dec 2021 – Supplement 14 of this PCN introduces **Security Service Pack #15** (PLAT-rhel7.6-0150.tar; **PLDS ID** CM000001571) and **Kernel Service Pack #15** (KERNEL-3.10.0-1160.45.1.el7.tar; **PLDS ID** CM000001572) for Avaya Aura® Communication Manager 8.1.x (R018x.00.0.890.0).

- A pre-activation patch is required if CM was upgraded in a specific scenario utilizing Avaya Aura® System Manager Solution Deployment Manager (SDM). Please see **PSN020355u** for details.
- Security and Kernel Service Packs should NOT be applied on the Software Only offer.

11 Oct 2021 – Supplement 13 of this PCN introduces **Security Service Pack #14** (PLAT-rhel7.6-0140.tar; **PLDS ID** CM000001569) and **Kernel Service Pack #14** (KERNEL-3.10.0-1160.42.2.el7.tar; **PLDS ID** CM000001570) for Avaya Aura® Communication Manager 8.1.x (R018x.00.0.890.0). Since there was no SSP in the previous supplement, to align SSP and KSP numbering, the SSP jumps from SSP#12 to SSP#14. SSP#13 was never built.

- A pre-activation patch is required if CM was upgraded in a specific scenario utilizing Avaya Aura® System Manager Solution Deployment Manager (SDM). Please see **PSN020355u** for details.
- Security and Kernel Service Packs should NOT be applied on the Software Only offer.

13 Sep 2021 – Supplement 12 of this PCN **Kernel Service Pack #13** (KERNEL-3.10.0-1160.36.2.el7.tar; **PLDS ID** CM000001567) for Avaya Aura® Communication Manager 8.1.x (R018x.00.0.890.0). This release of Security Updates did not require a new Security Service Pack. **Security Service Pack #12** should continue to be used.

- A pre-activation patch is required if CM was upgraded in a specific scenario utilizing Avaya Aura® System Manager Solution Deployment Manager (SDM). Please see **PSN020355u** for details.
- Security and Kernel Service Packs should NOT be applied on the Software Only offer.

9 Aug 2021 – Supplement 11 of this PCN introduces **Security Service Pack #12** (PLAT-rhel7.6-0120.tar; **PLDS ID** CM000001565) and **Kernel Service Pack #12** (KERNEL-3.10.0-1160.31.1.el7.tar; **PLDS ID** CM000001566) for Avaya Aura® Communication Manager 8.1.x (R018x.00.0.890.0). Since there were no KSPs in the previous two supplements, to align SSP and KSP numbering, the KSP jumps from KSP#9 to KSP#12. KSP#10 and KSP#11 were never built.

- A pre-activation patch is required if CM was upgraded in a specific scenario utilizing Avaya Aura® System Manager Solution Deployment Manager (SDM). Please see **PSN020355u** for details.
- Security and Kernel Service Packs should NOT be applied on the Software Only offer.

12 July 2021 – Supplement 10 of this PCN introduces **Security Service Pack #11** (PLAT-rhel7.6-0110.tar; **PLDS ID** CM000001564) for Avaya Aura® Communication Manager 8.1.x (R018x.00.0.890.0). This release of Security Updates did not require a new Kernel Service Pack. **Kernel Service Pack #9** should continue to be used.

- A pre-activation patch is required if CM was upgraded in a specific scenario utilizing Avaya

Aura® System Manager Solution Deployment Manager (SDM).

Please see **PSN020355u** for details.

- Security and Kernel Service Packs should NOT be applied on the Software Only offer.

14 June 2021 – Supplement 9 of this PCN introduces **Security Service Pack #10** (PLAT-rhel7.6-0100.tar; **PLDS ID** CM000001562) for Avaya Aura® Communication Manager 8.1.x (R018x.00.0.890.0). This release of Security Updates did not require a new Kernel Service Pack. **Kernel Service Pack #9** should continue to be used.

- A pre-activation patch is required if CM was upgraded in a specific scenario utilizing Avaya Aura® System Manager Solution Deployment Manager (SDM). Please see **PSN020355u** for details.
- Security and Kernel Service Packs should NOT be applied on the Software Only offer.

10 May 2021 – Supplement 8 of this PCN introduces **Security Service Pack #9** (PLAT-rhel7.6-0090.tar; **PLDS ID** CM000001560) and **Kernel Service Pack #9** (KERNEL-3.10.0-1160.24.1.el7.tar; **PLDS ID** CM000001561) for Avaya Aura® Communication Manager 8.1.x (R018x.00.0.890.0).

- A pre-activation patch is required if CM was upgraded in a specific scenario utilizing Avaya Aura® System Manager Solution Deployment Manager (SDM). Please see **PSN020355u** for details.
- Security and Kernel Service Packs should NOT be applied on the Software Only offer.

05 Apr 2021 – Supplement 7 of this PCN introduces **Security Service Pack #8** (PLAT-rhel7.6-0080.tar; **PLDS ID** CM000001558) and **Kernel Service Pack #8** (KERNEL-3.10.0-1160.15.2.el7.tar; **PLDS ID** CM000001559) for Avaya Aura® Communication Manager 8.1.x (R018x.00.0.890.0).

- A pre-activation patch is required if CM was upgraded in a specific scenario utilizing Avaya Aura® System Manager Solution Deployment Manager (SDM). Please see **PSN020355u** for details.
- Security and Kernel Service Packs should NOT be applied on the Software Only offer.

08 Feb 2021 – Supplement 6 of this PCN introduces **Security Service Pack #7** (PLAT-rhel7.6-0070.tar; **PLDS ID** CM000001554) and **Kernel Service Pack #7** (KERNEL-3.10.0-1160.11.1.el7.tar; **PLDS ID** CM000001555) for Avaya Aura® Communication Manager 8.1.x (R018x.00.0.890.0).

- A pre-activation patch is required if CM was upgraded in a specific scenario utilizing Avaya Aura® System Manager Solution Deployment Manager (SDM). Please see **PSN020355u** for details.
- Security and Kernel Service Packs should NOT be applied on the Software Only offer.

14 Dec 2020 – Supplement 5 of this PCN introduces **Security Service Pack #6** (PLAT-rhel7.6-0060.tar; **PLDS ID** CM000001548) and **Kernel Service Pack #6** (KERNEL-3.10.0-1160.6.1.el7.tar; **PLDS ID** CM000001549) for Avaya Aura® Communication Manager 8.1.x (R018x.00.0.890.0).

- A pre-activation patch is required if CM was upgraded in a specific scenario utilizing Avaya Aura® System Manager Solution Deployment Manager (SDM). Please see **PSN020355u** for details.
- Security and Kernel Service Packs should NOT be applied on the Software Only offer.

12 Oct 2020 – Supplement 4 of this PCN introduces **Security Service Pack #5** (PLAT-rhel7.6-0050.tar; **PLDS ID** CM000001546) and **Kernel Service Pack #5** (KERNEL-3.10.0-1127.19.1.el7.tar; **PLDS ID** CM000001547) for Avaya Aura® Communication Manager 8.1.x (R018x.00.0.890.0).

- A pre-activation patch is required if CM was upgraded in a specific scenario utilizing Avaya

Aura® System Manager Solution Deployment Manager (SDM).

Please see **PSN020355u** for details.

- Security and Kernel Service Packs should NOT be applied on the Software Only offer.

19 June 2020 – Supplement 3-1 of this PCN provides an update in **Section 1B – Security Information** to the list of **Security vulnerabilities resolved in CM 8.1 Security Service Pack #4**. RHSA-2020:1190 has been added as resolved in SSP#4.

08 June 2020 – Supplement 3 of this PCN introduces **Security Service Pack #4** (PLAT-rhel7.6-0040.tar; **PLDS ID** CM000001540) and **Kernel Service Pack #4** (KERNEL-3.10.0-1127.el7; **PLDS ID** CM000001541) for Avaya Aura® Communication Manager 8.1.x (R018x.00.0.890.0).

- A pre-activation patch is required if CM was upgraded in a specific scenario utilizing Avaya Aura® System Manager Solution Deployment Manager (SDM). Please see **PSN020355u** for details.
- Security and Kernel Service Packs should NOT be applied on the Software Only offer.

02 Mar 2020 – Supplement 2 of this PCN introduces **Security Service Pack #3** (PLAT-rhel7.6-0030.tar; **PLDS ID** CM000001532) and **Kernel Service Pack #3** (KERNEL-3.10.0-1062.9.1.el7; **PLDS ID** CM000001533) for Avaya Aura® Communication Manager 8.1.x (R018x.00.0.890.0).

- A pre-activation patch is required if CM was upgraded in a specific scenario utilizing Avaya Aura® System Manager Solution Deployment Manager (SDM). Please see **PSN020355u** for details.
- Security and Kernel Service Packs should NOT be applied on the Software Only offer.

28 Oct 2019 – Supplement 1 of this PCN introduces **Security Service Pack #2** (PLAT-rhel7.6-0020.tar; **PLDS ID** CM000001523) and **Kernel Service Pack #2** (KERNEL-3.10.0-1062.1.2.el7.tar; **PLDS ID** CM000001524) for Avaya Aura® Communication Manager 8.1.x (R018x.00.0.890.0).

- A pre-activation patch is required if CM was upgraded in a specific scenario utilizing Avaya Aura® System Manager Solution Deployment Manager (SDM). Please see **PSN020355u** for details.
- Security and Kernel Service Packs should NOT be applied on the Software Only offer.

15 July 2019 – This PCN introduces **Security Service Pack #1** (PLAT-rhel7.6-0010.tar; **PLDS ID** CM000001520) and **Kernel Service Pack #1** (KERNEL-3.10.0-957.21.3.el7.tar; **PLDS ID** CM000001521) for Avaya Aura® Communication Manager 8.1.x (R018x.00.0.890.0).

- A pre-activation patch is required if CM was upgraded in a specific scenario utilizing Avaya Aura® System Manager Solution Deployment Manager (SDM). Please see **PSN020355u** for details.
- Security and Kernel Service Packs should NOT be applied on the Software Only offer.

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

Class 2

**Is it required
that this PCN be
applied to my**

This PCN is recommended for Communication Manager 8.1.x. It is not applicable to the Software Only offer.

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 PCN applies to both US and non-US customers.

Does applying this PCN disrupt my service during installation?

Activation of the Security Service Pack and/or Kernel Service Pack will disrupt service since they both require a full Linux reboot of the Communication Manager Virtual Machine (VM) to take effect.

Installation of this PCN is required by:

Customer or Avaya Authorized Service Provider. This upgrade is customer installable and remotely installable.

Release notes and workarounds are located:

The Security Service Pack and Kernel Service Pack resolve vulnerabilities described by Avaya Security Advisories (ASA) referenced in section 1B – Security information. The ASAs referenced in section 1B can be viewed by performing the following steps in a browser.

1. Go to <http://support.avaya.com> 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 (SSP) and Kernel Service Packs (KSP) are cumulative. This means that all fixes in previous 8.1.x KSPs and SSPs are included in the most recent KSP and 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 Communication 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 Communication 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 and Kernel 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 **Communication Manager** and when Avaya Aura® Communication Manager appears as a selection below, select it.
4. Select 8.1.x from the **Choose Release** pull down menu to the right.
5. Select **Downloads** on the new page that is displayed. Scroll down (if necessary) and select **View All Downloads**.
6. Select **Avaya Aura® Communication Manager 8.1.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 **Communication Manager** in the **Product Line** search field to display frequently downloaded Communication Manager software, including recent Service Packs and other software updates.
2. All Communication Manager 8.1 software downloads are available on PLDS. In the PLDS **View Downloads** section under the **Search by Download** tab, select **Communication Manager** in the **Application** search field and **8.1** in the **Version** search field to display all available Communication Manager 8.1 software downloads.

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

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

The instructions for installing or upgrading Communication Manager software 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 click **LOG IN**.
2. Mouse over **Search Product** at the top of the page, click **Documents** in the menu.
3. Begin to type **Communication Manager** and when Avaya Aura® Communication Manager appears as a selection below, select it.
4. Select **8.1.x** from the **Choose Release** pull down menu to the right.

5. Select **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 **Installation Migrations Upgrades & Configurations**.
7. Select the appropriate deployment document based on the deployment platform..

Important Security Service Pack Installation Notes:

A pre-activation patch may be required if CM was upgraded in a specific scenario utilizing Avaya Aura® System Manager Solution Deployment Manager (SDM).
Please see **PSN020355u** for details.

1. Security Service Packs are independent of other Communication Manager software updates activated on a server including CM Service Packs, Kernel Service Packs, over-writable patches or custom patches. None of these other software updates should be deactivated before installing a Security Service Pack.
2. 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.
3. Any previous Security Service Pack must be deactivated before activating a new Security Service Pack.
4. If the system cannot reach the IP address or hostname for an NTP server, remove it from the NTP configuration. After removing any unreachable NTP servers, activate the Security Service Pack. The system will reboot automatically shortly after activation is successful. If desired, previously removed NTP servers may be re-added to the NTP configuration after the system has rebooted. Note that system time changes and NTP server changes can cause service disruptions.
5. **Important:** An automatic server reboot will occur after successful activation of a Security Service Pack. The activation steps for a Security Service Pack are:
 - a. Run the following bash Command Line Interface (CLI) commands on the server (Example is for SSP1):
 - `update_unpack PLAT-rhel7.6-0010`
 - `update_activate PLAT-rhel7.6-0010`
 - b. After successful activation of the Security Service Pack the server will automatically do a full Linux reboot in about 2 minutes.
 - c. After the reboot nothing else needs to be done, the Security Service Pack will be fully activated and in use by the Communication Manager Virtual Machine.

Important Kernel Service Pack Installation Notes:

A pre-activation patch may be required CM was upgraded in a specific scenario utilizing Avaya Aura® System Manager Solution Deployment Manager (SDM).
Please see **PSN020355u** for details.

1. Kernel Service Packs are independent of other Communication Manager software updates activated, including Communication Manager Service Packs, Security Service Packs, over-writable patches or custom patches. None of these other software updates should be deactivated before activating a Kernel Service Pack.

2. Kernel Service Packs are cumulative for the release they apply to. In other words, the current Kernel Service Pack for a release will include the fixes from all previous Kernel Service Packs for that release.
3. It is not necessary to deactivate an existing Kernel Service Pack before activating a new Kernel Service Pack. Doing so will result in unnecessary additional reboots.

SECTION 1A – SOFTWARE SERVICE PACK INFORMATION

Note: Customers are required to backup their systems before applying Service Packs/Feature Packs.

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

Using the bash Command Line Interface (CLI) run the following command on the server:

➤ update_show

This should show the status of the Security Service Pack and/or Kernel Service Pack (Update ID) as “activated”.

You can also use the Communication Manager System Management Interface (SMI) from the **Administration > Server (Maintenance) > Server Upgrades > Manage Updates** page.

What you should do if the Service Pack installation fails?

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

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

To remove (deactivate) the Kernel Service Pack use the Communication Manager System Management Interface (SMI) from the **Administration > Server (Maintenance) > Server Upgrades > Manage Updates** page.

Although Security Service Packs can be deactivated, the updates installed will still be in use by the server and cannot be removed or backed out to previous versions.

➤ **NOTE:** With Security Service Packs, deactivating the Security Service Pack and attempting to activate an older/lower numbered Security Service Pack will fail and include errors similar to the following:

Install of rpms in PLAT-rhel7.6-00x0 failed!
Failed to activate PLAT-rhel7.6-00x0!

SECTION 1B – SECURITY INFORMATION

Are there any security risks involved?

Issues described by the Avaya Security Advisories listed in the next section are corrected by the Security Service Pack or Kernel Service Pack as noted. Security Service Packs (SSP) and Kernel Service Packs (KSP) include the fixes from all previous SSPs and KSPs respectively for a given CM release.

Avaya Security Vulnerability Classification:

Note: A Classification of None in the tables below means the affected components are installed, but the vulnerability is not exploitable.
As noted in the Description section of this PCN, SSP and KSP required artifacts and fix IDs will

no longer be tracked in the Avaya Aura 8.1.x Release Notes but will be included in this PCN.

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

CM 8.1.x SSP #30 includes the following rpm updates:

bind-export-libs-9.11.4-26.P2.el7_9.13.x86_64.rpm	nss-softokn-3.79.0-4.el7_9.x86_64.rpm
bind-libs-9.11.4-26.P2.el7_9.13.x86_64.rpm	nss-softokn-freebl-3.79.0-4.el7_9.i686.rpm
bind-libs-lite-9.11.4-26.P2.el7_9.13.x86_64.rpm	nss-softokn-freebl-3.79.0-4.el7_9.x86_64.rpm
bind-license-9.11.4-26.P2.el7_9.13.noarch.rpm	nss-sysinit-3.79.0-5.el7_9.x86_64.rpm
bind-utils-9.11.4-26.P2.el7_9.13.x86_64.rpm	nss-tools-3.79.0-5.el7_9.x86_64.rpm
httpd-2.4.6-98.el7_9.7.x86_64.rpm	nss-util-3.79.0-1.el7_9.i686.rpm
httpd-tools-2.4.6-98.el7_9.7.x86_64.rpm	nss-util-3.79.0-1.el7_9.x86_64.rpm
mod_ssl-2.4.6-98.el7_9.7.x86_64.rpm	openssl-1.0.2k-26.el7_9.x86_64.rpm
nspr-4.34.0-3.1.el7_9.i686.rpm	openssl-libs-1.0.2k-26.el7_9.i686.rpm
nspr-4.34.0-3.1.el7_9.x86_64.rpm	openssl-libs-1.0.2k-26.el7_9.x86_64.rpm
nss-3.79.0-5.el7_9.i686.rpm	zlib-1.2.7-21.el7_9.i686.rpm
nss-3.79.0-5.el7_9.x86_64.rpm	zlib-1.2.7-21.el7_9.x86_64.rpm
nss-softokn-3.79.0-4.el7_9.i686.rpm	

Security vulnerabilities resolved in CM 8.1 Security Service Pack #30

Fix ID	Updated Package	RHSA/RHBA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-53715	bind-export-libs bind-libs bind-libs-lite bind-license bind-utils	RHSA-2023:0402	CVE-2021-25220 CVE-2022-2795	Moderate	ASA-2023-014	Medium
	httpd httpd-tools mod_ssl	RHSA-2023:1593	CVE-2023-25690	Important	ASA-2023-032	Critical
	nss nss-sysinit nss-tools	RHSA-2023:1332	CVE-2023-0767	Important	none	none
	openssl openssl-libs	RHSA-2023:1335	CVE-2023-0286	Important	ASA-2023-030	High
	zlib	RHSA-2023:1095	CVE-2022-37434	Moderate	none	none

CM 8.1.x KSP #30 includes the following rpm updates:

kernel-3.10.0-1160.88.1.el7.x86_64	kernel-tools-3.10.0-1160.88.1.el7.x86_64
kernel-devel-3.10.0-1160.88.1.el7.x86_64	kernel-tools-libs-3.10.0-1160.88.1.el7.x86_64
kernel-headers-3.10.0-1160.88.1.el7.x86_64	python-perf-3.10.0-1160.88.1.el7.x86_64

Security vulnerabilities resolved in CM 8.1 Kernel Service Pack #30

Fix ID	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-53174	kernel security, bug fix, and enhancement update	RHSA-2023:1091	CVE-2022-4378 CVE-2022-42703	Important	ASA-2023-029	High

CM 8.1.x SSP #29 includes the following rpm updates:

java-1.8.0-openjdk-headless-1:1.8.0.362.b08-1.el7_9.x86_64 sudo-1.8.23-10.el7_9.3.x86_64	tzdata-java-2022g-1.el7.noarch.rpm
---	------------------------------------

Security vulnerabilities resolved in CM 8.1 Security Service Pack #29

Fix ID	Updated Package	RHSA/RHBA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-53040	java	RHSA-2023:0203	CVE-2023-21830 CVE-2023-21843	Moderate	ASA-2023-015	Medium
	tzdata-java	RHBA-2022:8785	none	Bug fix advisory	none	none
	sudo	RHSA-2023:0291	CVE-2023-22809	Important	none	none

The February 2023 release of Security Updates did not require a new Kernel Service Pack. **Kernel Service Pack #27** should continue to be used.

CM 8.1.x SSP #28 includes the following rpm updates:

krb5-libs-1.15.1-55.el7_9.i686.rpm	krb5-libs-1.15.1-55.el7_9.x86_64.rpm
------------------------------------	--------------------------------------

Security vulnerabilities resolved in CM 8.1 Security Service Pack #28

Fix ID	Updated Package	RHSA/RHBA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-52890	krb5	RHSA-2022:8640	CVE-2022-42898	Important	ASA-2022-161	Medium

The January 2023 release of Security Updates did not require a new Kernel Service Pack. **Kernel Service Pack #27** should continue to be used.

.....

CM 8.1.x SSP #27 includes the following rpm updates:

kpartx-0.4.9-136.el7_9.x86_64.rpm	php-pear-1.9.4-23.el7_9.noarch.rpm
-----------------------------------	------------------------------------

Security vulnerabilities resolved in CM 8.1 Security Service Pack #27

Fix ID	Updated Package	RHSA/RHBA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-52566	kpartx	RHSA-2022:7186	CVE-2022-41974	Important	None	None
	php-pear	RHSA-2022:7340	CVE-2022-28948,CVE-2022-28949,CVE-2022-36193	Moderate	ASA-2022-133	High

CM 8.1.x KSP #27 includes the following rpm updates:

kernel-3.10.0-1160.80.1.el7.x86_64.rpm kernel-devel-3.10.0-1160.80.1.el7.x86_64.rpm kernel-headers-3.10.0-1160.80.1.el7.x86_64.rpm	kernel-tools-3.10.0-1160.80.1.el7.x86_64.rpm kernel-tools-libs-3.10.0-1160.80.1.el7.x86_64.rpm python-perf-3.10.0-1160.80.1.el7.x86_64.rpm
--	--

Security vulnerabilities resolved in CM 8.1 Kernel Service Pack #27

Fix ID	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-52567	kernel security, bug fix, and enhancement update	RHSA-2022:7337	CVE-2022-2588 CVE-2022-23816 CVE-2022-23825 CVE-2022-26373 CVE-2022-29900 CVE-2022-29901	Important	ASA-2022-152	High

.....

CM 8.1.x SSP #26 includes the following rpm updates:

bind-export-libs-32:9.11.4-26.P2.el7_9.10.x86_64 bind-libs-lite-32:9.11.4-26.P2.el7_9.10.x86_64 bind-libs-32:9.11.4-26.P2.el7_9.10.x86_64	bind-utils-32:9.11.4-26.P2.el7_9.10.x86_64 expat-2.1.0-15.el7_9.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.352.b08-2.el7_9.x86_64
---	---

bind-license-32:9.11.4-26.P2.el7_9.10.noarch

tzdata-java-2022e-1.el7.noarch.rpm

Security vulnerabilities resolved in CM 8.1 Security Service Pack #26

Fix ID	Updated Package	RHSA/RHBA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-52297	bind-export-libs; bind-libs; bind-libs-lite; bind-license; bind-utils	RHSA-2022:6765	CVE-2022-38177 CVE-2022-38178	Important	ASA-2022-124	High
	xpat	RHSA-2022:6834	CVE-2022-40674	Important	ASA-2022-125	Critical
	java	RHSA-2022:7002	CVE-2022-21619 CVE-2022-21624 CVE-2022-21626 CVE-2022-21628	Moderate	ASA-2022-127	Medium
	tzdata-java-2022e update	RHBA-2022:7067	NA	Bug Fix Advisory	NA	NA

The November 2022 release of Security Updates did not require a new Kernel Service Pack. **Kernel Service Pack #24** should continue to be used.

CM 8.1.x SSP #25 includes the following rpm updates:

libgudev1-219-78.el7_9.7.x86_64.rpm	systemd-219-78.el7_9.7.x86_64.rpm
open-vm-tools-11.0.5-3.el7_9.4.x86_64.rpm	systemd-libs-219-78.el7_9.7.x86_64.rpm
rsync-3.1.2-11.el7_9.x86_64.rpm	systemd-sysv-219-78.el7_9.7.x86_64.rpm

Security vulnerabilities resolved in CM 8.1 Security Service Pack #25

Fix ID	Updated Package	RHSA/RHBA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-52063	libgudev1; systemd; systemd-libs; systemd-sysv	RHSA-2022:6160	CVE-2022-2526	Important	ASA-2022-115	High
	rsync	RHSA-2022:6170	CVE-2018-29154	Important	ASA-2022-116	High
	open-vm-tools	RHSA-2022:6381	CVE-2022-31676	Important	ASA-2022-119	High

The October 2022 release of Security Updates did not require a new Kernel Service Pack. **Kernel Service Pack #24** should continue to be used.

CM 8.1.x SSP #24 includes the following rpm updates:

java-1.8.0-openjdk-headless-1.8.0.342.b07-1.el7_9.x86_64.rpm	
--	--

Security vulnerabilities resolved in CM 8.1 Security Service Pack #24

Fix ID	Updated Package	RHSA/RHBA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-51722	java	RHSA-2022:5698	CVE-2022-21540 CVE-2022-21541 CVE-2022-34169	Important	ASA-2022-106	High

CM 8.1.x KSP #24 includes the following rpm updates:

kernel-3.10.0-1160.76.1.el7.x86_64.rpm kernel-devel-3.10.0-1160.76.1.el7.x86_64.rpm kernel-headers-3.10.0-1160.76.1.el7.x86_64.rpm	kernel-tools-3.10.0-1160.76.1.el7.x86_64.rpm kernel-tools-libs-3.10.0-1160.76.1.el7.x86_64.rpm python-perf-3.10.0-1160.76.1.el7.x86_64.rpm
--	--

Security vulnerabilities resolved in CM 8.1 Kernel Service Pack #24

Fix ID	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-51721	kernel security, bug fix, and enhancement update	RHSA-2022:5937	CVE-2022-21123 CVE-2022-21125 CVE-2022-21166	Moderate	ASA-2022-113	Medium

CM 8.1.x SSP #23 includes the following rpm updates:

python-2.7.5-92.el7_9.x86_64.rpm python-libs-2.7.5-92.el7_9.x86_64.rpm sudo-1.8.23-10.el7_9.1.x86_64.rpm	xz-5.2.2-2.el7_9.x86_64.rpm xz-libs-5.2.2-2.el7_9.i686.rpm xz-libs-5.2.2-2.el7_9.x86_64.rpm
--	---

Security vulnerabilities resolved in CM 8.1 Security Service Pack #23

Fix ID	Updated Package	RHSA/RHBA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-50981	sudo	RHSA-2019:3197	CVE-2019-14287	Important	ASA-2019-233	High
	xz;xz-libs;xz-libs	RHSA-2022:5052	CVE-2022-1271	Important	ASA-2022-081	High
	python;python-libs	RHSA-2022:5235	CVE-2020-26116 CVE-2020-26137 CVE-2021-3177	Important	None	None

CM 8.1.x KSP #23 includes the following rpm updates:

kernel-3.10.0-1160.71.1.el7.x86_64.rpm kernel-devel-3.10.0-1160.71.1.el7.x86_64.rpm kernel-headers-3.10.0-1160.71.1.el7.x86_64.rpm	kernel-tools-3.10.0-1160.71.1.el7.x86_64.rpm kernel-tools-libs-3.10.0-1160.71.1.el7.x86_64.rpm python-perf-3.10.0-1160.71.1.el7.x86_64.rpm
--	--

Security vulnerabilities resolved in CM 8.1 Kernel Service Pack #23

Fix ID	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-50982	kernel security, bug fix, and enhancement update	RHSA-2022:5232	CVE-2022-1729 CVE-2022-1966 CVE-2022-32250	Important	ASA-2022-097	High

CM 8.1.x SSP #22 includes the following rpm updates:

gzip-1.5-11.el7_9.x86_64.rpm rsyslog-8.24.0-57.el7_9.3.x86_64.rpm rsyslog-gnutls-8.24.0-57.el7_9.3.x86_64.rpm	zlib-1.2.7-20.el7_9.i686.rpm zlib-1.2.7-20.el7_9.x86_64.rpm
---	--

Security vulnerabilities resolved in CM 8.1 Security Service Pack #22

Fix ID	Updated Package	RHSA/RHBA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-50703	gzip	RHSA-2022:2191	CVE-2022-1271	Important	None	None
CM-50247	zlib;zlib	RHSA-2022:2213	CVE-2018-25032	Important	ASA-2022-064	High
CM-50674	rsyslog;rsyslog-gnutls	RHSA-2022:4803	CVE-2022-24903	Important	ASA-2022-076	High

The July 2022 release of Security Updates did not require a new Kernel Service Pack. **Kernel Service Pack #20** should continue to be used.

CM 8.1.x SSP #21 includes the following rpm updates:

java-1.8.0-openjdk-headless-1.8.0.332.b09-1.el7_9.x86_64.rpm	
--	--

Security vulnerabilities resolved in CM 8.1 Security Service Pack #21

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

CM-50138	java-1.8.0-openjdk security, bug fix, and enhancement update	RHSA-2022:1487	CVE-2022-21426 CVE-2022-21434 CVE-2022-21443 CVE-2022-21476 CVE-2022-21496	Important	ASA-2022-039	High
----------	--	----------------	--	-----------	--------------	------

The June 2022 release of Security Updates did not require a new Kernel Service Pack. **Kernel Service Pack #20** should continue to be used.

.....

CM 8.1.x SSP #20 includes the following rpm updates:

expat-2.1.0-14.el7_9.x86_64.rpm httpd-2.4.6-97.el7_9.5.x86_64.rpm httpd-tools-2.4.6-97.el7_9.5.x86_64.rpm java-1.8.0-openjdk-headless-1.8.0.322.b06-1.el7_9.x86_64.rpm mod_ssl-2.4.6-97.el7_9.5.x86_64.rpm	openssl-1.0.2k-25.el7_9.x86_64.rpm openssl-libs-1.0.2k-25.el7_9.i686.rpm openssl-libs-1.0.2k-25.el7_9.x86_64.rpm tzdata-java-2022a-1.el7.noarch.rpm
--	--

Security vulnerabilities resolved in CM 8.1 Security Service Pack #20

Fix ID	Updated Package	RHSA/RHBA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-49270	httpd security update	RHSA-2022:1045	CVE-2022-22720	Important	ASA-2022-035	Critical
CM-49860	expat security update	RHSA-2022:1069	CVE-2021-45960 CVE-2021-46143 CVE-2022-22822 CVE-2022-22823 CVE-2022-22824 CVE-2022-22825 CVE-2022-22826 CVE-2022-22827 CVE-2022-23852 CVE-2022-25235 CVE-2022-25236 CVE-2022-25315	Important	ASA-2022-067	Critical

CM-49867	java openjdk security update	RHSA-2022:0306	CVE-2022-21248 CVE-2022-21282 CVE-2022-21283 CVE-2022-21293 CVE-2022-21294 CVE-2022-21296 CVE-2022-21299 CVE-2022-21305 CVE-2022-21340 CVE-2022-21341 CVE-2022-21360 CVE-2022-21365	Moderate	ASA-2022-018	Medium
CM-49868	openssl security update	RHSA-2022:1066	CVE-2022-0778	Important	None	None
CM-49862	java-1.8.0-openjdk security update	RHSA-2020:2968	CVE-2020-14556 CVE-2020-14577 CVE-2020-14578 CVE-2020-14579 CVE-2020-14583 CVE-2020-14593 CVE-2020-14621	Important	ASA-2020-098	High
CM-49863	java-1.8.0-openjdk security update	RHSA-2020:4350	CVE-2020-14779 CVE-2020-14781 CVE-2020-14782 CVE-2020-14792 CVE-2020-14796 CVE-2020-14797 CVE-2020-14803	Moderate	ASA-2020-148	Medium
CM-49865	java-1.8.0-openjdk security update	RHSA-2021:2845	CVE-2021-2341 CVE-2021-2369 CVE-2021-2388	Important	ASA-2021-095	High
CM-49812	tzdata-2022a update	RHBA-2022:1032	NA	Bug Fix Advisory	NA	NA

CM 8.1.x KSP #20 includes the following rpm updates:

kernel-3.10.0-1160.62.1.el7.x86_64.rpm	kernel-tools-3.10.0-1160.62.1.el7.x86_64.rpm
kernel-devel-3.10.0-1160.62.1.el7.x86_64.rpm	kernel-tools-libs-3.10.0-1160.62.1.el7.x86_64.rpm
kernel-headers-3.10.0-1160.62.1.el7.x86_64.rpm	python-perf-3.10.0-1160.62.1.el7.x86_64.rpm

Security vulnerabilities resolved in CM 8.1 Kernel Service Pack #20

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

CM-49574	kernel security, bug fix, and enhancement update	RHSA-2022:1198	CVE-2021-4028 CVE-2021-4083	Important	ASA-2022-037	High
----------	--	----------------	--------------------------------	-----------	--------------	------

.....

CM 8.1.x SSP #19 includes the following rpm updates:

cyrus-sasl-lib-2.1.26-24.el7_9.i686.rpm cyrus-sasl-lib-2.1.26-24.el7_9.x86_64.rpm cyrus-sasl-md5-2.1.26-24.el7_9.x86_64.rpm cyrus-sasl-ntlm-2.1.26-24.el7_9.x86_64.rpm cyrus-sasl-plain-2.1.26-24.el7_9.x86_64.rpm	openldap-2.4.44-25.el7_9.i686.rpm openldap-2.4.44-25.el7_9.x86_64.rpm openldap-clients-2.4.44-25.el7_9.x86_64.rpm openldap-servers-2.4.44-25.el7_9.x86_64.rpm
--	--

Security vulnerabilities resolved in CM 8.1 Security Service Pack #19

Fix ID	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-48960	cyrus-sasl	RHSA-2022:0666	CVE-2022-24407	Important	ASA-2022-027	Critical
CM-48785	openldap	RHSA-2022:0621	CVE-2020-25709 CVE-2020-25710	Moderate	ASA-2022-025	High

CM 8.1.x KSP #19 includes the following rpm updates:

kernel-3.10.0-1160.59.1.el7.x86_64.rpm kernel-devel-3.10.0-1160.59.1.el7.x86_64.rpm kernel-headers-3.10.0-1160.59.1.el7.x86_64.rpm	kernel-tools-3.10.0-1160.59.1.el7.x86_64.rpm kernel-tools-libs-3.10.0-1160.59.1.el7.x86_64.rpm python-perf-3.10.0-1160.59.1.el7.x86_64.rpm
--	--

Security vulnerabilities resolved in CM 8.1 Kernel Service Pack #19

Fix ID	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-48803	kernel security and bug fix update	RHSA-2022:0620	CVE-2020-0465 CVE-2020-0466 CVE-2021-0920 CVE-2021-3564 CVE-2021-3573 CVE-2021-3752 CVE-2021-4155 CVE-2022-0330 CVE-2022-22942	Important	ASA-2022-026	High

CM 8.1.x SSP #18 includes the following rpm updates:

aide-0.15.1-13.el7_9.1.x86_64.rpm	polkit-0.112-26.el7_9.1.x86_64.rpm
-----------------------------------	------------------------------------

Security vulnerabilities resolved in CM 8.1 Security Service Pack #18

Fix ID	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-48368	Polkit	RHSA-2022:0274	CVE-2021-4034	Important	ASA-2022-010	High
CM-48628	aide	RHSA-2022:0473	CVE-2021-45417	Important	N/A	N/A

CM 8.1.x KSP #18 includes the following rpm updates:

kernel-3.10.0-1160.53.1.el7.x86_64.rpm	kernel-tools-3.10.0-1160.53.1.el7.x86_64.rpm
kernel-devel-3.10.0-1160.53.1.el7.x86_64.rpm	kernel-tools-libs-3.10.0-1160.53.1.el7.x86_64.rpm
kernel-headers-3.10.0-1160.53.1.el7.x86_64.rpm	python-perf-3.10.0-1160.53.1.el7.x86_64.rpm

Security vulnerabilities resolved in CM 8.1 Kernel Service Pack #18

Fix ID	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-48370	kernel security and bug fix update	RHSA-2022:0063	CVE-2020-25704 CVE-2020-36322 CVE-2021-42739	Moderate	ASA-2022-011	Medium

CM 8.1.x SSP #17 includes the following rpm updates:

httpd-2.4.6-97.el7_9.4.x86_64.rpm	openssl-1.0.2k-23.el7_9.x86_64.rpm
httpd-tools-2.4.6-97.el7_9.4.x86_64.rpm	openssl-libs-1.0.2k-23.el7_9.i686.rpm
mod_ssl-2.4.6-97.el7_9.4.x86_64.rpm	openssl-libs-1.0.2k-23.el7_9.x86_64.rpm

Security vulnerabilities resolved in CM 8.1 Security Service Pack #17

Fix ID	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-48231	httpd	RHSA-2022:0143	CVE-2021-44790 CVE-2021-26691 CVE-2021-34798 CVE-2021-39275	Important	ASA-2022-003	Critical
CM-48244	openssl	RHSA-2022:0064	CVE-2021-3712	Moderate	ASA-2022-004	High

.....

CM 8.1.x SSP #16 includes the following rpm updates:

krb5-libs-1.15.1-51.el7_9.i686.rpm	nss-tools-3.67.0-4.el7_9.x86_64.rpm
krb5-libs-1.15.1-51.el7_9.x86_64.rpm	nss-util-3.67.0-1.el7_9.i686.rpm
nspr-4.32.0-1.el7_9.i686.rpm	nss-util-3.67.0-1.el7_9.x86_64.rpm
nspr-4.32.0-1.el7_9.x86_64.rpm	openssh-7.4p1-22.el7_9.x86_64.rpm
nss-3.67.0-4.el7_9.i686.rpm	openssh-clients-7.4p1-22.el7_9.x86_64.rpm
nss-3.67.0-4.el7_9.x86_64.rpm	openssh-server-7.4p1-22.el7_9.x86_64.rpm
nss-softokn-3.67.0-3.el7_9.i686.rpm	rpm-4.11.3-48.el7_9.x86_64.rpm
nss-softokn-3.67.0-3.el7_9.x86_64.rpm	rpm-build-libs-4.11.3-48.el7_9.x86_64.rpm
nss-softokn-freebl-3.67.0-3.el7_9.i686.rpm	rpm-libs-4.11.3-48.el7_9.x86_64.rpm
nss-softokn-freebl-3.67.0-3.el7_9.x86_64.rpm	rpm-python-4.11.3-48.el7_9.x86_64.rpm
nss-sysinit-3.67.0-4.el7_9.x86_64.rpm	

Security vulnerabilities resolved in CM 8.1 Security Service Pack #16

Fix ID	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-47715	krb5	RHSA-2021:4788	CVE-2021-37750	Moderate	ASA-2021-179	Medium
CM-47717	rpm	RHSA-2021:4785	CVE-2021-20271	Moderate	ASA-2021-180	Medium
CM-47788	openssh	RHSA-2021:4782	CVE-2021-41617	Moderate	ASA-2021-183	High
CM-47789	nss	RHSA-2021:4904	CVE-2021-43527	Critical	ASA-2021-184	Critical

CM 8.1.x KSP #16 includes the following rpm updates:

kernel-3.10.0-1160.49.1.el7.x86_64.rpm	kernel-tools-3.10.0-1160.49.1.el7.x86_64.rpm
kernel-devel-3.10.0-1160.49.1.el7.x86_64.rpm	kernel-tools-libs-3.10.0-1160.49.1.el7.x86_64.rpm
kernel-headers-3.10.0-1160.49.1.el7.x86_64.rpm	python-perf-3.10.0-1160.49.1.el7.x86_64.rpm

Security vulnerabilities resolved in CM 8.1 Kernel Service Pack #16

Fix ID	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-47718	kernel security and bug fix update	RHSA-2021:4777	CVE-2020-36385	Important	ASA-2021-182	High

.....

CM 8.1.x SSP #15 includes the following rpm updates:

binutils-2.27-44.base.el7_9.1.x86_64.rpm	libxml2-2.9.1-6.el7_9.6.x86_64.rpm
httpd-2.4.6-97.el7_9.1.x86_64.rpm	libxml2-python-2.9.1-6.el7_9.6.x86_64.rpm
httpd-tools-2.4.6-97.el7_9.1.x86_64.rpm	mod_ssl-2.4.6-97.el7_9.1.x86_64.rpm
java-1.8.0-openjdk-headless-1.8.0.312.b07-1.el7_9.x86_64.rpm	openssl-1.0.2k-22.el7_9.x86_64.rpm
libxml2-2.9.1-6.el7_9.6.i686.rpm	openssl-libs-1.0.2k-22.el7_9.i686.rpm
	openssl-libs-1.0.2k-22.el7_9.x86_64.rpm

Security vulnerabilities resolved in CM 8.1 Security Service Pack #15

Fix ID	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-47139	httpd security update	RHSA-2021:3856	CVE-2021-40438	Important	ASA-2021-119	Critical
CM-47140	openssl security update	RHSA-2021:3798	CVE-2021-23840 CVE-2021-23841	Moderate	ASA-2021-120	High
CM-47143	java-1.8.0-openjdk security and bug fix update	RHSA-2021:3889	CVE-2021-35565 CVE-2021-35567 CVE-2021-35550 CVE-2021-35556 CVE-2021-35559 CVE-2021-35561 CVE-2021-35564 CVE-2021-35578 CVE-2021-35586 CVE-2021-35588 CVE-2021-35603	Important	ASA-2021-124	Medium
CM-47144	binutils security update	RHSA-2021:4033	CVE-2021- 42574	Moderate	ASA-2021-128	High
CM-47145	libxml2 security update	RHSA-2021:3810	CVE-2016-4658	Moderate	ASA-2021-129	Medium

CM 8.1.x KSP #15 includes the following rpm updates:

kernel-3.10.0-1160.45.1.el7.x86_64.rpm	kernel-tools-3.10.0-1160.45.1.el7.x86_64.rpm
kernel-devel-3.10.0-1160.45.1.el7.x86_64.rpm	kernel-tools-libs-3.10.0-1160.45.1.el7.x86_64.rpm
kernel-headers-3.10.0-1160.45.1.el7.x86_64.rpm	python-perf-3.10.0-1160.45.1.el7.x86_64.rpm

Security vulnerabilities resolved in CM 8.1 Kernel Service Pack #15

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

CM-47138	kernel security and bug fix update	RHSA-2021:3801	CVE-2021-22543 CVE-2021-37576 CVE-2021-3653 CVE-2021-3656	Important	ASA-2021-118	High
----------	------------------------------------	----------------	--	-----------	--------------	------

.....

CM 8.1.x SSP #14 includes the following rpm updates:

bind-export-libs-9.11.4-26.P2.el7_9.7.x86_64.rpm bind-libs-9.11.4-26.P2.el7_9.7.x86_64.rpm bind-libs-lite-9.11.4-26.P2.el7_9.7.x86_64.rpm bind-license-9.11.4-26.P2.el7_9.7.noarch.rpm bind-utils-9.11.4-26.P2.el7_9.7.x86_64.rpm	java-1.8.0-openjdk-headless-1.8.0.302.b08-0.el7_9.x86_64.rpm libX11-1.6.7-4.el7_9.x86_64.rpm libX11-common-1.6.7-4.el7_9.noarch.rpm libsndfile-1.0.25-12.el7_9.1.x86_64.rpm microcode_ctl-2.1-73.11.el7_9.x86_64.rpm
---	--

Security vulnerabilities resolved in CM 8.1 Security Service Pack #14

Fix ID	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-43371	java-1.8.0-openjdk security and bug fix update	RHSA-2021:2845	CVE-2021-2388 CVE-2021-2341 CVE-2021-2369	Important	ASA-2021-095	High
CM-43372	microcode_ctl security, bug fix and enhancement update	RHSA-2021:3028	CVE-2020-0543 CVE-2020-0548 CVE-2020-0549 CVE-2020-24489 CVE-2020-24511 CVE-2020-24512 CVE-2020-8695 CVE-2020-8696 CVE-2020-8698	Important	ASA-2021-105	High
CM-43820	libsndfile security update	RHSA-2021:3295	CVE-2021-3246	Important	ASA-2021-109	High
CM-44400	libX11 security update	RHSA-2021:3296	CVE-2021-31535	Important	ASA-2021-114	High
CM-44605	bind security update	RHSA-2021:3325	CVE-2021-25214	Moderate	ASA-2021-122	Medium

CM 8.1.x KSP #14 includes the following rpm updates:

kernel-3.10.0-1160.42.2.el7.x86_64.rpm kernel-devel-3.10.0-1160.42.2.el7.x86_64.rpm kernel-headers-3.10.0-1160.42.2.el7.x86_64.rpm	kernel-tools-3.10.0-1160.42.2.el7.x86_64.rpm kernel-tools-libs-3.10.0-1160.42.2.el7.x86_64.rpm python-perf-3.10.0-1160.42.2.el7.x86_64.rpm
--	--

Security vulnerabilities resolved in CM 8.1 Kernel Service Pack #14

Fix ID	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-44187	Important: kernel security and bug fix update	RHSA-2021:3327	CVE-2020-27777 CVE-2021-22555 CVE-2021-32399 CVE-2021-29154 CVE-2021-29650	Important	ASA-2021-110	High
CM-44401	Moderate: kernel security and bug fix update	RHSA-2021:3438	CVE-2021-3715	Moderate	ASA-2021-113	High

.....

CM 8.1.x KSP #13 includes the following rpm updates:

kernel-3.10.0-1160.36.2.el7.x86_64.rpm kernel-devel-3.10.0-1160.36.2.el7.x86_64.rpm kernel-headers-3.10.0-1160.36.2.el7.x86_64.rpm	kernel-tools-3.10.0-1160.36.2.el7.x86_64.rpm kernel-tools-libs-3.10.0-1160.36.2.el7.x86_64.rpm python-perf-3.10.0-1160.36.2.el7.x86_64.rpm
--	--

Security vulnerabilities resolved in CM 8.1 Kernel Service Pack #12

Fix ID	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-42341	Important: kernel security and bug fix update	RHSA-2021:2725	CVE-2019-20934 CVE-2020-11668 CVE-2021-33033 CVE-2021-33034 CVE-2021-33909	Important	ASA-2021-103	High

.....

CM 8.1.x SSP #12 includes the following rpm updates:

dhclient-4.2.5-83.el7_9.1.x86_64.rpm dhcp-common-4.2.5-83.el7_9.1.x86_64.rpm	dhcp-libs-4.2.5-83.el7_9.1.x86_64.rpm microcode_ctl-2.1-73.9.el7_9.x86_64.rpm
---	--

Security vulnerabilities resolved in CM 8.1 Security Service Pack #11

Fix ID	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-42168	microcode_ctl	RHSA-2021:2305	CVE-2020-24489 CVE-2020-24511 CVE-2020-24512 CVE-2020-24513	Important	ASA-2021-079	High
CM-42169	dhcp	RHSA-2021:2357	CVE-2021-25217	Important	ASA-2021-085	High

CM 8.1.x KSP #12 includes the following rpm updates:

kernel-3.10.0-1160.21.1.el7.x86_64 kernel-devel-3.10.0-1160.21.1.el7.x86_64 kernel-headers-3.10.0-1160.21.1.el7.x86_64	kernel-tools-3.10.0-1160.21.1.el7.x86_64 kernel-tools-libs-3.10.0-1160.21.1.el7.x86_64 python-perf-3.10.0-1160.21.1.el7.x86_64
--	--

Security vulnerabilities resolved in CM 8.1 Kernel Service Pack #12

Fix ID	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-41482	Important: kernel security and bug fix update	RHSA-2021-2314	CVE-2020-12362	Important	ASA-2021-083	High

CM 8.1.x SSP #11 includes the following rpm updates:

glib2-2.56.1-9.el7_9.i686.rpm	glib2-2.56.1-9.el7_9.x86_64.rpm
-------------------------------	---------------------------------

Security vulnerabilities resolved in CM 8.1 Security Service Pack #11

Fix ID	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-41377	glib2	RHSA-2021:2147	CVE-2021-27219	Important	ASA-2021-072	Critical

CM 8.1.x SSP #10 includes the following rpm updates:

bind-export-libs-9.11.4-26.P2.el7_9.5.x86_64.rpm bind-libs-9.11.4-26.P2.el7_9.5.x86_64.rpm bind-libs-lite-9.11.4-26.P2.el7_9.5.x86_64.rpm bind-license-9.11.4-26.P2.el7_9.5.noarch.rpm bind-utils-9.11.4-26.P2.el7_9.5.x86_64.rpm java-1.8.0-openjdk-headless-1.8.0.292.b10-1.el7_9.x86_64.rpm openldap-2.4.44-23.el7_9.i686.rpm openldap-2.4.44-23.el7_9.x86_64.rpm	openldap-clients-2.4.44-23.el7_9.x86_64.rpm openldap-servers-2.4.44-23.el7_9.x86_64.rpm nss-3.53.1-7.el7_9.i686.rpm nss-3.53.1-7.el7_9.x86_64.rpm nss-sysinit-3.53.1-7.el7_9.x86_64.rpm nss-tools-3.53.1-7.el7_9.x86_64.rpm tzdata-2021a-1.el7.noarch.rpm tzdata-java-2021a-1.el7.noarch.rpm
---	---

Security vulnerabilities resolved in CM 8.1 Security Service Pack #10

Fix ID	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-40950	nss nss-sysinit nss-tools	RHSA-2021:1384	CVE-2020-25648	Moderate	ASA-2021-035	High

CM-40951	bind-libs bind-libs-lite bind-license bind-utils bind-export-libs	RHSA-2021:1469	CVE-2021-25215	Important	ASA-2021-037	High
CM-40952	java-1.8.0- openjdk- headless	RHSA-2021:1298	CVE-2021-2163	Moderate	ASA-2021-034	Medium
CM-40953	openldap openldap- servers openldap-clients	RHSA-2021:1389	CVE-2020-25692	Moderate	ASA-2021-042	High

.....

CM 8.1.x SSP #9 includes the following rpm updates:

nettle-2.7.1-9.el7_9.x86_64.rpm	wpa_supplicant-2.6-12.el7_9.2.x86_64.rpm
screen-4.1.0-0.27.20120314git3c2946.el7_9.x86_64.rpm	

Security vulnerabilities resolved in CM 8.1 Security Service Pack #9

Fix ID	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-40532	screen	RHSA-2021:0742	CVE-2021-26937	Important	ASA-2021-024	Critical
CM-40530	wpa_supplicant	RHSA-2021:0808	CVE-2021-27803	Important	ASA-2021-022	High
CM-40523	nettle	RHSA-2021:1145	CVE-2021-20305	Important	ASA-2021-028	High

CM 8.1.x KSP #9 includes the following rpm updates:

kernel-3.10.0-1160.21.1.el7.x86_64	kernel-tools-3.10.0-1160.21.1.el7.x86_64
kernel-devel-3.10.0-1160.21.1.el7.x86_64	kernel-tools-libs-3.10.0-1160.21.1.el7.x86_64
kernel-headers-3.10.0-1160.21.1.el7.x86_64	python-perf-3.10.0-1160.21.1.el7.x86_64

Security vulnerabilities resolved in CM 8.1 Kernel Service Pack #9

Fix ID	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-40527	kernel	RHSA-2021:0856	CVE-2021-27364 CVE-2021-27365 CVE-2021-27363	Important	ASA-2021-021	High

CM-40395	kernel-devel kernel-headers kernel-tools kernel-tools-libs python-perf	RHSA-2021:1071	CVE-2020-25211 CVE-2020-28374 CVE-2020-29661 CVE-2019-19532 CVE-2020-0427 CVE-2020-7053 CVE-2020-14351 CVE-2020-25645 CVE-2020-25656 CVE-2020-25705 CVE-2021-20265	Important	ASA-2021-027	High
----------	--	----------------	--	-----------	--------------	------

Security vulnerabilities resolved in CM 8.1 Security Service Pack #8

Fix Id	RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
CM-39465	RHSA-2021:0221	Important	ASA-2021-009	High
CM-39465	RHSA-2021:0339	Important	ASA-2021-011	High
CM-39465	RHSA-2021:0343	Moderate	ASA-2021-013	High
CM-39465	RHSA-2021:0348	Moderate	ASA-2021-014	High
CM-39465	RHSA-2021:0671	Important	ASA-2021-018	High
CM-39465	RHSA-2020:5350	Important	ASA-2020-205	High
CM-39465	RHSA-2021:0699	Moderate	ASA-2021-019	High

Security vulnerabilities resolved in CM 8.1 Kernel Service Pack #8

Fix Id	RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
CM-39449	RHSA-2021:0336	Moderate	ASA-2021-010	Medium

Security vulnerabilities resolved in CM 8.1 Security Service Pack #7

Fix Id	RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
CM-38154	RHSA-2020:5566	Important	ASA-2021-001	Medium
CM-36234	RHSA-2020:4041	Moderate	ASA-2020-121	High

Security vulnerabilities resolved in CM 8.1 Kernel Service Pack #7

Fix Id	RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
CM-38153	RHSA-2020:5437	Important	ASA-2020-208	High

Security vulnerabilities resolved in CM 8.1 Security Service Pack #6

Fix Id	RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
CM-36613	RHSA-2020:3915	Moderate	ASA-2020-135	Medium
CM-36612	RHSA-2020:4011	Moderate	ASA-2020-133	High
CM-36609	RHSA-2020:4032	Moderate	ASA-2020-136	High
CM-36603	RHSA-2020:4007	Low	ASA-2020-128	Low
CM-36606	RHSA-2020:3978	Moderate	ASA-2020-125	Medium
CM-36607	RHSA-2020:3996	Moderate	ASA-2020-122	High
CM-36601	RHSA-2020:3958	Moderate	ASA-2020-142	Medium
CM-36604	RHSA-2020:3861	Low	ASA-2020-124	Low
CM-36599	RHSA-2020:4003	Moderate	ASA-2020-127	Medium
CM-36602	RHSA-2020:4072	Moderate	ASA-2020-131	High
CM-36608	RHSA-2020:3908	Moderate	ASA-2020-120	Medium
CM-36605	RHSA-2020:4076	Moderate	ASA-2020-119	High
CM-36598	RHSA-2020:3916	Moderate	ASA-2020-132	Medium
CM-36924	RHSA-2020:3952	Moderate	ASA-2020-116	Medium
CM-36933	RHSA-2020:4026	Moderate	ASA-2020-112	Medium
CM-36932	RHSA-2020:3902	Moderate	ASA-2020-139	High
CM-36942	RHSA-2020:3922	Low	ASA-2020-126	Low
CM-36929	RHSA-2020:4350	Moderate	ASA-2020-148	Medium
CM-36926	RHSA-2020:4908	Important	ASA-2020-182	Medium
CM-36944	RHSA-2020:4907	Important	ASA-2020-187	High
CM-36940	RHSA-2019:2136	Important	ASA-2019-185	Medium
CM-36938	RHSA-2019:2181	Low	ASA-2019-183	Low
CM-33631	RHSA-2020:1334	Important	ASA-2020-064	Critical
CM-33650	RHSA-2020:3864	Moderate	ASA-2020-129	Medium
CM-37073	RHSA-2020:5009	Moderate	ASA-2020-201	High
CM-37072	RHSA-2020:5083	Moderate	ASA-2020-193	Medium
CM-37094	RHSA-2020:5011	Moderate	N/A	N/A

Additional deliveries into SSP #6:

Fix ID CM-37068: Updated tzdata:

tzdata-2020d-2.el7.noarch.rpm

tzdata-java-2020d-2.el7.noarch.rpm (AAM specific)

Security vulnerabilities resolved in CM 8.1 Kernel Service Pack #6

Fix Id	RHSA/RHBA Number	RHSA/RHBA Severity	ASA Number	ASA Overall Severity
CM-36678	RHSA-2020:4060	Important	ASA-2020-140	High
CM-36687	RHSA-2020:4276	Important	ASA-2020-146	High
CM-36888	RHSA-2020:5023	Moderate	ASA-2020-186	Medium
N/A	RHBA-2020:4180	Bug Fix Advisory	N/A	N/A

Security vulnerabilities resolved in CM 8.1 Security Service Pack #5

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2020:2344	Important	ASA-2020-079	High
RHSA-2020:2894	Important	ASA-2020-092	Medium
RHSA-2020:2432	Moderate	ASA-2020-083	Medium
RHSA-2020:3217	Moderate	ASA-2020-102	High
RHSA-2020:2663	Moderate	ASA-2020-090	High

Security vulnerabilities resolved in CM 8.1 Kernel Service Pack #5

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2020:2082	Important	ASA-2020-075	High
RHBA-2020:2355	N/A	N/A	N/A
RHSA-2020:2664	Important	ASA-2020-089	Medium
RHSA-2020:3220	Important	ASA-2020-103	High
RHBA-2020-3528	N/A	N/A	N/A

Security vulnerabilities resolved in CM 8.1 Security Service Pack #4

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2020:1190	Moderate	ASA-2020-050	High
RHSA-2020:0227	Important	ASA-2020-008	High
RHSA-2020:0540	Important	ASA-2020-006	High
RHSA-2020:1112	Moderate	ASA-2020-046	Medium
RHSA-2020:1180	Moderate	ASA-2020-035	High
RHSA-2020:1100	Moderate	ASA-2020-032	Medium
RHSA-2020:1021	Moderate	ASA-2020-033	Medium
RHSA-2020:1138	Low	N/A	N/A
RHSA-2020:1000	Moderate	ASA-2020-041	High
RHSA-2020:1131	Moderate	ASA-2020-038	High
RHSA-2020:1135	Low	ASA-2020-051	Medium
RHSA-2020:1113	Moderate	N/A	N/A
RHSA-2020:1081	Moderate	N/A	N/A
RHSA-2020:1011	Moderate	ASA-2020-037	Medium
RHSA-2020:1061	Moderate	N/A	N/A
RHSA-2020:1022	Low	ASA-2020-043	Medium
RHSA-2020:1121	Moderate	N/A	N/A
RHSA-2020:1020	Low	ASA-2020-040	Medium
RHSA-2020:1047	Moderate	ASA-2020-044	Medium
RHSA-2020:0630	Important	ASA-2020-017	Critical
RHSA-2020:0897	Important	ASA-2020-031	High

RHSA-2019:2169	Important	ASA-2019-144	High
----------------	-----------	--------------	------

Additional deliveries into SSP #4:

Updated tzdata to tzdata-2020a-1.el7.noarch.rpm (ID CM-33870)

Fix for hostname disappearing when deactivated old and activate new SSP (ID CM-31119)

Security vulnerabilities resolved in CM 8.1 Kernel Service Pack #4

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2020:0374	Important	ASA-2020-010	High
RHSA-2020:0834	Important	ASA-2020-026	High
RHSA-2020:1016	Moderate	ASA-2020-036	High

Security vulnerabilities resolved in CM 8.1 Security Service Pack #3

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2019:2964	Important	ASA-2019-227	High
RHSA-2019:3197	Important	ASA-2019-233	High
RHSA-2019:3286	Critical	ASA-2019-240	High
RHSA-2019:4190	Important	ASA-2019-247	High

Additional delivery into Security Service Pack #3 via CM-24834 fixes an issue where the time zone name displayed in the CLI could be lost on a restore and display as "n/a". This was not service impacting as the correct timezone abbreviation and offset was still shown. This is resolved with SSP #3.

Example:

n/a (MST, -0700)

vs

America/Denver (MST, -0700)

Security vulnerabilities resolved in CM 8.1 Kernel Service Pack #3

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2019:3055	Important	ASA-2019-228	High
RHSA-2019:3834	Important	ASA-2019-237	Medium
RHSA-2019:3872	Important	ASA-2019-241	High
RHSA-2019:3979	Important	ASA-2019-245	High
RHSA-2019:4106	Bug Fix Advisory	N/A	N/A

Security vulnerabilities resolved in CM 8.1 Security Service Pack #2

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2019:1619	Important	ASA-2019-121	Medium
RHSA-2019:1880	Low	ASA-2019-178	High
RHSA-2019:1884	Moderate	ASA-2019-136	High
RHSA-2019:1898	Low	ASA-2019-135	Medium
RHSA-2019:2030	Moderate	ASA-2019-191	High
RHSA-2019:2033	Low	ASA-2019-196	Low

RHSA-2019:2046	Moderate	ASA-2019-152	High
RHSA-2019:2047	Moderate	ASA-2019-147	Medium
RHSA-2019:2049	Moderate	ASA-2019-169	Medium
RHSA-2019:2057	Moderate	ASA-2019-202	Medium
RHSA-2019:2060	Moderate	ASA-2019-194	Medium
RHSA-2019:2075	Moderate	ASA-2019-188	High
RHSA-2019:2077	Low	ASA-2019-189	High
RHSA-2019:2091	Moderate	ASA-2019-203	Medium
RHSA-2019:2110	Moderate	ASA-2019-211	Medium
RHSA-2019:2118	Moderate	ASA-2019-192	Medium
RHSA-2019:2136	Moderate	ASA-2019-185	Medium
RHSA-2019:2143	Low	ASA-2019-204	Medium
RHSA-2019:2181	Low	ASA-2019-183	Low
RHSA-2019:2189	Moderate	ASA-2019-158	Medium
RHSA-2019:2197	Low	ASA-2019-154	Medium
RHSA-2019:2237	Moderate	ASA-2019-205	Medium
RHSA-2019:2304	Moderate	ASA-2019-193	Medium
RHSA-2019:2327	Moderate	ASA-2019-155	Medium
RHSA-2019:2343	Moderate	ASA-2019-197	High

Security vulnerabilities resolved in CM 8.1 Kernel Service Pack #2

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2019:1873	Important	ASA-2019-207	High
RHSA-2019:2029	Important	ASA-2019-208	High
RHSA-2019:2600	Important	ASA-2019-220	Medium
RHSA-2019:2829	Important	ASA-2019-226	High

Security vulnerabilities resolved in CM 8.1 Security Service Pack #1

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2019-0710	Important	ASA-2019-080	Critical
RHSA-2019-0368	Important	ASA-2019-054	High
RHSA-2019:0194	Moderate	ASA-2019-020	Medium
RHSA-2019:1228	Important	ASA-2019-106	High

Security vulnerabilities resolved in CM 8.1 Kernel Service Pack #1

RHSA Number	RHSA Severity	ASA Number	ASA Overall Severity
RHSA-2019:0818	Important	ASA-2019-084	High
RHSA-2019:1168	Important	ASA-2019-095	Medium
RHSA-2019:1481	Important	ASA-2019-109	High

Mitigation: N/A

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](#).