Product Correction Notice (PCN)

Issue Date:	**29-October-2024**
Supplement Date:	**3-February-2026**
Expiration Date:	**NA**
PCN Number:	**2173S**

SECTION 1 - CUSTOMER NOTICE

Products affected by this PCN:

Avaya Solutions Platform 130 R6.0.x

Note: *Avaya Converged Platform (ACP) was rebranded to Avaya Solutions Platform (ASP) in December of 2019.*

Description:

3 February 2026 – Supplement 7 of this PCN introduces Avaya Solutions Platform R6.0.0.4.0 customized zip bundle. All RHSA updates are now provided through Security Service Packs (SSPs) and tracked in PCN2179S.
Note that PLDS requires a unique PLDS ID if the same file is located under multiple Releases/Versions, therefore there will be unique PLDS IDs for ASP S8300 and ASP 130 for the ASP R6.0.0.4.0 release.

- **ASP R6.0.0.4.0 Customized KVM on RHEL 8.10 ZIP File (*update-asp-all-6.0.0.4.0-03.zip*; PLDS ID: ASP000000051)**

Note: The Initialization and Service Configuration Tool *av-asp-tools-1.5-3.el8.x86_64.rpm* referenced in Supplement 1 below is required only when updating from the R6.0.0.0 GA load. For hosts running ASP R6.0.0.**1**.0 or later releases an updated Avaya 'av-asp-tools' will be automatically installed as part of the main update procedure.

15 October 2025 – Supplement 6 of this PCN introduces Avaya Solutions Platform R6.0.0.3.0 customized zip bundle. Reference the "***Security Information"*** section of this PCN for a list of the updated and new rpm package(s) included in this bundle. This release introduces a *Security Service Pack Framework* so that all future RHSA updates can be provided by a separate Security Service Pack (SSP). A separate PCN (PCN2179S) to track the SSPs will be posted at that time.
Note that PLDS requires a unique PLDS ID if the same file is located under multiple Releases/Versions, therefore there will be unique PLDS IDs for ASP S8300 and ASP 130 for the ASP R6.0.0.3.0 release.

- **ASP R6.0.0.3.0 Customized KVM on RHEL 8.10 ZIP File (*update-asp-all-6.0.0.3.0-01.zip*; PLDS ID: ASP000000049)**

Note: The Initialization and Service Configuration Tool *av-asp-tools-1.5-3.el8.x86_64.rpm* referenced in Supplement 1 below is required only when updating from the R6.0.0.0 GA load. For hosts running ASP R6.0.0.**1**.0 or later releases an updated Avaya 'av-asp-tools' will be automatically installed as part of the main update procedure.

30 September 2025 – Supplement 5 of this PCN introduces ***Avaya Solutions Platform R5.1.x to R6.0.x Configuration Migration Utility***. Migrations are catastrophic. Several steps are required prior to a catastrophic migration, including backing up host and application-level data. The migration utilities facilitate the migration of host-level parameters and include export and import functionality. They are provided in a zip file on PLDS and will need to be extracted to the individual components. PLDS requires a unique PLDS ID if the same file is located under multiple Releases/Versions, therefore there will be unique PLDS IDs for each release within ASP S8300 and ASP 130. The zip file will extract to the following python scripts:

host_config_export_v1.py
host_config_import_v1.py

Reference the ***Application Note for ASP R5.1.x to ASP R6.0.x Configuration Migration Utility*** for detailed instructions.

- **ASP 130 R6.0.x Migration Utility v1 ZIP File**
  (*asp_migration_utility-v1.zip* **; PLDS ID:** ASP000000048**)**
- **ASP 130 R5.1.x.Migration Utility v1 ZIP File**
  (*asp_migration_utility-v1.zip* **; PLDS ID:** ASP000000032**)**

3 June 2025 – Supplement 4 of this PCN introduces Avaya Solutions Platform R6.0.0.2.0 customized zip bundle. Reference the "***Security Information"*** section of this PCN for a list of the updated rpm package(s) included in this bundle.

- **ASP R6.0.0.2.0 Customized KVM on RHEL 8.10 ZIP File**
  (*update-asp-all-6.0.0.2.0-02.zip*; PLDS ID: ASP000000045)

Note: The Initialization and Service Configuration Tool *av-asp-tools-1.5-3.el8.x86_64.rpm* referenced in Supplement 1 below is required only when updating from the R6.0.0.0 GA load. For hosts running ASP R6.0.0.**1**.0 or later releases an updated Avaya 'av-asp-tools' will be automatically installed as part of the main update procedure.

7 April 2025 – Supplement 3 of this PCN introduces Avaya Solutions Platform R6.0.0.1.1 customized zip bundle. This update does not include any additional Security related rpm package updates but does contain an Avaya custom rpm update. Reference the "***Security Information"*** section of this PCN for a list of the updated rpm package(s) included in this bundle.

- **ASP R6.0.0.1.1 Customized KVM on RHEL 8.10 ZIP File**
  (*update-asp-all-6.0.0.1.1-02.zip*; PLDS ID: ASP000000044)

Note: The Initialization and Service Configuration Tool *av-asp-tools-1.5-3.el8.x86_64.rpm* referenced in Supplement 1 below is required only when updating from the R6.0.0.0 GA load. For hosts running ASP R6.0.0.**1**.0 or later releases an updated Avaya 'av-asp-tools' will be automatically installed as part of the main update procedure.

31 March 2025 – Supplement 2 of this PCN announces the General Availability of the paravirtualized device driver required for Avaya applications that are certified to be deployed on a Windows VM on ASP 130. The only Avaya application currently certified to be deployed on a Windows VM on ASP 130 is Avaya Messaging v11.0.0.4020 Service Pack 3.
This driver CANNOT be distributed or deployed in any other scenario due to licensing requirements.

- **ASP 130 R6.0.0.1 Paravirtualized device driver (*virtio-win-1.9.39.iso*; PLDS ID: ASP000000043)**

24 February 2025 – Supplement 1 of this PCN introduces Avaya Solutions Platform R6.0.0.1 customized zip bundle, an updated av-asp-tools rpm, and a paravirtualized device driver (*for future use only*) required for Avaya applications that are certified to be deployed on a Windows VM on ASP 130. Reference the "***Security Information"*** section of this PCN for a list of updated rpm packages included in this bundle.

- **Updated ASP R6.0.0.0 Initialization and service configuration tools RPM file (*av-asp-tools-1.5-3.el8.x86_64.rpm*; PLDS ID: ASP000000041)**
- **ASP R6.0.0.1.0 Customized KVM on RHEL 8.10 ZIP File (*update-asp-all-6.0.0.1.0-04.zip*; PLDS ID: ASP000000042)**
- **ASP 130 R6.0.0.1 Paravirtualized device driver (***for future use only – see details in ASP R6.0.0.1 Release Notes***). (*virtio-win-1.9.39.iso*; PLDS ID: ASP000000043)**

29 October 2024 - This PCN introduces the general availability of Avaya Solutions Platform 130 R6.0.x software lineup and is provided as an upgrade for the ACP/ASP 130 R4.0 and R5.x releases and ASP 120 (AVP 8.1.3) release. The ASP R6.0.x program introduces a new hypervisor and updated Server hardware. In June 2024, Broadcom made the strategic decision to discontinue its Embedded OEM program. As Avaya is an Embedded OEM partner of VMware, this decision impacted the ASP 130 and S8300 solutions leading to the necessity of identifying a new hypervisor. The ASP R6.0.x program will introduce *KVM on Red Hat Enterprise Linux 8.10*. In addition to the new hypervisor, ASP R6.0.x will also introduce an updated server hardware platform with the Dell R660xs. All ASP R6.0.x solutions (ASP 130 and ASP S8300) will only ship with the new *KVM on RHEL 8.10* hypervisor. All ASP R6.0.x solutions (ASP 130 and ASP S8300) will exclusively be available with the new KVM on RHEL 8.10 hypervisor. ***ASP R6.0.x will never be offered with VMware ESXi as the hypervisor. Installation of ASP R5.x and earlier (ESXi) is not supported on the Dell R660xs.***

- **ASP 130 R6.0.x Dell® R660xs Customized KVM on RHEL 8.10 ISO image (ASP_R6_all_4.6-4.8.iso; PLDS ID: ASP000000040)**
  ASP 130 R6.0.x Dell® R660xs Customized KVM on RHEL 8.10 ISO image for installation on the ASP 130 servers. This file is ONLY applicable to ASP 130 and ASP S8300 servers and should not be used for other ASP server models (ASP 110, ASP 120, ASP 4200*). While there is one common image for ASP 130 and ASP S8300, separate PLDS IDs are provided and it imperative that customers have the correct record in PLDS for each and every instance of the server hypervisor as customers and Avaya will be subject to audits to ensure right to use royalties have been paid.*
  EASG is built into the ISO file, no separate install required. Configuration of OOBM (Out of Band Management) is part of the initial configuration and does not require a separate script. All media installation of ASP R6.0.x will be done via USB and the kickstart file is included in the ISO.

NOTE: Please refer to Avaya Solutions Platform R6.0.x official documentation, including Release Notes, for detailed upgrade supportability and installation procedures.

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 the ASP R6.0.x release. In the event of an escalation to Avaya Services, Avaya may require an update to the latest files listed in the **Description** section of this PCN in order to isolate an issue.
The risk if this PCN is not installed:	Important fixes will not be installed.
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?	Yes. ASP 130 environment software and firmware will be installed, upgraded, reinstalled and/or reconfigured. This will cause disruptions during deployment and is to be completed during a customer approved maintenance window.
Installation of this PCN is required by:	Customer or Avaya Authorized Service Provider. This upgrade is customer installable.
Release notes and workarounds are located:	**Note: All ASP related files and documents can be found under the "Avaya Solutions Platform" product name on the Avaya Support site. For PLDS, all related files can be found under the "Solutions Platform 1XX" application name.** The **Avaya Solutions Platform 130 Series Release Notes** contain the specific software updates included in the release and can be obtained by performing the following steps from a browser: 1. Go to http://support.avaya.com then enter your **Username** and **Password** and select **LOG IN.** 2. Select **Product Documents** 3. Mouse over **Search Product** at the top of the page. 4. Begin to type **Solutions Platform** and when **Avaya Solutions Platform** appears as a selection below, select it. 5. Select "**ASP 130 6.0.x"** from the **Select Release** pull down menu to the right. 6. Under **Select Content Type**, select **Release & Software Update Notes**. 7. Select the document titled "**Avaya Solutions Platform 130 6.0.x Release Notes**".
What materials are required to	This PCN is being issued as a customer installable PCN. The specified Avaya Solutions Platform files are required. To obtain the update files refer to the **How do I order this PCN** section of this PCN.

implement this PCN (If PCN can be customer installed):

If upgrading to ASP 130 R6.0.x the following order codes are required depending on the current platform/release.

Order Code	Description
4434562	ASP 120 AVP UPG ASP 130 R6 RHEL LIC
4434563	ASP 130 R4 UPG ASP 130 R6 RHEL LIC
4434495	ASP 130 R5 UPG ASP 130 R6 RHEL LIC

Ordering any of the above three codes will trigger the following 4434496 ASP 130 R6 RHEL LIC (not orderable, this is an entitlement) which will be present in the customer record.

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

The specified Avaya Solutions Platform files can be downloaded by performing the following steps from a browser:

1. Go to http://support.avaya.com then enter your **Username** and **Password** and select **LOG IN.**
2. Mouse over **Search Product** at the top of the page.
3. Begin to type **Solutions Platform** and when **Avaya Solutions Platform** appears as a selection below, select it.
4. Select **ASP 130 6.0.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 Solutions Platform ASP 130 Series Release 6.0.**
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 **Solutions Platform 1XX** in the **Product Line** search field to display frequently downloaded Avaya Solutions Platform 130 software.
2. All Avaya Solutions Platform 130 software downloads are available on PLDS. In the PLDS **View Downloads** section under the **Search by Download** tab, select **Solutions Platform 1XX** in the **Application** search field and **6.0** in the **Version** search field to display all available **Solutions Platform 1XX** 6.0.x downloads.

The MD5, SHA1 and SHA256 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 the Avaya Solutions Platform files detailed in this PCN can be found in the following documents.

Title	Description
Avaya Solutions Platform 130/S8300 Overview and Specification	Describes the key features of Avaya Solutions Platform.
Installing, Maintaining, and Troubleshooting Avaya Solutions Platform S8300	Describes how to install, maintain, and troubleshoot Avaya Solutions Platform S8300.
Installing the Avaya Solutions Platform 130 Series	Describes how to install Avaya Solutions Platform 13 Describes how to install Avaya Solutions Platform 130 Series 6.0.x.0 Series 6.0.x.
Maintaining and Troubleshooting the Avaya Solutions Platform 130 Series 6.0.x	Describes procedures to maintain and troubleshoot Avaya Solutions Platform 130 Series 6.0.x.
Avaya Solutions Platform S8300 6.0.x Release Notes	Release Notes.
Avaya Solutions Platform 130 6.0.x Release Notes	Release Notes.
PCN2174Su - Avaya Solutions Platform S8300 6.0.x	Product Correction Notice (PCN) introducing the ASP S8300 R6.0.x software and subsequent Service Packs.
PCN2180Su - Avaya Solutions Platform S8300 6.0 SSP	Product Correction Notice (PCN) introducing the ASP S8300 R6.0.x Security Service Packs (SSPs) available beginning with ASP R6.0.0.3.0 and later.
PCN2173Su - Avaya Solutions Platform 130 6.0.x	Product Correction Notice (PCN) introducing the ASP 130 R6.0.x software and subsequent Service Packs.
PCN2179Su - Avaya Solutions Platform 130 6.0 SSP	Product Correction Notice (PCN) introducing the ASP 130 R6.0.x Security Service Packs (SSPs) available beginning with ASP R6.0.0.3.0 and later.
Avaya Solutions Platform R6.0.x Security Service Pack Installation Application Note	Instructions for installing ASP Security Service Packs (SSPs).
ASP 130 R6.0.0.4.0 and Later VLAN & VLAN TRUNKING CONFIGURATION GUIDE	This application note provides guidance for configuring VLANs and enabling VLAN trunking on ASP R6.0.0.4.0 (KVM on RHEL 8.10) or later release. It is intended for system administrators and technical users responsible for deploying and managing virtual infrastructure on Avaya Solutions Platform (ASP) compute servers.

ASP 130 R6.0.0.3.0 and Earlier VLAN & VLAN TRUNKING CONFIGURATION GUIDE	This application note provides guidance for configuring VLANs and enabling VLAN trunking on ASP R6.0.0.3.0 (KVM on RHEL 8.10) or earlier release. It is intended for system administrators and technical users responsible for deploying and managing virtual infrastructure on Avaya Solutions Platform (ASP) compute servers.
Port Matrix for ASP S8300	This document provides a list of interfaces, TCP and UDP ports that hardware components and applications use for intra-connections and for inter-connections with external applications or devices.
Port Matrix for ASP 130	This document provides a list of interfaces, TCP and UDP ports that hardware components and applications use for intra-connections and for inter-connections with external applications or devices
Policies for technical support of the Avaya Solutions Platform (ASP) 130 and S8300E R6.0.x	This document and statements related to support are only with respect to Avaya Services support of the software and hardware of the Avaya Solutions Platform (ASP) 130 server and S8300E server based on supported and tested configurations.
Avaya Solutions Platform 130 Series iDRAC9 Best Practices	Describes the best practices of using the Integrated Dell Remote Access Controller (iDRAC).
PSN027113u - Avaya Solutions Platform 100 Series Dell® R660xs Avaya Certified BIOS/Firmware Update, Version 2	Always check for a newer version of Avaya certified BIOS/Firmware. New PSNs are published for each new release.
PSN027112u - Avaya Solutions Platform 100 Series Dell® R640 Avaya Certified BIOS/Firmware Update, Version 16	Always check for a newer version of Avaya certified BIOS/Firmware. New PSNs are published for each new release.
Avaya Solutions Platform 130 & S8300 Series Updating to R6.0.0.x.0 documents listed below	Follow the steps outlined in the appropriate document(s) when planning and conducting updates to ASP R6.0.x KVM on RHEL 8.10 hosts running on ASP 130 & S8300E servers using the Avaya certified and approved files. Always check support.avaya.com for new documents as new Service Packs are released.
Avaya Solutions Platform 130 & S8300 Series Updating to R6.0.0.4.0 (RHEL 8.10) from R6.0.0.3.0 (RHEL 8.10)	NOTE: Upgrades to R6.0.0.4.0 and later R6.0.0.x.0 service packs require a step upgrade to R6.0.0.3.0 first.

Avaya Solutions Platform 130 & S8300 Series Updating to R6.0.0.3.0 (RHEL 8.10) from R6.0.x (RHEL 8.10)	
Avaya Solutions Platform 130 & S8300 Series Updating to R6.0.0.2.0 (RHEL 8.10) from R6.0.x (RHEL 8.10)	
Avaya Solutions Platform 130 & S8300 Series Updating to R6.0.0.1.1 (RHEL 8.10) from R6.0.x (RHEL 8.10)	
Avaya Solutions Platform 130 & S8300 Series Updating to R6.0.0.1 (RHEL 8.10) from R6.0.x (RHEL 8.10)	
Documents for migrating from AVP and older ASP R5.x EOMS releases can be found on support.avaya.com.	

SECTION 1A – SOFTWARE INFORMATION

Note: A system/software backup is required before upgrading to Avaya Solutions Platform 130 R6.0.x

How to verify the installation of the Service Pack has been successful:	Verification of application/installation of the files listed in the **Description** section of this PCN are covered in the documents referenced in the **Finding the installation instructions (If PCN can be customer installed)** section of this PCN.
What you should do if the Service Pack installation fails?	Steps for troubleshooting failure on application/installation of the files listed in **Description** section of this PCN are covered in the documents referenced in the **Finding the installation instructions (If PCN can be customer installed)** section of this PCN.
How to remove the Service Pack if malfunction of your system occurs:	Steps for rollback/removal (if possible) of the files listed in **Description** section of this PCN are covered in the documents referenced in the **Finding the installation instructions (If PCN can be customer installed)** section of this PCN.

SECTION 1B – SECURITY INFORMATION

Are there any security risks involved?	Please see the "Security Statement" section in the ASP 130 R6.0.x release notes located at support.avaya.com for details.
Avaya Security	NA

Vulnerability Classification:	
Mitigation:	Solutions for vulnerabilities are delivered by Avaya's Third-Party vendors (e.g., Red Hat, Dell, etc.).

All RHSA updates are now provided through Security Service Packs (SSPs) and tracked in PCN2179S.

NOTE: When a new ASP R6.0.x bundle is created (**only through R6.0.0.3.0**), all RHSA fixes that are available from Red Hat at that point in time are included. New RHSAs/updated packages released from Red Hat after that point in time will be included in the next update bundle.
Avaya picks up fixes from official RHEL repositories only. Even though a fix may be available, RHEL may take time to incorporate it into their base, so it is important to look at RHEL CVE dates and not dates from any other source.

If a scanning tool is flagging a vulnerability, it is important to see when the RPM fix was released by Red Hat.
If the fix was released after the build date of the ASP 130 R6.0.x update bundle (typically GA date minus 3 weeks), then it will be included in a future ASP R6.0.x update bundle.
If the fix was released by Red Hat prior to the build date of the ASP 130 R6.0.x update bundle, open a Service Request with Avaya to have it reviewed.

A security scan that only considers the Red Hat version may incorrectly report that an older release of RHEL is unsupported. If a scan reports a RHEL vulnerability then please check the actual RPM version on the system to confirm that it is not a false positive. If it is not a false positive then perform the following:

- Please check when the RPM fix was released by RHEL. If the fix was released by RHEL between the build date of the ASP bundle and the GA date, then the fix was not picked up as part of the build and will be available in a subsequent update bundle.
- If the fix was released by RHEL prior to the build date of the ASP bundle then open an SR with Avaya to have it reviewed.

Update bundles are cumulative.
This section contains detailed lists of updated RHEL rpms related to security updates and Avaya custom rpm updates.

ASP 6.0.0.3.0 October 2025 update bundle (build date Sept. 3, 2025) includes the following rpm updates and new rpms:

aide-0.16-15.el8_10.2.x86_64.rpm	libvirt-daemon-driver-storage-mpath-8.0.0-23.4.module+el8.10.0+23205+d8da55c1.x86_64.rpm
bind-libs-9.11.36-16.el8_10.4.x86_64.rpm	libvirt-daemon-driver-storage-rbd-8.0.0-23.4.module+el8.10.0+23205+d8da55c1.x86_64.rpm
bind-libs-lite-9.11.36-16.el8_10.4.x86_64.rpm	libvirt-daemon-driver-storage-scsi-8.0.0-23.4.module+el8.10.0+23205+d8da55c1.x86_64.rpm
bind-license-9.11.36-16.el8_10.4.noarch.rpm	libvirt-libs-8.0.0-23.4.module+el8.10.0+23205+d8da55c1.x86_64.rpm
bind-utils-9.11.36-16.el8_10.4.x86_64.rpm	libxml2-2.9.7-21.el8_10.3.x86_64.rpm
bpftool-4.18.0-553.72.1.el8_10.x86_64.rpm	libxslt-1.1.32-6.2.el8_10.x86_64.rpm
emacs-filesystem-26.1-15.el8_10.noarch.rpm	lz4-libs-1.8.3-5.el8_10.x86_64.rpm
fstrm-0.6.1-3.el8.x86_64.rpm	microcode_ctl-20250512-1.el8_10.x86_64.rpm
gdk-pixbuf2-2.36.12-7.el8_10.x86_64.rpm	pam-1.3.1-38.el8_10.x86_64.rpm
glib2-2.56.4-166.el8_10.x86_64.rpm	perl-Errno-1.28-423.el8_10.x86_64.rpm
glibc-2.28-251.el8_10.25.x86_64.rpm	perl-interpreter-5.26.3-423.el8_10.x86_64.rpm
glibc-all-langpacks-2.28-251.el8_10.25.x86_64.rpm	perl-IO-1.38-423.el8_10.x86_64.rpm
glibc-common-2.28-251.el8_10.25.x86_64.rpm	perl-libs-5.26.3-423.el8_10.x86_64.rpm
glibc-gconv-extra-2.28-251.el8_10.25.x86_64.rpm	perl-macros-5.26.3-423.el8_10.x86_64.rpm
jq-1.6-11.el8_10.x86_64.rpm	platform-python-3.6.8-71.el8_10.x86_64.rpm
kernel-4.18.0-553.72.1.el8_10.x86_64.rpm	platform-python-setuptools-39.2.0-9.el8_10.noarch.rpm
kernel-core-4.18.0-553.72.1.el8_10.x86_64.rpm	protobuf-c-1.3.0-8.el8.x86_64.rpm
kernel-modules-4.18.0-553.72.1.el8_10.x86_64.rpm	
kernel-tools-4.18.0-553.72.1.el8_10.x86_64.rpm	
kernel-tools-libs-4.18.0-553.72.1.el8_10.x86_64.rpm	

krb5-libs-1.18.2-32.el8_10.x86_64.rpm	python3-bind-9.11.36-16.el8_10.4.noarch.rpm
libarchive-3.3.3-6.el8_10.x86_64.rpm	python3-cryptography-3.2.1-8.el8_10.x86_64.rpm
libblockdev-2.28-7.el8_10.x86_64.rpm	python3-libs-3.6.8-71.el8_10.x86_64.rpm
libblockdev-crypto-2.28-7.el8_10.x86_64.rpm	python3-libxml2-2.9.7-21.el8_10.3.x86_64.rpm
libblockdev-fs-2.28-7.el8_10.x86_64.rpm	python3-perf-4.18.0-553.72.1.el8_10.x86_64.rpm
libblockdev-loop-2.28-7.el8_10.x86_64.rpm	python3-requests-2.20.0-6.el8_10.noarch.rpm
libblockdev-lvm-2.28-7.el8_10.x86_64.rpm	python3-setuptools-39.2.0-9.el8_10.noarch.rpm
libblockdev-mdraid-2.28-7.el8_10.x86_64.rpm	python3-setuptools-wheel-39.2.0-9.el8_10.noarch.rpm
libblockdev-part-2.28-7.el8_10.x86_64.rpm	python3-unbound-1.16.2-5.9.el8_10.x86_64.rpm
libblockdev-swap-2.28-7.el8_10.x86_64.rpm	qemu-guest-agent-6.2.0-
libblockdev-utils-2.28-7.el8_10.x86_64.rpm	53.module+el8.10.0+23081+c18b1ee3.4.x86_64.rpm
libsoup-2.62.3-9.el8_10.x86_64.rpm	qemu-img-6.2.0-53.module+el8.10.0+23081+c18b1ee3.4.x86_64.rpm
libtpms-0.9.1-	qemu-kvm-6.2.0-53.module+el8.10.0+23081+c18b1ee3.4.x86_64.rpm
3.20211126git1ff6fe1f43.module+el8.10.0+23348+204cfc70.x86_64.rpm	qemu-kvm-block-curl-6.2.0-
libudisks2-2.9.0-16.el8_10.1.x86_64.rpm	53.module+el8.10.0+23081+c18b1ee3.4.x86_64.rpm
libvirt-8.0.0-23.4.module+el8.10.0+23205+d8da55c1.x86_64.rpm	qemu-kvm-block-gluster-6.2.0-
libvirt-client-8.0.0-23.4.module+el8.10.0+23205+d8da55c1.x86_64.rpm	53.module+el8.10.0+23081+c18b1ee3.4.x86_64.rpm
libvirt-daemon-8.0.0-	qemu-kvm-block-iscsi-6.2.0-
23.4.module+el8.10.0+23205+d8da55c1.x86_64.rpm	53.module+el8.10.0+23081+c18b1ee3.4.x86_64.rpm
libvirt-daemon-config-network-8.0.0-	qemu-kvm-block-rbd-6.2.0-
23.4.module+el8.10.0+23205+d8da55c1.x86_64.rpm	53.module+el8.10.0+23081+c18b1ee3.4.x86_64.rpm
libvirt-daemon-config-nwfilter-8.0.0-	qemu-kvm-block-ssh-6.2.0-
23.4.module+el8.10.0+23205+d8da55c1.x86_64.rpm	53.module+el8.10.0+23081+c18b1ee3.4.x86_64.rpm
libvirt-daemon-driver-interface-8.0.0-	qemu-kvm-common-6.2.0-
23.4.module+el8.10.0+23205+d8da55c1.x86_64.rpm	53.module+el8.10.0+23081+c18b1ee3.4.x86_64.rpm
libvirt-daemon-driver-network-8.0.0-	qemu-kvm-core-6.2.0-53.module+el8.10.0+23081+c18b1ee3.4.x86_64.rpm
23.4.module+el8.10.0+23205+d8da55c1.x86_64.rpm	qemu-kvm-docs-6.2.0-
libvirt-daemon-driver-nodedev-8.0.0-	53.module+el8.10.0+23081+c18b1ee3.4.x86_64.rpm
23.4.module+el8.10.0+23205+d8da55c1.x86_64.rpm	qemu-kvm-hw-usbredir-6.2.0-
libvirt-daemon-driver-nwfilter-8.0.0-	53.module+el8.10.0+23081+c18b1ee3.4.x86_64.rpm
23.4.module+el8.10.0+23205+d8da55c1.x86_64.rpm	qemu-kvm-ui-opengl-6.2.0-
libvirt-daemon-driver-qemu-8.0.0-	53.module+el8.10.0+23081+c18b1ee3.4.x86_64.rpm
23.4.module+el8.10.0+23205+d8da55c1.x86_64.rpm	qemu-kvm-ui-spice-6.2.0-
libvirt-daemon-driver-secret-8.0.0-	53.module+el8.10.0+23081+c18b1ee3.4.x86_64.rpm
23.4.module+el8.10.0+23205+d8da55c1.x86_64.rpm	rsync-3.1.3-23.el8_10.x86_64.rpm
libvirt-daemon-driver-storage-8.0.0-	sqlite-libs-3.26.0-20.el8_10.x86_64.rpm
23.4.module+el8.10.0+23205+d8da55c1.x86_64.rpm	sudo-1.9.5p2-1.el8_10.1.x86_64.rpm
libvirt-daemon-driver-storage-core-8.0.0-	udisks2-2.9.0-16.el8_10.1.x86_64.rpm
23.4.module+el8.10.0+23205+d8da55c1.x86_64.rpm	udisks2-iscsi-2.9.0-16.el8_10.1.x86_64.rpm
libvirt-daemon-driver-storage-disk-8.0.0-	udisks2-lvm2-2.9.0-16.el8_10.1.x86_64.rpm
23.4.module+el8.10.0+23205+d8da55c1.x86_64.rpm	unbound-libs-1.16.2-5.9.el8_10.x86_64.rpm
libvirt-daemon-driver-storage-gluster-8.0.0-	
23.4.module+el8.10.0+23205+d8da55c1.x86_64.rpm	
libvirt-daemon-driver-storage-iscsi-8.0.0-	
23.4.module+el8.10.0+23205+d8da55c1.x86_64.rpm	
libvirt-daemon-driver-storage-iscsi-direct-8.0.0-	
23.4.module+el8.10.0+23205+d8da55c1.x86_64.rpm	
libvirt-daemon-driver-storage-logical-8.0.0-	
23.4.module+el8.10.0+23205+d8da55c1.x86_64.rpm	

Security vulnerabilities resolved in ASP R6.0.0.3.0 October 2025 update bundle (build date Sept. 3, 2025)

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
pam	RHSA-2025:10027	CVE-2025-6020	Important
sudo	RHSA-2025:10110	CVE-2025-32462	Important
platform-python python3-libs	RHSA-2025:10128	CVE-2024-12718 CVE-2025-4138 CVE-2025-4330 CVE-2025-4435 CVE-2025-4517	Important
jq	RHSA-2025:10618	CVE-2024-23337 CVE-2025-48060	Moderate

Bpftool Kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:10669	CVE-2022-49111 CVE-2022-49136 CVE-2022-49846	Important
libxml2 python3-libxml2	RHSA-2025:10698	CVE-2025-49794 CVE-2025-49796 CVE-2025-6021	Important
microcode_ctl	RHSA-2025:10991	CVE-2024-28956 CVE-2024-43420 CVE-2024-45332 CVE-2025-20012 CVE-2025-20623 CVE-2025-24495	Moderate
emacs-filesystem	RHSA-2025:11030	CVE-2024-53920	Moderate
lz4-libs	RHSA-2025:11035	CVE-2019-17543	Moderate
platform-python-setuptools python3-setuptools python3-setuptools-wheel	RHSA-2025:11036	CVE-2025-47273	Moderate
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:11298	CVE-2022-49058 CVE-2022-49788 CVE-2024-57980 CVE-2024-58002 CVE-2025-21991 CVE-2025-22004 CVE-2025-23150 CVE-2025-37738	Moderate
glib2	RHSA-2025:11327	CVE-2024-34397 CVE-2024-52533 CVE-2025-4373	Moderate
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:11455	CVE-2024-50154 CVE-2025-38086	Moderate
perl-Errno perl-IO perl-interpreter perl-libs perl-macros	RHSA-2025:11805	CVE-2025-40909	Moderate
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:11850	CVE-2022-49977 CVE-2025-21905 CVE-2025-21919	Moderate
python3-unbound unbound-libs	RHSA-2025:11884	CVE-2025-5994	Important
sqlite-libs	RHSA-2025:12010	CVE-2025-6965	Important
libxml2 python3-libxml2	RHSA-2025:12450	CVE-2025-7425	Important

libtpms libvirt libvirt-client libvirt-daemon libvirt-daemon-config-network libvirt-daemon-config-nwfilter libvirt-daemon-driver-interface libvirt-daemon-driver-network libvirt-daemon-driver-nodedev libvirt-daemon-driver-nwfilter libvirt-daemon-driver-qemu libvirt-daemon-driver-secret libvirt-daemon-driver-storage libvirt-daemon-driver-storage-core libvirt-daemon-driver-storage-disk libvirt-daemon-driver-storage-gluster libvirt-daemon-driver-storage-iscsi libvirt-daemon-driver-storage-iscsi-direct libvirt-daemon-driver-storage-logical libvirt-daemon-driver-storage-mpath libvirt-daemon-driver-storage-rbd libvirt-daemon-driver-storage-scsi libvirt-libs qemu-guest-agent qemu-img qemu-kvm qemu-kvm-block-curl qemu-kvm-block-gluster qemu-kvm-block-iscsi qemu-kvm-block-rbd qemu-kvm-block-ssh qemu-kvm-common qemu-kvm-core qemu-kvm-docs qemu-kvm-hw-usbredir qemu-kvm-ui-opengl qemu-kvm-ui-spice	RHSA-2025:12527	CVE-2025-49133	Moderate
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:12752	CVE-2022-50020 CVE-2025-21928 CVE-2025-22020 CVE-2025-37890 CVE-2025-38052 CVE-2025-38079	Important
glibc glibc-all-langpacks glibc-common glibc-gconv-extra	RHSA-2025:12980	CVE-2025-8058	Moderate
libxml2 python3-libxml2	RHSA-2025:13203	CVE-2025-32415	Moderate
python3-requests	RHSA-2025:13234	CVE-2024-47081	Moderate
gdk-pixbuf2	RHSA-2025:13315	CVE-2025-7345	Moderate

bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:13589	CVE-2021-47670 CVE-2024-56644 CVE-2025-21727 CVE-2025-21759 CVE-2025-38085 CVE-2025-38159	Moderate
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:13960	CVE-2022-50269 CVE-2022-50369 CVE-2025-22097 CVE-2025-37914 CVE-2025-38250 CVE-2025-38380	Important
libarchive	RHSA-2025:14135	CVE-2025-5914	Important
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:14438	CVE-2025-22058 CVE-2025-38200	Moderate
python3-cryptography	RHSA-2025:14553	CVE-2023-49083	Moderate
pam	RHSA-2025:14557	CVE-2025-6020 CVE-2025-8941	Important
platform-python python3-libs	RHSA-2025:14560	CVE-2025-8194	Moderate
aide	RHSA-2025:14573	CVE-2025-54389	Important
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:15008	CVE-2025-38211 CVE-2025-38332 CVE-2025-38464 CVE-2025-38477	Moderate
libudisks2 udisks2 udisks2-iscsi udisks2-lvm2	RHSA-2025:15017	CVE-2025-8067	Important
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:8056	CVE-2024-40906 CVE-2024-44970 CVE-2025-21756	Important
libsoup	RHSA-2025:8132	CVE-2025-2784 CVE-2025-32049 CVE-2025-32914 CVE-2025-4948	Important
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:8246	CVE-2024-43842 CVE-2025-38234	Moderate
rsync	RHSA-2025:8395	CVE-2016-9840	Low

krb5-libs	RHSA-2025:8411	CVE-2025-3576	Moderate
libxslt	RHSA-2025:8676	CVE-2023-40403	Moderate
glibc glibc-all-langpacks glibc-common glibc-gconv-extra	RHSA-2025:8686	CVE-2025-4802	Moderate
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:8743	CVE-2022-49395	Moderate
libxml2 python3-libxml2	RHSA-2025:8958	CVE-2025-32414	Moderate
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:9580	CVE-2022-48919 CVE-2024-50301 CVE-2024-53064 CVE-2025-21764 CVE-2025-38053	Moderate
libblockdev libblockdev-crypto libblockdev-fs libblockdev-loop libblockdev-lvm libblockdev-mdraid libblockdev-part libblockdev-swap libblockdev-utils	RHSA-2025:9878	CVE-2025-6019	Important

ASP 6.0.0.2.0 June 2025 update bundle (build date May 20, 2025) includes the following rpm updates:

adcli-0.9.2-1.el8.x86_64.rpm	libstdc8.5.0-23.el8_10.x86_64.rpm
audispd-plugins-3.1.2-1.el8.x86_64.rpm	libtasn1-4.13-5.el8_10.x86_64.rpm
av-asp-tools-1.7-1.el8.x86_64.rpm	libxml2-2.9.7-19.el8_10.x86_64.rpm
av-s8300-watchd-1.2-1.el8.x86_64.rpm	libxslt-1.1.32-6.1.el8_10.x86_64.rpm
bind-export-libs-9.11.36-16.el8_10.4.x86_64.rpm	mailx-12.5-29.el8.x86_64.rpm
binutils-2.30-125.el8_10.x86_64.rpm	NetworkManager-1.40.16-18.el8_10.x86_64.rpm
bpftool-4.18.0-553.52.1.el8_10.x86_64.rpm	NetworkManager-libnm-1.40.16-18.el8_10.x86_64.rpm
bzip2-1.0.6-28.el8_10.x86_64.rpm	NetworkManager-team-1.40.16-18.el8_10.x86_64.rpm
bzip2-libs-1.0.6-28.el8_10.x86_64.rpm	NetworkManager-tui-1.40.16-18.el8_10.x86_64.rpm
edk2-ovmf-20220126gitbb1bba3d77-13.el8_10.4.noarch.rpm	openldap-clients-2.4.46-19.el8_10.x86_64.rpm
emacs-filesystem-26.1-13.el8_10.noarch.rpm	opensc-0.20.0-8.el8_9.x86_64.rpm
expat-2.2.5-17.el8_10.x86_64.rpm	pam-1.3.1-36.el8_10.x86_64.rpm
fapolicyd-1.3.2-1.el8.x86_64.rpm	pcsc-lite-1.9.5-1.el8.x86_64.rpm
fapolicyd-selinux-1.3.2-1.el8.noarch.rpm	pcsc-lite-ccid-1.4.29-5.1.el8_4.x86_64.rpm
freetype-2.9.1-10.el8_10.x86_64.rpm	pcsc-lite-libs-1.9.5-1.el8.x86_64.rpm
glibc-2.28-251.el8_10.16.x86_64.rpm	perccli-007.2616.0000.0000-1.noarch.rpm
glibc-all-langpacks-2.28-251.el8_10.16.x86_64.rpm	platform-python-3.6.8-69.el8_10.x86_64.rpm
glibc-common-2.28-251.el8_10.16.x86_64.rpm	postfix-3.5.8-7.el8.x86_64.rpm
glibc-gconv-extra-2.28-251.el8_10.16.x86_64.rpm	protobuf-3.5.0-15.el8.x86_64.rpm
gnutls-3.6.16-8.el8_10.3.x86_64.rpm	python3-libs-3.6.8-69.el8_10.x86_64.rpm
gnutls-dane-3.6.16-8.el8_10.3.x86_64.rpm	python3-libxml2-2.9.7-19.el8_10.x86_64.rpm
gnutls-utils-3.6.16-8.el8_10.3.x86_64.rpm	python3-perf-4.18.0-553.52.1.el8_10.x86_64.rpm
grub2-common-2.02-162.el8_10.noarch.rpm	python3-requests-2.20.0-5.el8_10.noarch.rpm

grub2-efi-x64-2.02-162.el8_10.x86_64.rpm	python3-sss-2.9.4-4.el8_10.x86_64.rpm
grub2-pc-2.02-162.el8_10.x86_64.rpm	python3-unbound-1.16.2-5.8.el8_10.x86_64.rpm
grub2-pc-modules-2.02-162.el8_10.noarch.rpm	rng-tools-6.16-1.el8.x86_64.rpm
grub2-tools-2.02-162.el8_10.x86_64.rpm	rpm-plugin-fapolicyd-4.14.3-31.el8.x86_64.rpm
grub2-tools-efi-2.02-162.el8_10.x86_64.rpm	rsync-3.1.3-21.el8_10.x86_64.rpm
grub2-tools-extra-2.02-162.el8_10.x86_64.rpm	sssd-dbus-2.9.4-4.el8_10.x86_64.rpm
grub2-tools-minimal-2.02-162.el8_10.x86_64.rpm	sssd-tools-2.9.4-4.el8_10.x86_64.rpm
gstreamer1-plugins-base-1.16.1-5.el8_10.x86_64.rpm	sysstat-11.7.3-13.el8_10.x86_64.rpm
kernel-4.18.0-553.52.1.el8_10.x86_64.rpm	systemd-239-82.el8_10.5.x86_64.rpm
kernel-core-4.18.0-553.52.1.el8_10.x86_64.rpm	systemd-container-239-82.el8_10.5.x86_64.rpm
kernel-modules-4.18.0-553.52.1.el8_10.x86_64.rpm	systemd-libs-239-82.el8_10.5.x86_64.rpm
kernel-tools-4.18.0-553.52.1.el8_10.x86_64.rpm	systemd-pam-239-82.el8_10.5.x86_64.rpm
kernel-tools-libs-4.18.0-553.52.1.el8_10.x86_64.rpm	systemd-udev-239-82.el8_10.5.x86_64.rpm
krb5-libs-1.18.2-31.el8_10.x86_64.rpm	tuned-2.22.1-5.el8_10.noarch.rpm
libgcc-8.5.0-23.el8_10.x86_64.rpm	tzdata-2025b-1.el8.noarch.rpm
libgomp-8.5.0-23.el8_10.x86_64.rpm	unbound-libs-1.16.2-5.8.el8_10.x86_64.rpm
libjpeg-turbo-1.5.3-14.el8_10.x86_64.rpm	usbguard-1.0.0-13.el8.x86_64.rpm
libqb-1.0.3-13.el8_7.x86_64.rpm	usbguard-selinux-1.0.0-13.el8.noarch.rpm
libsoup-2.62.3-8.el8_10.x86_64.rpm	

Security vulnerabilities resolved in ASP R6.0.0.2.0 June 2025 update bundle (build date May 20, 2025)

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
tzdata	RHBA-2025:3394	NA	bugfix
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:1068	CVE-2024-26935 CVE-2024-50275	Moderate
bpftool Kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:1266	CVE-2024-53104	Important
libgcc libgomp libstdc++	RHSA-2025:1301	CVE-2020-11023	Moderate
libxml2 python3-libxml2	RHSA-2025:1517	CVE-2022-49043	Moderate
bind-export-libs	RHSA-2025:1675	CVE-2024-11187	Important
emacs-filesystem	RHSA-2025:1917	CVE-2025-1244	Important
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:2473	CVE-2024-50302 CVE-2024-53197 CVE-2024-57807 CVE-2024-57979	Important

rsync	RHSA-2025:2600	CVE-2024-12087 CVE-2024-12088 CVE-2024-12747	Moderate
libxml2 python3-libxml2	RHSA-2025:2686	CVE-2024-56171 CVE-2025-24928	Important
krb5-libs	RHSA-2025:2722	CVE-2025-24528	Moderate
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:3026	CVE-2023-52922	Important
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:3260	CVE-2025-21785	Important
grub2-common grub2-efi-x64 grub2-pc grub2-pc-modules grub2-tools grub2-tools-extra grub2-tools-minimal	RHSA-2025:3367	CVE-2025-0624	Important
freetype	RHSA-2025:3421	CVE-2025-27363	Important
libxslt	RHSA-2025:3615	CVE-2024-55549 CVE-2025-24855	Important
glibc glibc-all-langpacks glibc-common glibc-gconv-extra	RHSA-2025:3828	CVE-2025-0395	Moderate
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:3893	CVE-2024-53150 CVE-2024-53241	Moderate
expat	RHSA-2025:3913	CVE-2024-8176	Moderate
libtasn1	RHSA-2025:4049	CVE-2024-12133	Moderate
gnutls gnutls-dane gnutls-utils	RHSA-2025:4051	CVE-2024-12243	Moderate

libsoup	RHSA-2025:4560	CVE-2025-32050 CVE-2025-32052 CVE-2025-32053 CVE-2025-32906 CVE-2025-32911 CVE-2025-32913 CVE-2025-46420 CVE-2025-46421	Important
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:7531	CVE-2022-49011 CVE-2024-53141	Important
libjpeg-turbo	RHSA-2025:7540	CVE-2020-13790	Moderate

ASP 6.0.0.1.1 April 2025 update bundle includes the following rpm updates:

av-asp-tools-1.6-2.el8.x86_64.rpm.	

ASP 6.0.0.1 February 2025 update bundle (build date Feb, 3, 2025) includes the following rpm updates:

audispd-plugins-3.1.2-1.el8.x86_64.rpm	NetworkManager-tui-1.40.16-18.el8_10.x86_64.rpm
av-asp-tools-1.5-3.el8.x86_64.rpm	opensc-0.20.0-8.el8_9.x86_64.rpm
av-s8300-watchd-1.1-1.el8.x86_64.rpm	pam-1.3.1-36.el8_10.x86_64.rpm
binutils-2.30-125.el8_10.x86_64.rpm	pcsc-lite-1.9.5-1.el8.x86_64.rpm
bpftool-4.18.0-553.34.1.el8_10.x86_64.rpm	pcsc-lite-ccid-1.4.29-5.1.el8_4.x86_64.rpm
bzip2-1.0.6-28.el8_10.x86_64.rpm	pcsc-lite-libs-1.9.5-1.el8.x86_64.rpm
bzip2-libs-1.0.6-28.el8_10.x86_64.rpm	perccli-007.2616.0000.0000-1.noarch.rpm
edk2-ovmf-20220126gitbb1bba3d77-13.el8_10.4.noarch.rpm	platform-python-3.6.8-69.el8_10.x86_64.rpm
expat-2.2.5-16.el8_10.x86_64.rpm	postfix-3.5.8-7.el8.x86_64.rpm
fapolicyd-1.3.2-1.el8.x86_64.rpm	protobuf-3.5.0-15.el8.x86_64.rpm
fapolicyd-selinux-1.3.2-1.el8.noarch.rpm	python3-libs-3.6.8-69.el8_10.x86_64.rpm
gstreamer1-plugins-base-1.16.1-5.el8_10.x86_64.rpm	python3-perf-4.18.0-553.34.1.el8_10.x86_64.rpm
kernel-4.18.0-553.34.1.el8_10.x86_64.rpm	python3-requests-2.20.0-5.el8_10.noarch.rpm
kernel-core-4.18.0-553.34.1.el8_10.x86_64.rpm	python3-unbound-1.16.2-5.8.el8_10.x86_64.rpm
kernel-modules-4.18.0-553.34.1.el8_10.x86_64.rpm	rng-tools-6.16-1.el8.x86_64.rpm
kernel-tools-4.18.0-553.34.1.el8_10.x86_64.rpm	rpm-plugin-fapolicyd-4.14.3-31.el8.x86_64.rpm
kernel-tools-libs-4.18.0-553.34.1.el8_10.x86_64.rpm	rsync-3.1.3-20.el8_10.x86_64.rpm
krb5-libs-1.18.2-30.el8_10.x86_64.rpm	sysstat-11.7.3-13.el8_10.x86_64.rpm
libqb-1.0.3-13.el8_7.x86_64.rpm	tuned-2.22.1-5.el8_10.noarch.rpm
libsoup-2.62.3-7.el8_10.x86_64.rpm	tzdata-2024b-4.el8.noarch.rpm
mailx-12.5-29.el8.x86_64.rpm	unbound-libs-1.16.2-5.8.el8_10.x86_64.rpm
NetworkManager-1.40.16-18.el8_10.x86_64.rpm	usbguard-1.0.0-13.el8.x86_64.rpm
NetworkManager-libnm-1.40.16-18.el8_10.x86_64.rpm	usbguard-selinux-1.0.0-13.el8.noarch.rpm
NetworkManager-team-1.40.16-18.el8_10.x86_64.rpm	

SECTION 1C – ENTITLEMENTS AND CONTACTS

Material Coverage Entitlements:

Customer will need to work with their Avaya Account Manager to plan upgrades, installations and discuss pricing details.

Avaya Customer Service Coverage Entitlements:

Avaya On-Site Services and/or Avaya Authorized and Certified Business Partner are 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.