Product Correction Notice (PCN)

Issue Date:	**06-January-2026**
Supplement Date:	**30-July-2026**
Expiration Date:	**NA**
PCN Number:	**2180S**

SECTION 1 - CUSTOMER NOTICE

Products affected by this PCN:

Avaya Solutions Platform S8300 R6.0.x .

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

Description:

IMPORTANT NOTE –

- ASP R6.0.x Security Service Packs (SSPs) are ONLY applicable to ASP R6.0.0.3.0 and later. They cannot be installed on any ASP R6.0.x release < R6.0.0.3.0.
- In order to maintain code stability and compatibility, Red Hat typically does not rebase packages to older versions. Instead, they backport fixes to older versions. This can result in security scanners that only consider the Red Hat version to report vulnerabilities that are false positives. See **Section 1B** of this PCN for additional information.

30 July 2026 – Supplement 2 of this PCN introduces **Avaya Aura Solutions Platform (ASP) S8300 R6.0.x Security Service Pack #3**
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 Security Service Pack SSP#3.
(*SSP_3-asp-all-6.0.0.0.0-02.zip*; PLDS ID ASP000000141)

- Beginning with ASP R6.0.0.3.0, ASP R6.x security updates (both Linux and Kernel) are provided in a Security Service Pack (SSP).
- ASP R6.x SSPs are only applicable to ASP R6.0.0.3.0 and later. They will not work on earlier ASP R6.x releases.
- ASP R6.x SSP #3 must be installed to ensure robust security protection.
- Reference the "***Security Information"*** section of this PCN for updates to the rpm and RHSAs for SSP #3.

31 March 2026 – Supplement 1 of this PCN introduces **Avaya Aura Solutions Platform (ASP) S8300 R6.0.x Security Service Pack #2**
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 Security Service Pack SSP#2.
(*SSP_2-asp-all-6.0.0.0.0-02.zip*; PLDS ID ASP000000139)

- Beginning with ASP R6.0.0.3.0, ASP R6.x security updates (both Linux and Kernel) are

provided in a Security Service Pack (SSP).

- ASP R6.x SSPs are only applicable to ASP R6.0.0.3.0 and later. They will not work on earlier ASP R6.x releases.
- ASP R6.x SSP #2 must be installed to ensure robust security protection.
- Reference the "***Security Information"*** section of this PCN for updates to the rpm and RHSAs for SSP #2.

6 January 2026 – This PCN introduces **Avaya Aura Solutions Platform (ASP) S8300 R6.0.x Security Service Pack #1**
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 Security Service Pack SSP#1.

(*SSP_1-asp-all-6.0.0.0.0-02.zip*; PLDS ID ASP0000000137)

- Beginning with ASP R6.0.0.3.0, ASP R6.x security updates (both Linux and Kernel) are provided in a Security Service Pack (SSP).
- ASP R6.x SSPs are only applicable to ASP R6.0.0.3.0 and later. They will not work on earlier ASP R6.x releases.
- ASP R6.x SSP #1 must be installed to ensure robust security protection.
- Reference the "***Security Information"*** section of this PCN for updates to the rpm and RHSAs for SSP #1.

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 ASP R6.0.0.3.0 and later.
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 will disrupt service since it requires a full Linux reboot.
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** resolves vulnerabilities described by RHSAs/CVES referenced in **Section 1B – Security information.** Security Service Packs (SSPs) are cumulative.
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 ASP R6.x 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 ASP R6.x security updates, the installation instructions are required. To obtain the installation instructions please refer to the **Finding the installation instructions** section of this PCN.
How do I order this PCN (If PCN can be customer installed):	The specified Avaya Solutions Platform SSP 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 S8300 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 S8300 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. **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 S8300 software. 2. All Avaya Solutions Platform S8300 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):	Reference the ***Avaya Solutions Platform (ASP) R6.0.x (KVM on RHEL 8.10) Security Service Pack (SSP) Installation Application Note*** for detailed installation instructions. **Notes:** ● Once an SSP is activated, it cannot be deactivated/removed. It is advised to have application level backups and a Virtual Machine Backup (Clone) prior to activation of the SSP. ● Security Service Packs are independent of other ASP R6.x software updates (Service Packs). ● SSPs are cumulative. The current SSP will include the fixes from all previous SSPs.

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:	Reference the ***Avaya Solutions Platform (ASP) R6.0.x (KVM on RHEL 8.10) Security Service Pack (SSP) Installation Application Note*** for detailed verification instructions.
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:	Security Service Packs cannot be deactivated.

SECTION 1B – SECURITY INFORMATION

Are there any security risks involved?	Issues described by the RHSAs listed in the next section are corrected by the Security Service Pack as noted. Security Service Packs (SSPs) include the fixes from all previous SSPs.
Avaya Security	NA

Vulnerability Classification:	

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

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

NOTE: *SSP #3 was built July 9, 2026. Therefore, any fix released by RHEL AFTER July 9 will not be in SSP #3.*

Avaya adopts security fixes exclusively from the official Red Hat Enterprise Linux (RHEL) repositories. Because fixes may become available before they are incorporated into an official RHEL package, vulnerability timelines should always be based on the RHEL CVE dates rather than dates published by other sources.

Security Service Packs (SSPs) are cumulative.

ASP R6.0.x SSP #3 July 2026 includes the following rpm updates:

av-asp-tools-1.8-2.el8.x86_64.rpm	net-snmp-agent-libs-5.8-33.el8_10.x86_64.rpm
bind-export-libs-9.11.36-16.el8_10.8.x86_64.rpm	net-snmp-libs-5.8-33.el8_10.x86_64.rpm
bind-libs-9.11.36-16.el8_10.8.x86_64.rpm	net-snmp-utils-5.8-33.el8_10.x86_64.rpm
bind-libs-lite-9.11.36-16.el8_10.8.x86_64.rpm	nfs-utils-2.3.3-68.el8_10.x86_64.rpm
bind-license-9.11.36-16.el8_10.8.noarch.rpm	openssh-8.0p1-29.el8_10.x86_64.rpm
bind-utils-9.11.36-16.el8_10.8.x86_64.rpm	openssh-clients-8.0p1-29.el8_10.x86_64.rpm
binutils-2.30-128.el8_10.x86_64.rpm	openssh-server-8.0p1-29.el8_10.x86_64.rpm
bpftool-4.18.0-553.141.1.el8_10.x86_64.rpm	openssl-1.1.1k-16.el8_6.x86_64.rpm
brotli-1.0.6-4.el8_10.x86_64.rpm	openssl-libs-1.1.1k-16.el8_6.x86_64.rpm
cockpit-310.8-1.el8_10.x86_64.rpm	packageKit-1.1.12-8.el8_10.x86_64.rpm
cockpit-bridge-310.8-1.el8_10.x86_64.rpm	PackageKit-glib-1.1.12-8.el8_10.x86_64.rpm
cockpit-system-310.8-1.el8_10.noarch.rpm	platform-python-3.6.8-76.el8_10.x86_64.rpm
cockpit-ws-310.8-1.el8_10.x86_64.rpm	postfix-3.5.8-8.el8_10.x86_64.rpm
curl-7.61.1-34.el8_10.9.x86_64.rpm	python3-bind-9.11.36-16.el8_10.8.noarch.rpm
dnsmasq-2.79-36.el8_10.x86_64.rpm	python3-libs-3.6.8-76.el8_10.x86_64.rpm
dracut-049-244.git20260529.el8_10.x86_64.rpm	python3-libxml2-2.9.7-21.el8_10.6.x86_64.rpm
dracut-config-generic-049-244.git20260529.el8_10.x86_64.rpm	python3-perf-4.18.0-553.141.1.el8_10.x86_64.rpm
dracut-config-rescue-049-244.git20260529.el8_10.x86_64.rpm	python3-sss-2.9.4-5.el8_10.3.x86_64.rpm
dracut-network-049-244.git20260529.el8_10.x86_64.rpm	python3-sssdconfig-2.9.4-5.el8_10.3.noarch.rpm
dracut-squash-049-244.git20260529.el8_10.x86_64.rpm	python3-unbound-1.16.2-5.11.el8_10.x86_64.rpm
edk2-ovmf-20220126gitbb1bba3d77-13.el8_10.10.noarch.rpm	python3-urllib3-1.24.2-10.el8_10.noarch.rpm
expat-2.5.0-2.el8_10.x86_64.rpm	qemu-guest-agent-6.2.0-53.module+el8.10.0+23760+c0926e61.6.x86_64.rpm
gdk-pixbuf2-2.36.12-8.el8_10.x86_64.rpm	
glib2-2.56.4-169.el8_10.x86_64.rpm	qemu-img-6.2.0-

glibc-2.28-251.el8_10.38.x86_64.rpm
glibc-all-langpacks-2.28-251.el8_10.38.x86_64.rpm
glibc-common-2.28-251.el8_10.38.x86_64.rpm
glibc-gconv-extra-2.28-251.el8_10.38.x86_64.rpm
gnupg2-2.2.20-4.el8_10.x86_64.rpm
gnupg2-smime-2.2.20-4.el8_10.x86_64.rpm
gnutls-3.6.16-8.el8_10.6.x86_64.rpm
gnutls-dane-3.6.16-8.el8_10.6.x86_64.rpm
gnutls-utils-3.6.16-8.el8_10.6.x86_64.rpm
grub2-common-2.02-170.el8_10.1.noarch.rpm
grub2-efi-x64-2.02-170.el8_10.1.x86_64.rpm
grub2-pc-2.02-170.el8_10.1.x86_64.rpm
grub2-pc-modules-2.02-170.el8_10.1.noarch.rpm
grub2-tools-2.02-170.el8_10.1.x86_64.rpm
grub2-tools-efi-2.02-170.el8_10.1.x86_64.rpm
grub2-tools-extra-2.02-170.el8_10.1.x86_64.rpm
grub2-tools-minimal-2.02-170.el8_10.1.x86_64.rpm
gstreamer1-plugins-base-1.16.1-6.el8_10.x86_64.rpm
jq-1.6-12.el8_10.x86_64.rpm
kernel-4.18.0-553.141.1.el8_10.x86_64.rpm
kernel-core-4.18.0-553.141.1.el8_10.x86_64.rpm
kernel-modules-4.18.0-553.141.1.el8_10.x86_64.rpm
kernel-tools-4.18.0-553.141.1.el8_10.x86_64.rpm
kernel-tools-libs-4.18.0-553.141.1.el8_10.x86_64.rpm
krb5-libs-1.18.2-34.el8_10.x86_64.rpm
libarchive-3.3.3-7.el8_10.x86_64.rpm
libblkid-2.32.1-48.el8_10.x86_64.rpm
libcap-2.48-6.el8_10.1.x86_64.rpm
libcurl-7.61.1-34.el8_10.9.x86_64.rpm
libfdisk-2.32.1-48.el8_10.x86_64.rpm
libipa_hbac-2.9.4-5.el8_10.3.x86_64.rpm
libluksmeta-9-4.el8_10.1.x86_64.rpm
libmount-2.32.1-48.el8_10.x86_64.rpm
libnfsidmap-2.3.3-68.el8_10.x86_64.rpm
libnghttp2-1.33.0-6.el8_10.2.x86_64.rpm
libpng-1.6.34-11.el8_10.x86_64.rpm
libsmartcols-2.32.1-48.el8_10.x86_64.rpm
libsmbclient-4.19.4-16.el8_10.x86_64.rpm
libsolv-0.7.20-7.el8_10.x86_64.rpm
libsoup-2.62.3-14.el8_10.x86_64.rpm
libssh-0.9.6-16.el8_10.x86_64.rpm
libssh-config-0.9.6-16.el8_10.noarch.rpm
libsss_autofs-2.9.4-5.el8_10.3.x86_64.rpm
libsss_certmap-2.9.4-5.el8_10.3.x86_64.rpm
libsss_idmap-2.9.4-5.el8_10.3.x86_64.rpm
libsss_nss_idmap-2.9.4-5.el8_10.3.x86_64.rpm
Libsss_sudo-2.9.4-5.el8_10.3.x86_64.rpm
libtasn1-4.13-6.el8_10.x86_64.rpm
libuuid-2.32.1-48.el8_10.x86_64.rpm
libwbclient-4.19.4-16.el8_10.x86_64.rpm
libxml2-2.9.7-21.el8_10.6.x86_64.rpm
libxslt-1.1.32-6.4.el8_10.x86_64.rpm
luksmeta-9-4.el8_10.1.x86_64.rpm
net-snmp-5.8-33.el8_10.x86_64.rpm
53.module+el8.10.0+23760+c0926e61.6.x86_64.rpm
qemu-kvm-6.2.0-
53.module+el8.10.0+23760+c0926e61.6.x86_64.rpm
qemu-kvm-block-curl-6.2.0-
53.module+el8.10.0+23760+c0926e61.6.x86_64.rpm
qemu-kvm-block-gluster-6.2.0-
53.module+el8.10.0+23760+c0926e61.6.x86_64.rpm
qemu-kvm-block-iscsi-6.2.0-
53.module+el8.10.0+23760+c0926e61.6.x86_64.rpm
qemu-kvm-block-rbd-6.2.0-
53.module+el8.10.0+23760+c0926e61.6.x86_64.rpm
qemu-kvm-block-ssh-6.2.0-
53.module+el8.10.0+23760+c0926e61.6.x86_64.rpm
qemu-kvm-common-6.2.0-
53.module+el8.10.0+23760+c0926e61.6.x86_64.rpm
qemu-kvm-core-6.2.0-
53.module+el8.10.0+23760+c0926e61.6.x86_64.rpm
qemu-kvm-docs-6.2.0-
53.module+el8.10.0+23760+c0926e61.6.x86_64.rpm
qemu-kvm-hw-usbredir-6.2.0-
53.module+el8.10.0+23760+c0926e61.6.x86_64.rpm
qemu-kvm-ui-opengl-6.2.0-
53.module+el8.10.0+23760+c0926e61.6.x86_64.rpm
qemu-kvm-ui-spice-6.2.0-
53.module+el8.10.0+23760+c0926e61.6.x86_64.rpm
rsync-3.1.3-27.el8_10.x86_64.rpm
samba-client-libs-4.19.4-16.el8_10.x86_64.rpm
samba-common-4.19.4-16.el8_10.noarch.rpm
samba-common-libs-4.19.4-16.el8_10.x86_64.rpm
selinux-policy-3.14.3-139.el8_10.2.noarch.rpm
selinux-policy-targeted-3.14.3-139.el8_10.2.noarch.rpm
shim-x64-16.1-2.el8.x86_64.rpm
sssd-2.9.4-5.el8_10.3.x86_64.rpm
sssd-ad-2.9.4-5.el8_10.3.x86_64.rpm
sssd-client-2.9.4-5.el8_10.3.x86_64.rpm
sssd-common-2.9.4-5.el8_10.3.x86_64.rpm
sssd-common-pac-2.9.4-5.el8_10.3.x86_64.rpm
sssd-dbus-2.9.4-5.el8_10.3.x86_64.rpm
sssd-ipa-2.9.4-5.el8_10.3.x86_64.rpm
sssd-kcm-2.9.4-5.el8_10.3.x86_64.rpm
sssd-krb5-2.9.4-5.el8_10.3.x86_64.rpm
sssd-krb5-common-2.9.4-5.el8_10.3.x86_64.rpm
sssd-ldap-2.9.4-5.el8_10.3.x86_64.rpm
sssd-nfs-idmap-2.9.4-5.el8_10.3.x86_64.rpm
sssd-tools-2.9.4-5.el8_10.3.x86_64.rpm
sudo-1.9.5p2-1.el8_10.5.x86_64.rpm
tzdata-2026b-1.el8.noarch.rpm
unbound-libs-1.16.2-5.11.el8_10.x86_64.rpm
util-linux-2.32.1-48.el8_10.x86_64.rpm
util-linux-user-2.32.1-48.el8_10.x86_64.rpm
vim-common-8.0.1763-24.el8_10.x86_64.rpm
vim-enhanced-8.0.1763-24.el8_10.x86_64.rpm
vim-filesystem-8.0.1763-24.el8_10.noarch.rpm
vim-minimal-8.0.1763-24.el8_10.x86_64.rpm

Security vulnerabilities resolved in ASP R6.0.x Security Service Pack #3 July 2026

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
gdk-pixbuf2	RHSA-2026:10741	CVE-2026-5201	Important
platform-python python3-libs	RHSA-2026:11077	CVE-2026-4786 CVE-2026-6100	Important
libxml2 python3-libxml2	RHSA-2026:11349	CVE-2025-9714	Moderate
Vim-common Vim-enhanced Vim-filesystem vim-minimal	RHSA-2026:11509	CVE-2026-34982	Important
sudo	RHSA-2026:11521	CVE-2026-35535	Important
PackageKit PackageKit-glib	RHSA-2026:11635	CVE-2026-41651	Important
libcap	RHSA-2026:13285	CVE-2026-4878	Important
Openssh Openssh-clients openssh-server	RHSA-2026:13383	CVE-2026-35385 CVE-2026-35386 CVE-2026-35387 CVE-2026-35388 CVE-2026-35414	Important
Bpftool Kernel Kernel-core Kernel-modules Kernel-tools Kernel-tools-libs python3-perf	RHSA-2026:13577	CVE-2024-41073 CVE-2025-40252 CVE-2025-68724 CVE-2026-23401 CVE-2026-31402 CVE-2026-31431 CVE-2026-43077	Important
libsoup	RHSA-2026:14087	CVE-2026-5119	Moderate
glib2	RHSA-2026:15953	CVE-2025-14087;CVE-2025-14512	Moderate
Bpftool Kernel Kernel-core Kernel-modules Kernel-tools Kernel-tools-libs python3-perf	RHSA-2026:16195	CVE-2026-43284	Important
jq	RHSA-2026:16252	CVE-2026-39979 CVE-2026-40164	Important
krb5-libs	RHSA-2026:16799	CVE-2026-40355 CVE-2026-40356	Important

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
rsync	RHSA-2026:17481	CVE-2026-41035	Important
Bpftool Kernel Kernel-core Kernel-modules Kernel-tools Kernel-tools-libs python3-perf	RHSA-2026:19666	CVE-2026-43503 CVE-2026-46300 CVE-2026-46333	Important
Glibc Glibc-all-langpacks Glibc-common glibc-gconv-extra	RHSA-2026:20587	CVE-2026-4046	Moderate
Dnsmasq	RHSA-2026:20589	CVE-2026-2291 CVE-2026-4890 CVE-2026-4891 CVE-2026-4892 CVE-2026-4893	Important
Gnutls Gnutls-dane Gnutls-utils	RHSA-2026:20611	CVE-2026-33845 CVE-2026-33846 CVE-2026-3833 CVE-2026-42009 CVE-2026-42010 CVE-2026-42011 CVE-2026-42012 CVE-2026-42013 CVE-2026-42014 CVE-2026-42015 CVE-2026-5260	Important
Cockpit Cockpit-bridge Cockpit-system cockpit-ws	RHSA-2026:21700	CVE-2026-4802	Important

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
Bpftool Kernel Kernel-core Kernel-modules Kernel-tools Kernel-tools-libs Python3-perf	RHSA-2026:21706	CVE-2025-39981 CVE-2025-68183 CVE-2025-68347 CVE-2025-71116 CVE-2026-23243 CVE-2026-23270 CVE-2026-23455 CVE-2026-31408 CVE-2026-31532 CVE-2026-31684 CVE-2026-31685 CVE-2026-31709 CVE-2026-43020 CVE-2026-43027 CVE-2026-43051 CVE-2026-43158 CVE-2026-43163 CVE-2026-43190 CVE-2026-46195	Important
Libsmbclient Libwbclient Samba-client-libs Samba-common samba-common-libs	RHSA-2026:22644	CVE-2026-1933 CVE-2026-2340 CVE-2026-3012 CVE-2026-4408 CVE-2026-4480	Important
expat	RHSA-2026:22721	CVE-2026-45186	Important
Vim-common Vim-enhanced Vim-filesystem vim-minimal	RHSA-2026:22730	CVE-2026-35177	Moderate
Bpftool Kernel Kernel-core Kernel-modules Kernel-tools Kernel-tools-libs python3-perf	RHSA-2026:23258	CVE-2026-46243	Important
Bind-export-libs Bind-libs Bind-libs-lite Bind-license Bind-utils python3-bind	RHSA-2026:24339	CVE-2026-3039 CVE-2026-5946	Important
Python3-unbound unbound-libs	RHSA-2026:24365	CVE-2026-42944 CVE-2026-42959	Important

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
Bpftool Kernel Kernel-core Kernel-modules Kernel-tools Kernel-tools-libs Python3-perf	RHSA-2026:25121	CVE-2023-53781 CVE-2025-21858 CVE-2025-68366 CVE-2026-22984 CVE-2026-22990 CVE-2026-23392 CVE-2026-31581 CVE-2026-31613 CVE-2026-43037 CVE-2026-43038 CVE-2026-43125 CVE-2026-45852 CVE-2026-46181	Critical
postfix	RHSA-2026:25932	CVE-2026-43964	Important
Openssl openssl-libs	RHSA-2026:26275	CVE-2024-4741 CVE-2026-45447	Important
Libxml2 python3-libxml2	RHSA-2026:26354	CVE-2024-34459	Low
libxslt	RHSA-2026:26355	CVE-2025-10911	Moderate
rsync	RHSA-2026:26408	CVE-2026-29518 CVE-2026-43618	Important
Bpftool Kernel Kernel-core Kernel-modules Kernel-tools Kernel-tools-libs python3-perf	RHSA-2026:26427	CVE-2026-31669 CVE-2026-31786 CVE-2026-31787 CVE-2026-43110 CVE-2026-43329 CVE-2026-46056 CVE-2026-46125 CVE-2026-46152	Important
Dracut Dracut-config-generic Dracut-config-rescue Dracut-network dracut-squash	RHSA-2026:26534	CVE-2026-6893	Important
Bpftool Kernel Kernel-core Kernel-modules Kernel-tools Kernel-tools-libs python3-perf	RHSA-2026:27353	CVE-2026-31419 CVE-2026-31488 CVE-2026-43056 CVE-2026-43279 CVE-2026-46090 CVE-2026-46135 CVE-2026-46145 CVE-2026-46331	Important

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
Bpftool Kernel Kernel-core Kernel-modules Kernel-tools Kernel-tools-libs python3-perf	RHSA-2026:27811	CVE-2026-46054	Important
Vim-common Vim-enhanced Vim-filesystem vim-minimal	RHSA-2026:28553	CVE-2026-41411	Moderate
libpng	RHSA-2026:29898	CVE-2026-33416	Moderate
Openssl openssl-libs	RHSA-2026:3042	CVE-2025-69419	Moderate
Bpftool Kernel Kernel-core Kernel-modules Kernel-tools Kernel-tools-libs python3-perf	RHSA-2026:3083	CVE-2025-38129 CVE-2025-38248 CVE-2025-40064 CVE-2025-68800 CVE-2026-23074	Important
Glibc Glibc-all-langpacks Glibc-common glibc-gconv-extra	RHSA-2026:33126	CVE-2026-5450	Moderate
Bpftool Kernel Kernel-core Kernel-modules Kernel-tools Kernel-tools-libs python3-perf	RHSA-2026:33743	CVE-2026-23216 CVE-2026-45984 CVE-2026-46189	Important
Bpftool Kernel Kernel-core Kernel-modules Kernel-tools Kernel-tools-libs python3-perf	RHSA-2026:3464	CVE-2026-23097	Moderate

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
Bpftool Kernel Kernel-core Kernel-modules Kernel-tools Kernel-tools-libs python3-perf	RHSA-2026:36349	CVE-2025-10263 CVE-2026-43198 CVE-2026-43450 CVE-2026-46209 CVE-2026-46227 CVE-2026-46259	Important
Bpftool Kernel Kernel-core Kernel-modules Kernel-tools kernel-tools-libs python3-perf	RHSA-2026:36366	CVE-2026-43112	Important
edk2-ovmf	RHSA-2026:36721	CVE-2025-9230	Moderate
libtasn1	RHSA-2026:36728	CVE-2025-13151	Low
libsolv	RHSA-2026:36730	CVE-2026-48864	Moderate
python3-urllib3	RHSA-2026:36732	CVE-2026-44431	Moderate
Libxml2 python3-libxml2	RHSA-2026:36734	CVE-2025-6170	Low
Libnfsidmap nfs-utils	RHSA-2026:3938	CVE-2025-12801	Moderate
Bpftool Kernel Kernel-core Kernel-modules Kernel-tools Kernel-tools-libs python3-perf	RHSA-2026:3963	CVE-2025-71085 CVE-2026-23001	Moderate
Vim-common Vim-enhanced Vim-filesystem vim-minimal	RHSA-2026:4442	CVE-2026-25749	Moderate
Grub2-common Grub2-efi-x64 Grub2-pc Grub2-pc-modules Grub2-tools Grub2-tools-efi Grub2-tools-extra grub2-tools-minimal	RHSA-2026:4648	CVE-2025-61662	Moderate

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
libpng	RHSA-2026:4728	CVE-2026-22695 CVE-2026-22801 CVE-2026-25646	Important
Glibc Glibc-all-langpacks Glibc-common glibc-gconv-extra	RHSA-2026:4772	CVE-2025-15281 CVE-2026-0915	Moderate
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-2026:5578	CVE-2025-11234	Moderate
Gnutls Gnutls-dane gnutls-utils	RHSA-2026:5585	CVE-2025-14831 CVE-2025-9820	Moderate
platform-python;python3-libs	RHSA-2026:5588	CVE-2025-0938	Moderate
Bpftool Kernel Kernel-core Kernel-modules Kernel-tools Kernel-tools-libs python3-perf	RHSA-2026:6037	CVE-2025-38180 CVE-2026-23204 CVE-2026-23209	Moderate
rsync	RHSA-2026:6436	CVE-2025-10158	Moderate
Openssh Openssh-clients openssh-server	RHSA-2026:6461	CVE-2026-3497	Important
Platform-python python3-libs	RHSA-2026:6473	CVE-2026-4519	Important

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
Bpftool Kernel Kernel-core Kernel-modules Kernel-tools Kernel-tools-libs python3-perf	RHSA-2026:6571	CVE-2024-26984 CVE-2025-71238 CVE-2026-23193 CVE-2026-23231	Moderate
gstreamer1-plugins-base	RHSA-2026:6750	CVE-2026-2920 CVE-2026-2921 CVE-2026-2923 CVE-2026-3082 CVE-2026-3083 CVE-2026-3085	Important
Vim-common Vim-enhanced Vim-filesystem vim-minimal	RHSA-2026:6915	CVE-2026-28417 CVE-2026-28421 CVE-2026-33412	Important
libnghttp2	RHSA-2026:7667	CVE-2026-27135	Important
Bind-export-libs Bind-libs Bind-libs-lite Bind-license Bind-utils python3-bind	RHSA-2026:8352	CVE-2026-1519	Important
libarchive	RHSA-2026:8534	CVE-2026-4424 CVE-2026-5121	Important
Bpftool Kernel Kernel-core Kernel-modules Kernel-tools Kernel-tools-libs python3-perf	RHSA-2026:9131	CVE-2025-68741 CVE-2026-23191	Important

ASP R6.0.x SSP #2 March 2026 includes the following rpm updates:

binutils-2.30-128.el8_10.x86_64.rpm	libsoup-2.62.3-13.el8_10.x86_64.rpm
bpftool-4.18.0-553.105.1.el8_10.x86_64.rpm	libuuid-2.32.1-48.el8_10.x86_64.rpm
brotli-1.0.6-4.el8_10.x86_64.rpm	luksmeta-9-4.el8_10.1.x86_64.rpm
curl-7.61.1-34.el8_10.9.x86_64.rpm	net-snmp-5.8-33.el8_10.x86_64.rpm
glib2-2.56.4-168.el8_10.x86_64.rpm	net-snmp-agent-libs-5.8-33.el8_10.x86_64.rpm
gnupg2-2.2.20-4.el8_10.x86_64.rpm	net-snmp-libs-5.8-33.el8_10.x86_64.rpm
gnupg2-smime-2.2.20-4.el8_10.x86_64.rpm	net-snmp-utils-5.8-33.el8_10.x86_64.rpm
kernel-4.18.0-553.105.1.el8_10.x86_64.rpm	openssh-8.0p1-27.el8_10.x86_64.rpm
kernel-core-4.18.0-553.105.1.el8_10.x86_64.rpm	openssh-clients-8.0p1-27.el8_10.x86_64.rpm

kernel-modules-4.18.0-553.105.1.el8_10.x86_64.rpm kernel-tools-4.18.0-553.105.1.el8_10.x86_64.rpm kernel-tools-libs-4.18.0-553.105.1.el8_10.x86_64.rpm libblkid-2.32.1-48.el8_10.x86_64.rpm libcurl-7.61.1-34.el8_10.9.x86_64.rpm libfdisk-2.32.1-48.el8_10.x86_64.rpm libluksmeta-9-4.el8_10.1.x86_64.rpm libmount-2.32.1-48.el8_10.x86_64.rpm libpng-1.6.34-9.el8_10.x86_64.rpm libsmartcols-2.32.1-48.el8_10.x86_64.rpm	openssh-server-8.0p1-27.el8_10.x86_64.rpm openssl-1.1.1k-14.el8_10.x86_64.rpm openssl-libs-1.1.1k-14.el8_10.x86_64.rpm platform-python-3.6.8-73.el8_10.x86_64.rpm python3-libs-3.6.8-73.el8_10.x86_64.rpm python3-perf-4.18.0-553.105.1.el8_10.x86_64.rpm python3-urllib3-1.24.2-9.el8_10.noarch.rpm util-linux-2.32.1-48.el8_10.x86_64.rpm util-linux-user-2.32.1-48.el8_10.x86_64.rpm

Security vulnerabilities resolved in ASP R6.0.x Security Service Pack #2 March 2026

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:19102	CVE-2022-50386 CVE-2023-53297 CVE-2023-53386 CVE-2025-22045 CVE-2025-39817 CVE-2025-39841 CVE-2025-39849	Moderate
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:19447	CVE-2022-50856 CVE-2023-53226 CVE-2023-53257 CVE-2023-53751 CVE-2025-39864	Moderate
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:19931	CVE-2022-50367 CVE-2023-53178 CVE-2025-40300	Moderate
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:21398	CVE-2025-39718	Moderate
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:21917	CVE-2025-39697 CVE-2025-39971 CVE-2025-39973	Moderate

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:22388	CVE-2023-53513 CVE-2025-38724 CVE-2025-39825 CVE-2025-39883 CVE-2025-39898 CVE-2025-39955 CVE-2025-40186	Moderate
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:22801	CVE-2022-50543 CVE-2023-53401 CVE-2023-53539	Moderate
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2026:0444	CVE-2025-39993 CVE-2025-40240 CVE-2025-68285	Important
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2026:0759	CVE-2023-53552 CVE-2025-38051 CVE-2025-39933 CVE-2025-40096 CVE-2025-68301	Important
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2026:1142	CVE-2023-53673 CVE-2025-40154 CVE-2025-40248 CVE-2025-40277	Important
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2026:1162	CVE-2022-50865 CVE-2024-26766 CVE-2025-38022 CVE-2025-38024 CVE-2025-38415 CVE-2025-38459 CVE-2025-39760 CVE-2025-40258 CVE-2025-40271 CVE-2025-40322	Moderate

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2026:2264	CVE-2022-50673 CVE-2025-38403 CVE-2025-40135 CVE-2025-40158 CVE-2025-40170 CVE-2025-40269 CVE-2025-68349 CVE-2026-22998	Moderate
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2026:2720	CVE-2023-53762 CVE-2025-40168 CVE-2025-40304	Moderate
libluksmeta luksmeta	RHSA-2025:23086	CVE-2025-11568	Moderate
binutils	RHSA-2025:23382	CVE-2025-11083	Moderate
curl libcurl	RHSA-2025:23383	CVE-2025-9086	Moderate
openssh openssh-clients openssh-server	RHSA-2025:23481	CVE-2025-61984;CVE-2025-61985	Moderate
libpng	RHSA-2026:0241	CVE-2025-64720 CVE-2025-65018 CVE-2025-66293	Important
openssl openssl-libs	RHSA-2026:0337	CVE-2025-9230	Moderate
libsoup	RHSA-2026:0421	CVE-2025-14523	Important
gnupg2 gnupg2-smime	RHSA-2026:0728	CVE-2025-68973	Important
net-snmp net-snmp-agent-libs net-snmp-libs net-snmp-utils	RHSA-2026:0750	CVE-2025-68615	Important
glib2	RHSA-2026:0991	CVE-2025-13601	Moderate
python3-urllib3	RHSA-2026:1254	CVE-2025-66418 CVE-2025-66471 CVE-2026-21441	Important
platform-python python3-libs	RHSA-2026:1631	CVE-2025-12084	Moderate
libblkid libfdisk libmount libsmartcols libuuid util-linux util-linux-user	RHSA-2026:1852	CVE-2025-14104	Moderate

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
platform-python python3-libs	RHSA-2026:2128	CVE-2025-15366 CVE-2025-15367 CVE-2026-0865 CVE-2026-1299	Moderate
libsoup	RHSA-2026:2215	CVE-2026-0719 CVE-2026-1761	Important
brotli	RHSA-2026:2389	CVE-2025-6176	Important

ASP R6.0.x SSP #1 January 2026 includes the following rpm updates:

bind-export-libs-9.11.36-16.el8_10.6.x86_64.rpm	openssh-clients-8.0p1-26.el8_10.x86_64.rpm
bind-libs-9.11.36-16.el8_10.6.x86_64.rpm	openssh-server-8.0p1-26.el8_10.x86_64.rpm
bind-libs-lite-9.11.36-16.el8_10.6.x86_64.rpm	python3-bind-9.11.36-16.el8_10.6.noarch.rpm
bind-license-9.11.36-16.el8_10.6.noarch.rpm	python3-perf-4.18.0-553.80.1.el8_10.x86_64.rpm
bind-utils-9.11.36-16.el8_10.6.x86_64.rpm	python3-sss-2.9.4-5.el8_10.3.x86_64.rpm
bpftool-4.18.0-553.80.1.el8_10.x86_64.rpm	python3-sssdconfig-2.9.4-5.el8_10.3.noarch.rpm
expat-2.5.0-1.el8_10.x86_64.rpm	samba-client-libs-4.19.4-12.el8_10.x86_64.rpm
gnutls-3.6.16-8.el8_10.4.x86_64.rpm	samba-common-4.19.4-12.el8_10.noarch.rpm
gnutls-dane-3.6.16-8.el8_10.4.x86_64.rpm	samba-common-libs-4.19.4-12.el8_10.x86_64.rpm
gnutls-utils-3.6.16-8.el8_10.4.x86_64.rpm	sssd-2.9.4-5.el8_10.3.x86_64.rpm
kernel-4.18.0-553.80.1.el8_10.x86_64.rpm	sssd-ad-2.9.4-5.el8_10.3.x86_64.rpm
kernel-core-4.18.0-553.80.1.el8_10.x86_64.rpm	sssd-client-2.9.4-5.el8_10.3.x86_64.rpm
kernel-modules-4.18.0-553.80.1.el8_10.x86_64.rpm	sssd-common-2.9.4-5.el8_10.3.x86_64.rpm
kernel-tools-4.18.0-553.80.1.el8_10.x86_64.rpm	sssd-common-pac-2.9.4-5.el8_10.3.x86_64.rpm
kernel-tools-libs-4.18.0-553.80.1.el8_10.x86_64.rpm	sssd-dbus-2.9.4-5.el8_10.3.x86_64.rpm
libipa_hbac-2.9.4-5.el8_10.3.x86_64.rpm	sssd-ipa-2.9.4-5.el8_10.3.x86_64.rpm
libsmbclient-4.19.4-12.el8_10.x86_64.rpm	sssd-kcm-2.9.4-5.el8_10.3.x86_64.rpm
libsoup-2.62.3-10.el8_10.x86_64.rpm	sssd-krb5-2.9.4-5.el8_10.3.x86_64.rpm
libssh-0.9.6-16.el8_10.x86_64.rpm	sssd-krb5-common-2.9.4-5.el8_10.3.x86_64.rpm
libssh-config-0.9.6-16.el8_10.noarch.rpm	sssd-ldap-2.9.4-5.el8_10.3.x86_64.rpm
libsss_autofs-2.9.4-5.el8_10.3.x86_64.rpm	sssd-nfs-idmap-2.9.4-5.el8_10.3.x86_64.rpm
libsss_certmap-2.9.4-5.el8_10.3.x86_64.rpm	sssd-tools-2.9.4-5.el8_10.3.x86_64.rpm
libsss_idmap-2.9.4-5.el8_10.3.x86_64.rpm	vim-common-8.0.1763-21.el8_10.x86_64.rpm
libsss_nss_idmap-2.9.4-5.el8_10.3.x86_64.rpm	vim-enhanced-8.0.1763-21.el8_10.x86_64.rpm
libsss_sudo-2.9.4-5.el8_10.3.x86_64.rpm	vim-filesystem-8.0.1763-21.el8_10.noarch.rpm
libwbclient-4.19.4-12.el8_10.x86_64.rpm	vim-minimal-8.0.1763-21.el8_10.x86_64.rpm
openssh-8.0p1-26.el8_10.x86_64.rpm	

Security vulnerabilities resolved in ASP R6.0.x Security Service Pack #1 January 2026

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:15471	CVE-2022-49985 CVE-2025-38352	Important

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:15785	CVE-2023-53125 CVE-2025-38350 CVE-2025-38392 CVE-2025-38449 CVE-2025-38684	Important
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:16372	CVE-2025-38461 CVE-2025-38498 CVE-2025-38556	Moderate
openssh openssh-clients openssh-server	RHSA-2025:16823	CVE-2025-26465	Moderate
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:16919	CVE-2022-50087 CVE-2025-22026 CVE-2025-37797 CVE-2025-38718	Moderate
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-lib python3-perf	RHSA-2025:17397	CVE-2025-38527 CVE-2025-39730	Moderate
gnutl gnutls-dane gnutls-utils	RHSA-2025:17415	CVE-2025-32988 CVE-2025-32990 CVE-2025-6395	Moderate
vim-common vim-enhanced vim-filesystem vim-minimal	RHSA-2025:17715	CVE-2025-53905 CVE-2025-53906	Moderate
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:17797	CVE-2022-50228 CVE-2023-53305	Moderate
libssh libssh-config	RHSA-2025:18286	CVE-2025-5318	Moderate

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
bpftool kernel kernel-core kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2025:18297	CVE-2023-53373 CVE-2025-39751 CVE-2025-39757	Moderate
	RHSA-2025:19610	CVE-2025-11561	Important
libsoup	RHSA-2025:19714	CVE-2025-11021 CVE-2025-4945	Important
bind-export-libs bind-libs bind-libs-lite bind-license bind-utils python3-bind	RHSA-2025:19835	CVE-2025-40778	Important
expat	RHSA-2025:21776	CVE-2013-0340 CVE-2022-23990 CVE-2024-28757 CVE-2025-59375	Important
libssh libssh-config	RHSA-2025:21977	CVE-2025-5372	Moderate

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.