Product Correction Notice (PCN)

Issue Date:	**April 11, 2022**
Supplement Date:	**Nov 12, 2026**
Expiration Date:	**NA**
PCN Number:	**2149S**

SECTION 1 - CUSTOMER NOTICE

Products affected by this PCN:

Avaya Diagnostic Server 4.0 OVA
(for ADS-SAL, SLAMon and Policy Manager)
Secure Access Link 4.0 OVA
(Small SAL OVA)

Description:

Beginning April 2022, Security Service Packs (SSPs) will be released on a quarterly basis. These SSPs will be available on PLDS and documented in this PCN. SSP required artifacts and fix IDs will be included in this PCN.

12-Nov-2026 – Supplement 19 – Supplement 19 of this PCN introduces **Avaya Diagnostic Server 4.0 Security Service Pack SSP #17 (ADS_SAL_SLAMON_PM40_RHEL810_SSP_017_01.tar.gz PLDS ID - ADS40OVA017)**

- ADS SSP #17 is only applicable to ADS/SAL 4.0 or later OVA deployed systems. It can be installed directly on 4.0 or later Service Pack/Feature Pack or on 4.0 or later Service Pack/Feature Pack that has an earlier SSP installed.
- Security Service Packs should NOT be applied on the Software Only offer.
- Reference the "Finding the installation instructions" section of this PCN for detailed installation instructions.
- Reference the "Security Information" section of this PCN for updates to the rpm and RHSAs for SSP #17.
- SSP#17 is cumulative to ADS OS Upgrade Bundle. Please install ADS OS Upgrade Bundle and then you can install Security Service Pack 17.

02-Nov-2026 – Supplement 18 – Supplement 18 of this PCN introduces **Avaya Diagnostic Server 4.0 Security Service Pack SSP #16 (ADS_SAL_SLAMON_PM40_RHEL810_SSP_016_01.tar.gz PLDS ID - ADS40OVA016)**

- ADS SSP #16 is only applicable to ADS/SAL 4.0 or later OVA deployed systems. It can be installed directly on 4.0 or later Service Pack/Feature Pack or on 4.0 or later Service Pack/Feature Pack that has an earlier SSP installed.
- Security Service Packs should NOT be applied on the Software Only offer.
- Reference the "Finding the installation instructions" section of this PCN for detailed installation instructions.
- Reference the "Security Information" section of this PCN for updates to the rpm and RHSAs for SSP #16.
- SSP#16 is cumulative to ADS OS Upgrade Bundle. Please install ADS OS Upgrade Bundle and then you can install Security Service Pack 16.

09-Oct-2026 – Supplement 17 – Supplement 17 of this PCN introduces **Avaya Diagnostic Server 4.0**

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

Security Service Pack SSP #15 (ADS_SAL_SLAMON_PM40_RHEL810_SSP_015_01.tar.gz
PLDS ID - ADS40OVA015)

- ADS SSP #15 is only applicable to ADS/SAL 4.0 or later OVA deployed systems. It can be installed directly on 4.0 or later Service Pack/Feature Pack or on 4.0 or later Service Pack/Feature Pack that has an earlier SSP installed.
- Security Service Packs should NOT be applied on the Software Only offer.
- Reference the "Finding the installation instructions" section of this PCN for detailed installation instructions.
- Reference the "Security Information" section of this PCN for updates to the rpm and RHSAs for SSP #15.
- SSP#15 is cumulative to ADS OS Upgrade Bundle. Please install ADS OS Upgrade Bundle and then you can install Security Service Pack 15.

06-Jul-2026 – Supplement 16 – Supplement 16 of this PCN introduces **Avaya Diagnostic Server 4.0 Security Service Pack SSP #14 (ADS_SAL_SLAMON_PM40_RHEL810_SSP_014_01.tar.gz**
PLDS ID - ADS40OVA014)

- ADS SSP #14 is only applicable to ADS/SAL 4.0 or later OVA deployed systems. It can be installed directly on 4.0 or later Service Pack/Feature Pack or on 4.0 or later Service Pack/Feature Pack that has an earlier SSP installed.
- Security Service Packs should NOT be applied on the Software Only offer.
- Reference the "Finding the installation instructions" section of this PCN for detailed installation instructions.
- Reference the "Security Information" section of this PCN for updates to the rpm and RHSAs for SSP #14.
- SSP#14 is cumulative to ADS OS Upgrade Bundle. Please install ADS OS Upgrade Bundle and then you can install Security Service Pack 14.

31-Mar-2026 – Supplement 15 – Supplement 15 of this PCN introduces **Avaya Diagnostic Server 4.0 OS Upgrade Bundle (ADS_SAL_SLAMON_PM40_RHEL_810_02.tar.gz**
PLDS ID - ADS40OVAOSU)

- ADS OS Upgrade Bundle is only applicable to ADS/SAL 4.0 or later OVA deployed systems. It can be installed directly on 4.0 or later Service Pack/Feature Pack or on 4.0 or later Service Pack/Feature Pack that has an earlier SSP installed.
- Security Service Packs should NOT be applied on the Software Only offer.
- Reference the "Finding the installation instructions" section of this PCN for detailed installation instructions.
- Reference the "Security Information" section of this PCN for updates to the rpm and RHSAs for OS Upgrade Bundle.
- OS Upgrade Bundle is cumulative to Security Service Pack 13. Please install Security Service Pack 13 and then you can install OS Upgrade Bundle.

17-Nov-2025 – Supplement 14 – Supplement 14 of this PCN introduces **Avaya Diagnostic Server 4.0 Security Service Pack SSP #13 (ADS_SAL_SLAMON_PM40_SSP_013_01.tar.gz**
PLDS ID - ADS40OVA013)

- ADS SSP #13 is only applicable to ADS/SAL 4.0 or later OVA deployed systems. It can be installed directly on 4.0 or later Service Pack/Feature Pack or on 4.0 or later Service Pack/Feature Pack that has an earlier SSP installed.
- Security Service Packs should NOT be applied on the Software Only offer.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

- Reference the "Finding the installation instructions" section of this PCN for detailed installation instructions.
- Reference the "Security Information" section of this PCN for updates to the rpm and RHSAs for SSP #13.
- SSP#13 is cumulative to Security Service Pack 12. Please install Security Service Pack 11 and then you can install Security Service Pack 13.

18-Aug-2025 – Supplement 13 – Supplement 13 of this PCN introduces **Avaya Diagnostic Server 4.0 Security Service Pack SSP #12 (ADS_SAL_SLAMON_PM40_SSP_012_01.tar.gz PLDS ID - ADS40OVA012)**

- ADS SSP #12 is only applicable to ADS/SAL 4.0 or later OVA deployed systems. It can be installed directly on 4.0 or later Service Pack/Feature Pack or on 4.0 or later Service Pack/Feature Pack that has an earlier SSP installed.
- Security Service Packs should NOT be applied on the Software Only offer.
- Reference the "Finding the installation instructions" section of this PCN for detailed installation instructions.
- Reference the "Security Information" section of this PCN for updates to the rpm and RHSAs for SSP #12.
- SSP#12 is not cumulative. Please install Security Service Pack 11 and then you can install Security Service Pack 12.

28-Apr-2025 – Supplement 12 – Supplement 12 of this PCN introduces **Avaya Diagnostic Server 4.0 Security Service Pack SSP #11 (ADS_SAL_SLAMON_PM40_SSP_011_01.tar.gz PLDS ID - ADS40OVA011)**

- ADS SSP #11 is only applicable to ADS/SAL 4.0 or later OVA deployed systems. It can be installed directly on 4.0 or later Service Pack/Feature Pack or on 4.0 or later Service Pack/Feature Pack that has an earlier SSP installed.
- Security Service Packs should NOT be applied on the Software Only offer.
- Reference the "Finding the installation instructions" section of this PCN for detailed installation instructions.
- Reference the "Security Information" section of this PCN for updates to the rpm and RHSAs for SSP #11.
- SSP#11 is not cumulative. Please install Security Service Pack 9 and then you can install Security Service Pack 11.

06-Mar-2025 – Supplement 11 – Supplement 11 of this PCN introduces **Avaya Diagnostic Server 4.0 Security Service Pack SSP #10 (ADS_SAL_SLAMON_PM40_SSP_010_02.tar.gz PLDS ID - ADS40OVA010)**

- ADS SSP #10 is only applicable to ADS/SAL 4.0 or later OVA deployed systems. It can be installed directly on 4.0 or later Service Pack/Feature Pack or on 4.0 or later Service Pack/Feature Pack that has an earlier SSP installed.
- Security Service Packs should NOT be applied on the Software Only offer.
- Reference the "Finding the installation instructions" section of this PCN for detailed installation instructions.
- Reference the "Security Information" section of this PCN for updates to the rpm and RHSAs for SSP #10.
- SSP#10 is not cumulative. Please install Security Service Pack 9 and then you can install Security Service Pack 10.

15-Jan-2025 – Supplement 10-1 – Supplement 10-1 of this PCN corrects the typo from SSP#8 to

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

SSP#9 in RHSA and CVE section.

13-Jan-2025 – Supplement 10 – Supplement 10 of this PCN updates RHSA to CVE mapping for all released SSP.

13-Nov-2024 – Supplement 9-1 – Supplement 9-1 of this PCN corrects the description of Supplement 9 to mention correct SSP version.

21-Oct-2024 – Supplement 9 – Supplement 9 of this PCN introduces **Avaya Diagnostic Server 4.0 Security Service Pack SSP #9 (ADS_SAL_SLAMON_PM40_SSP_009_01.tar.gz**
PLDS ID - ADS40OVA009)

- ADS SSP #9 is only applicable to ADS/SAL 4.0 or later OVA deployed systems. It can be installed directly on 4.0 or later Service Pack/Feature Pack or on 4.0 or later Service Pack/Feature Pack that has an earlier SSP installed.
- Security Service Packs should NOT be applied on the Software Only offer.
- Reference the "Finding the installation instructions" section of this PCN for detailed installation instructions.
- Reference the "Security Information" section of this PCN for updates to the rpm and RHSAs for SSP #9.

21-Jun-2024 – Supplement 8 – Supplement 8 of this PCN introduces **Avaya Diagnostic Server 4.0 Security Service Pack SSP #8 (ADS_SAL_SLAMON_PM40_SSP_008_02.tar.gz**
PLDS ID - ADS40OVA008)

- ADS SSP #8 is only applicable to ADS/SAL 4.0 or later OVA deployed systems. It can be installed directly on 4.0 or later Service Pack/Feature Pack or on 4.0 or later Service Pack/Feature Pack that has an earlier SSP installed.
- Security Service Packs should NOT be applied on the Software Only offer.
- Reference the "Finding the installation instructions" section of this PCN for detailed installation instructions.
- Reference the "Security Information" section of this PCN for updates to the rpm and RHSAs for SSP #8.

16-Feb-2024 – Supplement 7 – Supplement 7 of this PCN introduces **Avaya Diagnostic Server 4.0 Security Service Pack SSP #7 (ADS_SAL_SLAMON_PM40_SSP_007_01.tar.gz**
PLDS ID - ADS40OVA007)

- ADS SSP #7 is only applicable to ADS/SAL 4.0 or later OVA deployed systems. It can be installed directly on 4.0 or later Service Pack/Feature Pack or on 4.0 or later Service Pack/Feature Pack that has an earlier SSP installed.
- Security Service Packs should NOT be applied on the Software Only offer.
- Reference the "Finding the installation instructions" section of this PCN for detailed installation instructions.
- Reference the "Security Information" section of this PCN for updates to the rpm and RHSAs for SSP #7.

6-Nov-2023 – Supplement 6-1 – Supplement 6-1 updates following notes for SSP#6.

- ADS SSP #6 is only applicable to ADS/SAL 4.0 or later OVA deployed systems. It can be installed directly on 4.0 or later Service Pack/Feature Pack or on 4.0 or later Service Pack/Feature Pack that has an earlier SSP installed.
- Security Service Packs should NOT be applied on the Software Only offer.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

- Reference the "Finding the installation instructions" section of this PCN for detailed installation instructions.
- Reference the "Security Information" section of this PCN for updates to the rpm and RHSAs for SSP #6.

27-Oct-2023 – Supplement 6 – Supplement 6 of this PCN introduces **Avaya Diagnostic Server 4.0 Security Service Pack SSP #6 (ADS_SAL_SLAMON_PM40_SSP_006_01.tar.gz PLDS ID - ADS40OVA006)**

17-Jul-2023 – Supplement 5-1 Supplement 5-1 updates "Important Notes" section.

30-June-2023 – Supplement 5 – Supplement 5 of this PCN introduces **Avaya Diagnostic Server 4.0 Security Service Pack SSP #5 (ADS_SAL_SLAMON_PM40_SSP_005_03.tar.gz PLDS ID - ADS40OVA005)**

15-January-2023 – Supplement 4 – Supplement 4 of this PCN introduces **Avaya Diagnostic Server 4.0 Security Service Pack SSP #4 (ADS_SAL_SLAMON_PM40_SSP_004_01.tar.gz PLDS ID - ADS40OVA04)**

21-October-2022 – Supplement 3 – Supplement 3 of this PCN introduces **Avaya Diagnostic Server 4.0 Security Service Pack SSP #3 (ADS_SAL_SLAMON_PM40_SSP_003_01.tar.gz PLDS ID - ADSOVA40003)**

04-August-2022 – Supplement 2-2 – Supplement 2-2 clarifies auto installation policy for Security Service Pack.

25-July-2022 – Supplement 2-1 – Supplement 2-1 corrects the steps required to install SSP.

7-July-2022 – Supplement 2 – Supplement 2 of this PCN introduces **Avaya Diagnostic Server 4.0 Security Service Pack SSP #2 (ADS_SAL_SLAMON_PM40_SSP_001_02.tar.gz PLDS ID - ADS40SP002)**

26-April-2022 – Supplement 1-1 – Supplement 1-1 corrects the AV_SSP_VERSION displayed after SSP#1 installation. The AV_SSP_VERSION displayed should be 001.

11-April-2022 – Supplement 1 – Supplement 1 of this PCN introduces **Avaya Diagnostic Server 4.0 Security Service Pack SSP #1 (ADS_SAL_SLAMON_PM40_SSP_001_01.tar.gz PLDS ID - ADSOVASP40)**

To determine that ADS/SAL OVA that is being run on your server you can:

- Log on to the ADS/SAL/SLAMon/PM console as admin user and run following command.

  For ADS-4.0 OVA

  ```
  [admin@linpubak025 ~]$ cat /etc/sysconfig/adsvm/release
  vapp.version=4.0.0.0
  vapp.build=11
  vapp.type=adsvapp
  ```

  For SAL-4.0 OVA

  ```
  [admin@linpubak025 ~]$ cat /etc/sysconfig/adsvm/release
  ```


© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

vapp.version=4.0.0.0
vapp.build=11
vapp.type=salvapp

- If the result of the final line indicates “adsvapp” or “salvapp” then this PCN and SSP is applicable. Otherwise, the SSP will not apply and the user will receive an error message “Product name mismatched”. The user will have to find the correct SSP to apply.
- If it is ADS software only solution, then /etc/sysconfig/adsvm/release file will not be present. For ADS software only solution (with customer provided OS), customer will be responsible to keep OS up to date to avoid security vulnerabilities.

IMPORTANT NOTE:

- Avaya Diagnostic Server 4.0 Security Service Pack 17 is applicable to ADS 4.0 OVA and SAL 4.0 OVA. Make sure you choose right SSP to install on your Virtual Appliance/OVA.
- Security Service Pack is not applicable to ADS 4.X Software Only or SAL Policy Manager 4.0 with SSH Proxy Software Only deployments.
- Avaya Diagnostic Server (ADS) 4.x OVA (Full-size) is applicable for the following applications: SAL Gateway 4.x, SLA Mon 4.x and Policy Manager 4.x.
- You can follow naming convention which will help to identify SSP to install – <ProductName><Version>_SSP_<SSP_Version>_<SSP_Build>
  ProductName – This will define the product for which the SSP is targeted
  Version – This will define the product version
  SSP_Version - This is a 3 digit number that defines the SSP version.
  SSP_Build - This is a 2 digit number that defines the build number of SSP
  (e.g. ADS_SAL_SLAMON_PM40_RHEL810_SSP_017_01.tar.gz)

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 Avaya Diagnostic Server 4.0 OVA or Secure Access Link 4.0 OVA release. Avaya Diagnostic Server (ADS) 4.x OVA (Full-size) which may include SAL Gateway 4.x, SLA Mon 4.x and SAL Policy Manager with SSH Proxy 4.x. Secure Access Link (SAL) 4.x OVA (small SAL OVA) which just includes SAL Gateway 4.x. This PCN is not applicable to ADS Software only solution.
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	This applies to both US and non-US customers.

© 2022-2026 Avaya LLC All Rights Reserved.
Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

both?	
Does applying this PCN disrupt my service during installation?	Activation of the Security Service Pack will disrupt the services since it requires a full system reboot of the ADS/SAL Virtual Machine (VM) to take effect. All active remote connections will be interrupted. SAL/SLAMon/Policy Manage WebUI will not be accessible. SLAMon agents will get disconnected from SLAMon server.
Installation of this PCN is required by:	Customer and/or Avaya Remote or On-Site Services and/or Avaya Authorized Business Partner.
Release notes and workarounds are located:	The Security Service Pack resolve vulnerabilities described by the Red Hat Security Advisories (RHSA) referenced in section 1B – Security information. Till Security Service Pack 9, Security Service Packs (SSP) were cumulative. This means that all fixes in previous 4.0.x SSPs are included in the most recent SSP. Please install OS Upgrade Bundle and then you can install Security Service Pack 17
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 ADS 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 ADS software updates, the installation instructions are required. To obtain the installation instructions please refer to the **Finding the installation instructions** section of this PCN.
How do I order this PCN (If PCN can be customer installed):	The Security Service Pack can be downloaded by performing the following steps from a browser: 1. Go to http://support.avaya.com then enter your **Username** and **Password** and select **LOG IN.** 2. Mouse over **Support by Product** at the top of the page, select **Downloads** in the menu. 3. Begin to type **Avaya Diagnostic Server** in the **Enter Product Name** box and when Avaya Diagnostic Server appears as a selection below, select it. 4. Select 4.0 from the **Choose Release** pull down menu to the right. 5. Scroll down if necessary and select **Avaya Diagnostic Server 4.0 SSP , 4.0.x.** 6. Scroll down the page to find the download link for the appropriate bin file. This link will take you to the PLDS system with the **Download pub ID** already entered. 7. This page also includes a link to this PCN. The MD5 sums are included in the Avaya Support and PLDS descriptions for the download files.

© 2022-2026 Avaya LLC All Rights Reserved.
Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

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

Important Security Service Pack Installation Notes:

- Security Service Packs were cumulative till the Security Service Pack #9. In other words, the current Security Service Pack for a release will include the fixes from all previous Security Service Packs (if available) for that release.
- For OS Upgrade Bundle, OS Upgrade Bundle is pre-requisite.

Avaya Diagnostic Server 4.0 Security Service Pack 16 is applicable to ADS 4.0 OVA or SAL 4.0 OVA.

Security Service Pack Installation instructions:

- Create a snapshot of ADS/SAL virtual machine.
  Note: This activity might impact the service.
  1. Click **Virtual Machines** in the VMware Host Client inventory.
  2. Right-click a virtual machine from the list and select **Snapshots** > **Take snapshot**.
  3. Enter a name for the snapshot.
  4. **(Optional)** Type a description for the snapshot.
  5. Select the **Snapshot the virtual machine's memory** check box to capture the memory of the virtual machine.
  6. Click **Take snapshot**.

Follow steps given below if you are downloading SSP from PLDS -

- Copy the Security Service Pack file to the ADS/SAL server at /home/admin account location.
- Log in to the ADS/SAL virtual machine using admin user and then switch to root user
- Verify md5sum of the bin file with the value mentioned in the support site.
  #md5sum ADS_SAL_SLAMON_PM40_RHEL810_SSP_017_01.tar.gz
- Extract SSP using following command –
  #tar -xzf ADS_SAL_SLAMON_PM40_RHEL810_SSP_017_01.tar.gz
- Run the patch installer using the following command:
  #./apply_ssp.sh AV-ADS4.0-RHEL8.x-SSP-017-01.tar.bz2
- Wait for the system to execute the security service pack.
- Please verify SSP installation logs to confirm successful patch installation at /var/log/avaya/
- Run following command to check SSP version –
  # /opt/avaya/common-os/bin/av-version

  OS_VERSION: Red Hat Enterprise Linux release 8.10 (Ootpa)
  AV_SSP_VERSION : 017
  AV_BUILD_NUMBER : 01
  AV_SSP_OS_VERSION : 8.10
  AV_OS_BUILD_NUMBER : 002

- Security service Pack requires a system reboot to take effect so **reboot** ADS/SAL virtual machine after SSP installation.

Follow steps given below if SSP is delivered through SAL Remote Package –
(Note - If you do not apply the service pack, and the auto update feature is enabled, system will automatically apply the service pack after 30 days of download. Please note that the system will also reboot the ADS VM to complete the update. This may impact the existing operations.)
If you want to manually install SSP, then follow steps given below.

- Login as a root user to ADS/SAL virtual machine

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

- As per received email notification, identify SSP download path and switch to that path - #cd /opt/avaya/SAL/gateway/SpiritAgent/persist/package-download/<directory_name>
- Run the patch installer using the following command: #./apply_ssp.sh AV-ADS4.0-RHEL8.x-SSP-017-01.tar.bz2
- Wait for the system to execute the security service pack.
- Please verify SSP installation logs to confirm successful patch installation at /var/log/avaya/
- Run following command to check SSP version –
  # /opt/avaya/common-os/bin/av-version

  OS_VERSION: Red Hat Enterprise Linux release 8.10 (Ootpa)
  AV_SSP_VERSION : 017
  AV_BUILD_NUMBER : 01
  AV_SSP_OS_VERSION : 8.10
  AV_OS_BUILD_NUMBER : 002

- Security service Pack requires a system reboot to take effect so **reboot** ADS/SAL virtual machine after SSP installation.

- Verify System functionality post system reboot and delete old VM snapshot post successful verification.
  1. Right-click the virtual machine and select Manage Snapshots.
     a. To locate a virtual machine, select a datacenter, folder, cluster, resource pool, host, or vApp.
     b. Click the VMs tab and click Virtual Machines.
  2. In the Snapshot Manager, click a snapshot to select it.
  3. Select whether to delete a single snapshot or all snapshots.
  4. Click Yes in the confirmation dialog box.
  5. Click Close to exit the Snapshot Manager.

Important Security Service Pack Installation Notes:

- Security Service Packs were cumulative till the Security Service Pack #9. In other words, the current Security Service Pack for a release will include the fixes from all previous Security Service Packs (if available) for that release.
- For Security Service Pack 17, OS Upgrade Bundle is pre-requisite.
- If someone tries to install different product's SSP on OVA, then SSP installation fails with error "Product name mismatched". Hence make sure, you select appropriate SSP as given in Description section.

SECTION 1A – SOFTWARE SERVICE PACK INFORMATION

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

How to verify To verify the successful installation of ADS Security Service Pack.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

the installation of the Service Pack has been successful:	• Log on to the ADS/SAL command line interface. • Run following command to check SSP version – # /opt/avaya/common-os/bin/av-version ---------- OS_VERSION: Red Hat Enterprise Linux release 8.10 (Ootpa) AV_SSP_VERSION : 017 AV_BUILD_NUMBER : 01 AV_SSP_OS_VERSION : 8.10 AV_OS_BUILD_NUMBER : 002 ----------
What you should do if the Service Pack installation fails?	• Open a Support Request with Avaya **Global Support Services (GSS)** or an Avaya authorized Business Partner if issue persists.
How to remove the Service Pack if malfunction of your system occurs:	N/A

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 as noted.
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.

Security Service Packs (SSP) are cumulative till SSP#9.
For SSP#16 installation, OS Upgrade Bundle should be installed first and then move ahead with SSP#16 installation.

ADS-4.0 OVA Security Service Pack 17 includes the following rpm updates:

bind-export-libs-32:9.11.36-18.el8_10.x86_64	kernel-tools-libs-4.18.0-553.181.1.el8_10.x86_64
glibc-2.28-251.el8_10.53.x86_64	kernel-tools-libs-4.18.0-553.182.1.el8_10.x86_64
glibc-all-langpacks-2.28-251.el8_10.53.x86_64	kernel-tools-libs-4.18.0-553.184.1.el8_10.x86_64
glibc-common-2.28-251.el8_10.53.x86_64	libXi-1.7.10-4.el8_10.x86_64
glibc-gconv-extra-2.28-251.el8_10.53.x86_64	libblkid-2.32.1-50.el8_10.x86_64
glibc-langpack-en-2.28-251.el8_10.53.x86_64	libfdisk-2.32.1-50.el8_10.x86_64
kernel-4.18.0-553.181.1.el8_10.x86_64	libmount-2.32.1-50.el8_10.x86_64
kernel-4.18.0-553.182.1.el8_10.x86_64	libnsl-2.28-251.el8_10.53.x86_64

© 2022-2026 Avaya LLC All Rights Reserved.
Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

kernel-4.18.0-553.184.1.el8_10.x86_64	libsmartcols-2.32.1-50.el8_10.x86_64
kernel-core-4.18.0-553.181.1.el8_10.x86_64	libuuid-2.32.1-50.el8_10.x86_64
kernel-core-4.18.0-553.182.1.el8_10.x86_64	python3-perf-4.18.0-553.181.1.el8_10.x86_64
kernel-core-4.18.0-553.184.1.el8_10.x86_64	python3-perf-4.18.0-553.182.1.el8_10.x86_64
kernel-modules-4.18.0-553.181.1.el8_10.x86_64	python3-perf-4.18.0-553.184.1.el8_10.x86_64
kernel-modules-4.18.0-553.182.1.el8_10.x86_64	qt5-qtbase-5.15.3-10.el8_10.x86_64
kernel-modules-4.18.0-553.184.1.el8_10.x86_64	qt5-qtbase-common-5.15.3-10.el8_10.noarch
kernel-tools-4.18.0-553.181.1.el8_10.x86_64	qt5-qtbase-gui-5.15.3-10.el8_10.x86_64
kernel-tools-4.18.0-553.182.1.el8_10.x86_64	qt5-qtdeclarative-5.15.3-3.el8_10.x86_64
kernel-tools-4.18.0-553.184.1.el8_10.x86_64	util-linux-2.32.1-50.el8_10.x86_64

Security vulnerabilities resolved in ADS 4.0 OVA OS Upgrade Bundle:

Updated Package	RHSA Number	CVE	RHSA Severity
kernel-4.18.0-553.182.1.el8_10.x86_64 kernel-core-4.18.0-553.182.1.el8_10.x86_64 kernel-modules-4.18.0-553.182.1.el8_10.x86_64 kernel-tools-4.18.0-553.182.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.182.1.el8_10.x86_64 python3-perf-4.18.0-553.182.1.el8_10.x86_64	RHSA-2026:93414	CVE-2026-98432	Critical/Sec.
kernel-4.18.0-553.181.1.el8_10.x86_64 kernel-core-4.18.0-553.181.1.el8_10.x86_64 kernel-modules-4.18.0-553.181.1.el8_10.x86_64 kernel-tools-4.18.0-553.181.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.181.1.el8_10.x86_64 python3-perf-4.18.0-553.181.1.el8_10.x86_64	RHSA-2026:93436	CVE-2026-63922 CVE-2026-63924 CVE-2026-64109 CVE-2026-72083 CVE-2026-74283 CVE-2026-93787	Important/Sec.
libXi-1.7.10-4.el8_10.x86_64	RHSA-2026:93438	CVE-2026-109089 CVE-2026-109090	Important/Sec.
qt5-qtbase-5.15.3-10.el8_10.x86_64 qt5-qtbase-common-5.15.3-10.el8_10.noarch qt5-qtbase-gui-5.15.3-10.el8_10.x86_64	RHSA-2026:93924	CVE-2026-11573 CVE-2026-19248	Important/Sec.
bind-export-libs-32:9.11.36-18.el8_10.x86_64	RHSA-2026:93925	CVE-2026-19630 CVE-2026-19662 CVE-2026-94300	Important/Sec.
kernel-4.18.0-553.184.1.el8_10.x86_64 kernel-core-4.18.0-553.184.1.el8_10.x86_64 kernel-modules-4.18.0-553.184.1.el8_10.x86_64 kernel-tools-4.18.0-553.184.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.184.1.el8_10.x86_64 python3-perf-4.18.0-553.184.1.el8_10.x86_64	RHSA-2026:95212	CVE-2026-52929 CVE-2026-64541 CVE-2026-74586 CVE-2026-80863 CVE-2026-80864 CVE-2026-89488	Important/Sec.
qt5-qtdeclarative-5.15.3-3.el8_10.x86_64	RHSA-2026:96075	CVE-2025-12385	Important/Sec.
glibc-2.28-251.el8_10.53.x86_64 glibc-all-langpacks-2.28-251.el8_10.53.x86_64 glibc-common-2.28-251.el8_10.53.x86_64 glibc-gconv-extra-2.28-251.el8_10.53.x86_64 glibc-langpack-en-2.28-251.el8_10.53.x86_64 libnsl-2.28-251.el8_10.53.x86_64	RHSA-2026:96087	CVE-2026-8674 CVE-2026-86805 CVE-2026-89092 CVE-2026-95818	Moderate/Sec.
libblkid-2.32.1-50.el8_10.x86_64	RHSA-202	CVE-2026-13595	Important/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

libfdisk-2.32.1-50.el8_10.x86_64 libmount-2.32.1-50.el8_10.x86_64 libsmartcols-2.32.1-50.el8_10.x86_64 libuuid-2.32.1-50.el8_10.x86_64 util-linux-2.32.1-50.el8_10.x86_64	6:96212	CVE-2026-53613 CVE-2026-53615	

ADS-4.0 OVA Security Service Pack 16 includes the following rpm updates:

expat-2.5.0-4.el8_10.x86_64	kernel-tools-4.18.0-553.174.1.el8_10.x86_64
kernel-4.18.0-553.169.1.el8_10.x86_64	kernel-tools-libs-4.18.0-553.174.1.el8_10.x86_64
kernel-core-4.18.0-553.169.1.el8_10.x86_64	python3-perf-4.18.0-553.174.1.el8_10.x86_64
kernel-modules-4.18.0-553.169.1.el8_10.x86_64	bind-export-libs-32:9.11.36-16.el8_10.7.x86_64
kernel-tools-4.18.0-553.169.1.el8_10.x86_64	libsoup-2.62.3-19.el8_10.x86_64
kernel-tools-libs-4.18.0-553.169.1.el8_10.x86_64	perl-URI-1.73-4.el8_10.noarch
python3-perf-4.18.0-553.169.1.el8_10.x86_64	platform-python-3.6.8-79.el8_10.x86_64
gawk-4.2.1-5.el8_10.x86_64	platform-python-devel-3.6.8-79.el8_10.x86_64
kernel-4.18.0-553.170.1.el8_10.x86_64	python3-libs-3.6.8-79.el8_10.x86_64
kernel-core-4.18.0-553.170.1.el8_10.x86_64	bubblewrap-0.4.0-3.el8_10.x86_64
kernel-modules-4.18.0-553.170.1.el8_10.x86_64	libarchive-3.3.3-7.el8_10.x86_64
kernel-tools-4.18.0-553.170.1.el8_10.x86_64	kernel-4.18.0-553.176.1.el8_10.x86_64
kernel-tools-libs-4.18.0-553.170.1.el8_10.x86_64	kernel-core-4.18.0-553.176.1.el8_10.x86_64
python3-perf-4.18.0-553.170.1.el8_10.x86_64	kernel-modules-4.18.0-553.176.1.el8_10.x86_64
sudo-1.9.5p2-2.el8_10.x86_64	kernel-tools-4.18.0-553.176.1.el8_10.x86_64
mariadb-connector-c-3.1.11-3.el8_10.x86_64	kernel-tools-libs-4.18.0-553.176.1.el8_10.x86_64
mariadb-connector-c-config-3.1.11-3.el8_10.noarch	python3-perf-4.18.0-553.176.1.el8_10.x86_64
kernel-4.18.0-553.171.1.el8_10.x86_64	openssl-1:1.1.1k-18.el8_6.x86_64
kernel-core-4.18.0-553.171.1.el8_10.x86_64	openssl-libs-1:1.1.1k-18.el8_6.x86_64
kernel-modules-4.18.0-553.171.1.el8_10.x86_64	openssl-perl-1:1.1.1k-18.el8_6.x86_64
kernel-tools-4.18.0-553.171.1.el8_10.x86_64	librsvg2-2.42.7-6.el8_10.x86_64
kernel-tools-libs-4.18.0-553.171.1.el8_10.x86_64	kernel-4.18.0-553.177.1.el8_10.x86_64
python3-perf-4.18.0-553.171.1.el8_10.x86_64	kernel-core-4.18.0-553.177.1.el8_10.x86_64
libpcap-14:1.9.1-6.el8_10.x86_64	kernel-modules-4.18.0-553.177.1.el8_10.x86_64
libnghttp2-1.33.0-6.el8_10.2.x86_64	kernel-tools-4.18.0-553.177.1.el8_10.x86_64
glibc-2.28-251.el8_10.43.x86_64	kernel-tools-libs-4.18.0-553.177.1.el8_10.x86_64
glibc-all-langpacks-2.28-251.el8_10.43.x86_64	python3-perf-4.18.0-553.177.1.el8_10.x86_64
glibc-common-2.28-251.el8_10.43.x86_64	openssh-8.0p1-34.el8_10.x86_64
glibc-gconv-extra-2.28-251.el8_10.43.x86_64	openssh-clients-8.0p1-34.el8_10.x86_64
glibc-langpack-en-2.28-251.el8_10.43.x86_64	openssh-server-8.0p1-34.el8_10.x86_64
libnsl-2.28-251.el8_10.43.x86_64	java-17-openjdk-1:17.0.21.0.9-2.1.el8.x86_64
vim-minimal-2:8.0.1763-32.el8_10.x86_64	java-17-openjdk-headless-1:17.0.21.0.9-2.1.el8.x86_64
kernel-4.18.0-553.172.1.el8_10.x86_64	ca-certificates-2026.2.92_v9.0.319-81.3.el8_10.noarch
kernel-core-4.18.0-553.172.1.el8_10.x86_64	giflib-5.1.4-4.el8_10.x86_64
kernel-modules-4.18.0-553.172.1.el8_10.x86_64	kernel-4.18.0-553.178.1.el8_10.x86_64
kernel-tools-4.18.0-553.172.1.el8_10.x86_64	kernel-core-4.18.0-553.178.1.el8_10.x86_64
kernel-tools-libs-4.18.0-553.172.1.el8_10.x86_64	kernel-modules-4.18.0-553.178.1.el8_10.x86_64
python3-perf-4.18.0-553.172.1.el8_10.x86_64	kernel-tools-4.18.0-553.178.1.el8_10.x86_64
kbd-2.0.4-11.el8_10.1.x86_64	kernel-tools-libs-4.18.0-553.178.1.el8_10.x86_64
kbd-legacy-2.0.4-11.el8_10.1.noarch	python3-perf-4.18.0-553.178.1.el8_10.x86_64
kbd-misc-2.0.4-11.el8_10.1.noarch	libX11-1.6.8-10.el8_10.x86_64
bind-export-libs-32:9.11.36-16.el8_10.16.x86_64	libX11-common-1.6.8-10.el8_10.noarch
compat-openssl10-1:1.0.2o-4.el8_10.4.x86_64	libX11-xcb-1.6.8-10.el8_10.x86_64

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

libxml2-2.9.7-21.el8_10.10.x86_64	kernel-4.18.0-553.179.1.el8_10.x86_64
python3-libxml2-2.9.7-21.el8_10.10.x86_64	kernel-core-4.18.0-553.179.1.el8_10.x86_64
glibc-2.28-251.el8_10.48.x86_64	kernel-modules-4.18.0-553.179.1.el8_10.x86_64
glibc-all-langpacks-2.28-251.el8_10.48.x86_64	kernel-tools-4.18.0-553.179.1.el8_10.x86_64
glibc-common-2.28-251.el8_10.48.x86_64	kernel-tools-libs-4.18.0-553.179.1.el8_10.x86_64
glibc-gconv-extra-2.28-251.el8_10.48.x86_64	python3-perf-4.18.0-553.179.1.el8_10.x86_64
glibc-langpack-en-2.28-251.el8_10.48.x86_64	libgcc-8.5.0-30.el8_10.x86_64
libnsl-2.28-251.el8_10.48.x86_64	libgfortran-8.5.0-30.el8_10.x86_64
rsyslog-8.2102.0-15.el8_10.3.x86_64	libgomp-8.5.0-30.el8_10.x86_64
rsyslog-gnutls-8.2102.0-15.el8_10.3.x86_64	libquadmath-8.5.0-30.el8_10.x86_64
pcre2-10.32-4.el8_10.x86_64	libstdc++-8.5.0-30.el8_10.x86_64
pcre2-utf16-10.32-4.el8_10.x86_64	brotli-1.0.6-5.el8_10.x86_64
kernel-4.18.0-553.173.1.el8_10.x86_64	libXrender-0.9.10-8.el8_10.x86_64
kernel-core-4.18.0-553.173.1.el8_10.x86_64	libXi-1.7.10-2.el8_10.x86_64
kernel-modules-4.18.0-553.173.1.el8_10.x86_64	libXtst-1.2.3-8.el8_10.x86_64
kernel-tools-4.18.0-553.173.1.el8_10.x86_64	kernel-4.18.0-553.180.1.el8_10.x86_64
kernel-tools-libs-4.18.0-553.173.1.el8_10.x86_64	kernel-core-4.18.0-553.180.1.el8_10.x86_64
python3-perf-4.18.0-553.173.1.el8_10.x86_64	kernel-modules-4.18.0-553.180.1.el8_10.x86_64
kernel-4.18.0-553.174.1.el8_10.x86_64	kernel-tools-4.18.0-553.180.1.el8_10.x86_64
kernel-core-4.18.0-553.174.1.el8_10.x86_64	kernel-tools-libs-4.18.0-553.180.1.el8_10.x86_64
kernel-modules-4.18.0-553.174.1.el8_10.x86_64	python3-perf-4.18.0-553.180.1.el8_10.x86_64

Security vulnerabilities resolved in ADS 4.0 OVA OS Upgrade Bundle:

Updated Package	RHSA Number	CVE	RHSA Severity
expat-2.5.0-4.el8_10.x86_64	RHSA-2026:72448	CVE-2026-66046 CVE-2026-93990	Important/Sec.
kernel-4.18.0-553.169.1.el8_10.x86_64 kernel-core-4.18.0-553.169.1.el8_10.x86_64 kernel-modules-4.18.0-553.169.1.el8_10.x86_64 kernel-tools-4.18.0-553.169.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.169.1.el8_10.x86_64 python3-perf-4.18.0-553.169.1.el8_10.x86_64	RHSA-2026:72468	CVE-2025-40323 CVE-2026-45942 CVE-2026-46199 CVE-2026-46204 CVE-2026-46230 CVE-2026-63875 CVE-2026-64034 CVE-2026-64556 CVE-2026-68155 CVE-2026-68156 CVE-2026-68159 CVE-2026-68273 CVE-2026-74753	Important/Sec.
gawk-4.2.1-5.el8_10.x86_64	RHSA-2026:73511	CVE-2026-40467 CVE-2026-40468	Moderate/Sec.
kernel-4.18.0-553.170.1.el8_10.x86_64 kernel-core-4.18.0-553.170.1.el8_10.x86_64 kernel-modules-4.18.0-553.170.1.el8_10.x86_64 kernel-tools-4.18.0-553.170.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.170.1.el8_10.x86_64 python3-perf-4.18.0-553.170.1.el8_10.x86_64	RHSA-2026:74133	CVE-2026-64102 CVE-2026-68299 CVE-2026-72099 CVE-2026-72329	Moderate/Sec.
sudo-1.9.5p2-2.el8_10.x86_64	RHSA-202	CVE-2026-96512	Important/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

	6:75580		
mariadb-connector-c-3.1.11-3.el8_10.x86_64 mariadb-connector-c-config-3.1.11-3.el8_10.noarch	RHSA-2026:75674	CVE-2026-44172	Important/Sec.
kernel-4.18.0-553.171.1.el8_10.x86_64 kernel-core-4.18.0-553.171.1.el8_10.x86_64 kernel-modules-4.18.0-553.171.1.el8_10.x86_64 kernel-tools-4.18.0-553.171.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.171.1.el8_10.x86_64 python3-perf-4.18.0-553.171.1.el8_10.x86_64	RHSA-2026:75747	CVE-2022-50756 CVE-2023-54048 CVE-2025-39994 CVE-2025-40242 CVE-2026-23105 CVE-2026-45856 CVE-2026-45861 CVE-2026-46319 CVE-2026-52972 CVE-2026-53049 CVE-2026-53230 CVE-2026-53270 CVE-2026-63794 CVE-2026-63829 CVE-2026-63992 CVE-2026-63994 CVE-2026-68432 CVE-2026-72052 CVE-2026-72255 CVE-2026-74516 CVE-2026-74569 CVE-2026-74669 CVE-2026-74744 CVE-2026-74746 CVE-2026-80921 CVE-2026-89481 CVE-2026-89972 CVE-2026-90227 CVE-2026-97417	Important/Sec.
libpcap-14:1.9.1-6.el8_10.x86_64	RHSA-2026:76045	CVE-2026-0799	Important/Sec.
glibc-2.28-251.el8_10.43.x86_64 glibc-all-langpacks-2.28-251.el8_10.43.x86_64 glibc-common-2.28-251.el8_10.43.x86_64 glibc-gconv-extra-2.28-251.el8_10.43.x86_64 glibc-langpack-en-2.28-251.el8_10.43.x86_64 libnsl-2.28-251.el8_10.43.x86_64	RHSA-2026:76777	CVE-2026-6368 CVE-2026-6791	Moderate/Sec.
vim-minimal-2:8.0.1763-32.el8_10.x86_64	RHSA-2026:77359	CVE-2026-73073	Important/Sec.
kernel-4.18.0-553.172.1.el8_10.x86_64 kernel-core-4.18.0-553.172.1.el8_10.x86_64 kernel-modules-4.18.0-553.172.1.el8_10.x86_64 kernel-tools-4.18.0-553.172.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.172.1.el8_10.x86_64 python3-perf-4.18.0-553.172.1.el8_10.x86_64	RHSA-2026:77498	CVE-2026-64115 CVE-2026-74582 CVE-2026-89530	Important/Sec.
kbd-2.0.4-11.el8_10.1.x86_64	RHSA-202	CVE-2026-72693	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

kbd-legacy-2.0.4-11.el8_10.1.noarch kbd-misc-2.0.4-11.el8_10.1.noarch	6:78951		
bind-export-libs-32:9.11.36-16.el8_10.16.x86_64	RHSA-202 6:79162	CVE-2026-19666 CVE-2026-19667 CVE-2026-80274	Important/Sec.
compat-openssl10-1:1.0.2o-4.el8_10.4.x86_64	RHSA-202 6:80510	CVE-2026-84782	Important/Sec.
libxml2-2.9.7-21.el8_10.10.x86_64 python3-libxml2-2.9.7-21.el8_10.10.x86_64	RHSA-202 6:80675	CVE-2026-86142	Moderate/Sec.
glibc-2.28-251.el8_10.48.x86_64 glibc-all-langpacks-2.28-251.el8_10.48.x86_64 glibc-common-2.28-251.el8_10.48.x86_64 glibc-gconv-extra-2.28-251.el8_10.48.x86_64 glibc-langpack-en-2.28-251.el8_10.48.x86_64 libnsl-2.28-251.el8_10.48.x86_64	RHSA-202 6:80798	CVE-2026-18374 CVE-2026-19542 CVE-2026-77117 CVE-2026-80489	Moderate/Sec.
rsyslog-8.2102.0-15.el8_10.3.x86_64 rsyslog-gnutls-8.2102.0-15.el8_10.3.x86_64	RHSA-202 6:80817	CVE-2026-19654 CVE-2026-78002	Important/Sec.
pcre2-10.32-4.el8_10.x86_64 pcre2-utf16-10.32-4.el8_10.x86_64	RHSA-202 6:81613	CVE-2026-103111 CVE-2026-86145 CVE-2026-89157 CVE-2026-89158	Important/Sec.
kernel-4.18.0-553.173.1.el8_10.x86_64 kernel-core-4.18.0-553.173.1.el8_10.x86_64 kernel-modules-4.18.0-553.173.1.el8_10.x86_64 kernel-tools-4.18.0-553.173.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.173.1.el8_10.x86_64 python3-perf-4.18.0-553.173.1.el8_10.x86_64	RHSA-202 6:82807	CVE-2026-31678 CVE-2026-63920 CVE-2026-68108 CVE-2026-68236 CVE-2026-68278 CVE-2026-68409 CVE-2026-72318 CVE-2026-80887 CVE-2026-89811	Important/Sec.
kernel-4.18.0-553.174.1.el8_10.x86_64 kernel-core-4.18.0-553.174.1.el8_10.x86_64 kernel-modules-4.18.0-553.174.1.el8_10.x86_64 kernel-tools-4.18.0-553.174.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.174.1.el8_10.x86_64 python3-perf-4.18.0-553.174.1.el8_10.x86_64	RHSA-202 6:83157	CVE-2026-68377 CVE-2026-72262 CVE-2026-74583 CVE-2026-74641 CVE-2026-74705 CVE-2026-89526 CVE-2026-90036 CVE-2026-93228 CVE-2026-93262	Important/Sec.
libsoup-2.62.3-19.el8_10.x86_64	RHSA-202 6:84586	CVE-2026-102556 CVE-2026-102557 CVE-2026-102558 CVE-2026-102559	Important/Sec.
perl-URI-1.73-4.el8_10.noarch	RHSA-202 6:84590	CVE-2026-19953	Moderate/Sec.
platform-python-3.6.8-79.el8_10.x86_64 platform-python-devel-3.6.8-79.el8_10.x86_64 python3-libs-3.6.8-79.el8_10.x86_64	RHSA-202 6:85239	CVE-2026-12345 CVE-2026-19445 CVE-2026-19553	Important/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

bubblewrap-0.4.0-3.el8_10.x86_64	RHSA-2026:85306	CVE-2026-87766	Important/Sec.
kernel-4.18.0-553.176.1.el8_10.x86_64 kernel-core-4.18.0-553.176.1.el8_10.x86_64 kernel-modules-4.18.0-553.176.1.el8_10.x86_64 kernel-tools-4.18.0-553.176.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.176.1.el8_10.x86_64 python3-perf-4.18.0-553.176.1.el8_10.x86_64	RHSA-2026:85773	CVE-2026-52935 CVE-2026-53196 CVE-2026-74588 CVE-2026-74752 CVE-2026-89479 CVE-2026-89631 CVE-2026-93288 CVE-2026-93817 CVE-2026-98320	Important/Sec.
openssl-1:1.1.1k-18.el8_6.x86_64 openssl-libs-1:1.1.1k-18.el8_6.x86_64 openssl-perl-1:1.1.1k-18.el8_6.x86_64	RHSA-2026:85968	CVE-2026-63072 CVE-2026-84782	Important/Sec.
librsvg2-2.42.7-6.el8_10.x86_64	RHSA-2026:86842		Important/Sec.
kernel-4.18.0-553.177.1.el8_10.x86_64 kernel-core-4.18.0-553.177.1.el8_10.x86_64 kernel-modules-4.18.0-553.177.1.el8_10.x86_64 kernel-tools-4.18.0-553.177.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.177.1.el8_10.x86_64 python3-perf-4.18.0-553.177.1.el8_10.x86_64	RHSA-2026:87375	CVE-2026-64114 CVE-2026-64266 CVE-2026-64572 CVE-2026-68202 CVE-2026-80536 CVE-2026-80590 CVE-2026-89777	Important/Sec.
openssh-8.0p1-34.el8_10.x86_64 openssh-clients-8.0p1-34.el8_10.x86_64 openssh-server-8.0p1-34.el8_10.x86_64	RHSA-2026:88211	CVE-2026-59997 CVE-2026-59998 CVE-2026-60000 CVE-2026-60001 CVE-2026-73283	Moderate/Sec.
java-17-openjdk-1:17.0.21.0.9-2.1.el8.x86_64 java-17-openjdk-headless-1:17.0.21.0.9-2.1.el8.x86_64	RHSA-2026:88352	CVE-2026-101516 CVE-2026-83374 CVE-2026-83376 CVE-2026-83380 CVE-2026-83381 CVE-2026-83387 CVE-2026-83395 CVE-2026-83400 CVE-2026-87290 CVE-2026-87292 CVE-2026-87294 CVE-2026-87367 CVE-2026-91332 CVE-2026-91334 CVE-2026-91335 CVE-2026-91373 CVE-2026-91374 CVE-2026-91375 CVE-2026-91379 CVE-2026-91380 CVE-2026-91382 CVE-2026-91394 CVE-2026-91397	Important/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

		CVE-2026-91398 CVE-2026-91400 CVE-2026-91410 CVE-2026-91415 CVE-2026-91418 CVE-2026-91451 CVE-2026-91452 CVE-2026-91453 CVE-2026-91461 CVE-2026-91462 CVE-2026-91463 CVE-2026-91464 CVE-2026-91487	
ca-certificates-2026.2.92_v9.0.319-81.3.el8_10.noarch	RHSA-2026:88550	CVE-2026-114406	Critical/Sec.
kernel-4.18.0-553.178.1.el8_10.x86_64 kernel-core-4.18.0-553.178.1.el8_10.x86_64 kernel-modules-4.18.0-553.178.1.el8_10.x86_64 kernel-tools-4.18.0-553.178.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.178.1.el8_10.x86_64 python3-perf-4.18.0-553.178.1.el8_10.x86_64	RHSA-2026:89083	CVE-2026-53236 CVE-2026-53388 CVE-2026-64378 CVE-2026-68136 CVE-2026-68138 CVE-2026-68140 CVE-2026-68338 CVE-2026-68476 CVE-2026-80586 CVE-2026-80824 CVE-2026-81003 CVE-2026-89638 CVE-2026-99999	Important/Sec.
libX11-1.6.8-10.el8_10.x86_64 libX11-common-1.6.8-10.el8_10.noarch libX11-xcb-1.6.8-10.el8_10.x86_64	RHSA-2026:89730	CVE-2026-88806	Important/Sec.
kernel-4.18.0-553.179.1.el8_10.x86_64 kernel-core-4.18.0-553.179.1.el8_10.x86_64 kernel-modules-4.18.0-553.179.1.el8_10.x86_64 kernel-tools-4.18.0-553.179.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.179.1.el8_10.x86_64 python3-perf-4.18.0-553.179.1.el8_10.x86_64	RHSA-2026:89816	CVE-2026-74515	Moderate/Sec.
libgcc-8.5.0-30.el8_10.x86_64 libgfortran-8.5.0-30.el8_10.x86_64 libgomp-8.5.0-30.el8_10.x86_64 libquadmath-8.5.0-30.el8_10.x86_64 libstdc++-8.5.0-30.el8_10.x86_64	RHSA-2026:89830	CVE-2026-102010 CVE-2026-95619	Moderate/Sec.
brotli-1.0.6-5.el8_10.x86_64	RHSA-2026:90501	CVE-2026-111497	Important/Sec.
libXrender-0.9.10-8.el8_10.x86_64	RHSA-2026:91267	CVE-2026-88807	Important/Sec.
libXi-1.7.10-2.el8_10.x86_64	RHSA-2026:91268	CVE-2026-93543	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

libXtst-1.2.3-8.el8_10.x86_64	RHSA-2026:91294	CVE-2026-94286	Important/Sec.
kernel-4.18.0-553.180.1.el8_10.x86_64 kernel-core-4.18.0-553.180.1.el8_10.x86_64 kernel-modules-4.18.0-553.180.1.el8_10.x86_64 kernel-tools-4.18.0-553.180.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.180.1.el8_10.x86_64 python3-perf-4.18.0-553.180.1.el8_10.x86_64	RHSA-2026:92209	CVE-2026-72288 CVE-2026-72289 CVE-2026-90011 CVE-2026-98222	Important/Sec.
expat-2.5.0-6.el8_10.x86_64	RHSA-2026:92323	CVE-2026-102633 CVE-2026-77214	Important/Sec.
curl-7.61.1-34.el8_10.18.x86_64 libcurl-7.61.1-34.el8_10.18.x86_64	RHSA-2026:92368	CVE-2026-11856 CVE-2026-8458 CVE-2026-8924 CVE-2026-8927 CVE-2026-8932	Important/Sec.

ADS-4.0 OVA Security Service Pack 15 includes the following rpm updates:

acl-2.4.0-1.el8_10.x86_64	kernel-tools-4.18.0-553.154.1.el8_10.x86_64
bind-export-libs-32:9.11.36-16.el8_10.14.x86_64	kernel-tools-4.18.0-553.155.1.el8_10.x86_64
compat-openssl10-1:1.0.2o-4.el8_10.3.x86_64	kernel-tools-4.18.0-553.156.1.el8_10.x86_64
coreutils-8.30-21.el8_10.x86_64	kernel-tools-4.18.0-553.157.1.el8_10.x86_64
coreutils-common-8.30-21.el8_10.x86_64	kernel-tools-4.18.0-553.158.1.el8_10.x86_64
cups-libs-1:2.2.6-68.el8_10.x86_64	kernel-tools-4.18.0-553.159.1.el8_10.x86_64
curl-7.61.1-34.el8_10.13.x86_64	kernel-tools-4.18.0-553.160.1.el8_10.x86_64
dracut-049-246.git20260728.el8_10.x86_64	kernel-tools-4.18.0-553.162.1.el8_10.x86_64
dracut-config-rescue-049-246.git20260728.el8_10.x86_64	kernel-tools-4.18.0-553.163.1.el8_10.x86_64
	kernel-tools-4.18.0-553.164.1.el8_10.x86_64
dracut-network-049-246.git20260728.el8_10.x86_64	kernel-tools-4.18.0-553.166.1.el8_10.x86_64
dracut-squash-049-246.git20260728.el8_10.x86_64	kernel-tools-4.18.0-553.167.1.el8_10.x86_64
expat-2.5.0-2.el8_10.2.x86_64	kernel-tools-4.18.0-553.168.1.el8_10.x86_64
giflib-5.1.4-5.el8_10.x86_64	kernel-tools-libs-4.18.0-553.139.1.el8_10.x86_64
glib2-2.56.4-170.el8_10.x86_64	kernel-tools-libs-4.18.0-553.140.1.el8_10.x86_64
glib2-2.56.4-177.el8_10.x86_64	kernel-tools-libs-4.18.0-553.141.1.el8_10.x86_64
glib2-2.56.4-178.el8_10.x86_64	kernel-tools-libs-4.18.0-553.143.1.el8_10.x86_64
glibc-2.28-251.el8_10.38.x86_64	kernel-tools-libs-4.18.0-553.144.1.el8_10.x86_64
glibc-2.28-251.el8_10.40.x86_64	kernel-tools-libs-4.18.0-553.146.1.el8_10.x86_64
glibc-all-langpacks-2.28-251.el8_10.38.x86_64	kernel-tools-libs-4.18.0-553.147.1.el8_10.x86_64
glibc-all-langpacks-2.28-251.el8_10.40.x86_64	kernel-tools-libs-4.18.0-553.148.1.el8_10.x86_64
glibc-common-2.28-251.el8_10.38.x86_64	kernel-tools-libs-4.18.0-553.150.1.el8_10.x86_64
glibc-common-2.28-251.el8_10.40.x86_64	kernel-tools-libs-4.18.0-553.151.1.el8_10.x86_64
glibc-gconv-extra-2.28-251.el8_10.38.x86_64	kernel-tools-libs-4.18.0-553.153.1.el8_10.x86_64
glibc-gconv-extra-2.28-251.el8_10.40.x86_64	kernel-tools-libs-4.18.0-553.154.1.el8_10.x86_64
glibc-langpack-en-2.28-251.el8_10.38.x86_64	kernel-tools-libs-4.18.0-553.155.1.el8_10.x86_64
glibc-langpack-en-2.28-251.el8_10.40.x86_64	kernel-tools-libs-4.18.0-553.156.1.el8_10.x86_64
gstreamer1-plugins-bad-free-1.16.1-8.el8_10.x86_64	kernel-tools-libs-4.18.0-553.157.1.el8_10.x86_64
gstreamer1-plugins-bad-free-1.16.1-9.el8_10.1.x86_64	kernel-tools-libs-4.18.0-553.158.1.el8_10.x86_64
gstreamer1-plugins-bad-free-1.16.1-9.el8_10.2.x86_64	kernel-tools-libs-4.18.0-553.159.1.el8_10.x86_64
gstreamer1-plugins-base-1.16.1-6.el8_10.1.x86_64	kernel-tools-libs-4.18.0-553.160.1.el8_10.x86_64
gstreamer1-plugins-base-1.16.1-7.el8_10.x86_64	kernel-tools-libs-4.18.0-553.162.1.el8_10.x86_64

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

gzip-1.9-15.el8_10.x86_64	kernel-tools-libs-4.18.0-553.163.1.el8_10.x86_64
java-1.8.0-openjdk-1:1.8.0.502.b07-1.1.el8.x86_64	kernel-tools-libs-4.18.0-553.164.1.el8_10.x86_64
java-1.8.0-openjdk-1:1.8.0.504.b01-1.1.el8.x86_64	kernel-tools-libs-4.18.0-553.166.1.el8_10.x86_64
java-1.8.0-openjdk-headless-1:1.8.0.502.b07-1.1.el8.x86_64	kernel-tools-libs-4.18.0-553.167.1.el8_10.x86_64
	kernel-tools-libs-4.18.0-553.168.1.el8_10.x86_64
java-1.8.0-openjdk-headless-1:1.8.0.504.b01-1.1.el8.x86_64	libacl-2.4.0-1.el8_10.x86_64
	libattr-2.6.0-1.el8_10.x86_64
java-17-openjdk-1:17.0.20.0.8-1.1.el8.x86_64	libcurl-7.61.1-34.el8_10.13.x86_64
java-17-openjdk-1:17.0.20.1.1-1.1.el8.x86_64	libevent-2.1.8-11.el8_10.x86_64
java-17-openjdk-headless-1:17.0.20.0.8-1.1.el8.x86_64	libgcrypt-1.8.5-8.el8_10.x86_64
java-17-openjdk-headless-1:17.0.20.1.1-1.1.el8.x86_64	libkcapi-1.4.0-3.el8_10.x86_64
kernel-4.18.0-553.139.1.el8_10.x86_64	libkcapi-hmaccalc-1.4.0-3.el8_10.x86_64
kernel-4.18.0-553.140.1.el8_10.x86_64	libnghttp2-1.33.0-6.el8_10.3.x86_64
kernel-4.18.0-553.141.1.el8_10.x86_64	libnsl-2.28-251.el8_10.38.x86_64
kernel-4.18.0-553.143.1.el8_10.x86_64	libnsl-2.28-251.el8_10.40.x86_64
kernel-4.18.0-553.144.1.el8_10.x86_64	libpng-2:1.6.34-11.el8_10.x86_64
kernel-4.18.0-553.146.1.el8_10.x86_64	libsolv-0.7.20-7.el8_10.x86_64
kernel-4.18.0-553.147.1.el8_10.x86_64	libsoup-2.62.3-15.el8_10.x86_64
kernel-4.18.0-553.148.1.el8_10.x86_64	libssh-0.9.6-17.el8_10.x86_64
kernel-4.18.0-553.150.1.el8_10.x86_64	libssh-config-0.9.6-17.el8_10.noarch
kernel-4.18.0-553.151.1.el8_10.x86_64	libtasn1-4.13-6.el8_10.x86_64
kernel-4.18.0-553.153.1.el8_10.x86_64	libtiff-4.0.9-38.el8_10.x86_64
kernel-4.18.0-553.154.1.el8_10.x86_64	libtiff-4.0.9-39.el8_10.x86_64
kernel-4.18.0-553.155.1.el8_10.x86_64	libxml2-2.9.7-21.el8_10.6.x86_64
kernel-4.18.0-553.156.1.el8_10.x86_64	libxml2-2.9.7-21.el8_10.7.x86_64
kernel-4.18.0-553.157.1.el8_10.x86_64	libxml2-2.9.7-21.el8_10.8.x86_64
kernel-4.18.0-553.158.1.el8_10.x86_64	libxml2-2.9.7-21.el8_10.9.x86_64
kernel-4.18.0-553.159.1.el8_10.x86_64	microcode_ctl-4:20260812-1.el8_10.x86_64
kernel-4.18.0-553.160.1.el8_10.x86_64	openssh-8.0p1-30.el8_10.x86_64
kernel-4.18.0-553.162.1.el8_10.x86_64	openssh-8.0p1-33.el8_10.x86_64
kernel-4.18.0-553.163.1.el8_10.x86_64	openssh-clients-8.0p1-30.el8_10.x86_64
kernel-4.18.0-553.164.1.el8_10.x86_64	openssh-clients-8.0p1-33.el8_10.x86_64
kernel-4.18.0-553.166.1.el8_10.x86_64	openssh-server-8.0p1-30.el8_10.x86_64
kernel-4.18.0-553.167.1.el8_10.x86_64	openssh-server-8.0p1-33.el8_10.x86_64
kernel-4.18.0-553.168.1.el8_10.x86_64	openssl-1:1.1.1k-17.el8_6.x86_64
kernel-core-4.18.0-553.139.1.el8_10.x86_64	openssl-libs-1:1.1.1k-17.el8_6.x86_64
kernel-core-4.18.0-553.140.1.el8_10.x86_64	openssl-perl-1:1.1.1k-17.el8_6.x86_64
kernel-core-4.18.0-553.141.1.el8_10.x86_64	pam-1.3.1-40.el8_10.x86_64
kernel-core-4.18.0-553.143.1.el8_10.x86_64	perl-Errno-1.28-423.el8_10.1.x86_64
kernel-core-4.18.0-553.144.1.el8_10.x86_64	perl-IO-1.38-423.el8_10.1.x86_64
kernel-core-4.18.0-553.146.1.el8_10.x86_64	perl-SelfLoader-1.23-423.el8_10.1.noarch
kernel-core-4.18.0-553.147.1.el8_10.x86_64	perl-interpreter-4:5.26.3-423.el8_10.1.x86_64
kernel-core-4.18.0-553.148.1.el8_10.x86_64	perl-libs-4:5.26.3-423.el8_10.1.x86_64
kernel-core-4.18.0-553.150.1.el8_10.x86_64	perl-macros-4:5.26.3-423.el8_10.1.x86_64
kernel-core-4.18.0-553.151.1.el8_10.x86_64	platform-python-3.6.8-77.el8_10.x86_64
kernel-core-4.18.0-553.153.1.el8_10.x86_64	platform-python-3.6.8-78.el8_10.x86_64
kernel-core-4.18.0-553.154.1.el8_10.x86_64	platform-python-devel-3.6.8-77.el8_10.x86_64
kernel-core-4.18.0-553.155.1.el8_10.x86_64	platform-python-devel-3.6.8-78.el8_10.x86_64
kernel-core-4.18.0-553.156.1.el8_10.x86_64	python3-libs-3.6.8-77.el8_10.x86_64
kernel-core-4.18.0-553.157.1.el8_10.x86_64	python3-libs-3.6.8-78.el8_10.x86_64
kernel-core-4.18.0-553.158.1.el8_10.x86_64	python3-libxml2-2.9.7-21.el8_10.6.x86_64
kernel-core-4.18.0-553.159.1.el8_10.x86_64	python3-libxml2-2.9.7-21.el8_10.7.x86_64

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

kernel-core-4.18.0-553.160.1.el8_10.x86_64	python3-libxml2-2.9.7-21.el8_10.8.x86_64
kernel-core-4.18.0-553.162.1.el8_10.x86_64	python3-libxml2-2.9.7-21.el8_10.9.x86_64
kernel-core-4.18.0-553.163.1.el8_10.x86_64	python3-perf-4.18.0-553.139.1.el8_10.x86_64
kernel-core-4.18.0-553.164.1.el8_10.x86_64	python3-perf-4.18.0-553.140.1.el8_10.x86_64
kernel-core-4.18.0-553.166.1.el8_10.x86_64	python3-perf-4.18.0-553.141.1.el8_10.x86_64
kernel-core-4.18.0-553.167.1.el8_10.x86_64	python3-perf-4.18.0-553.143.1.el8_10.x86_64
kernel-core-4.18.0-553.168.1.el8_10.x86_64	python3-perf-4.18.0-553.144.1.el8_10.x86_64
kernel-modules-4.18.0-553.139.1.el8_10.x86_64	python3-perf-4.18.0-553.146.1.el8_10.x86_64
kernel-modules-4.18.0-553.140.1.el8_10.x86_64	python3-perf-4.18.0-553.147.1.el8_10.x86_64
kernel-modules-4.18.0-553.141.1.el8_10.x86_64	python3-perf-4.18.0-553.148.1.el8_10.x86_64
kernel-modules-4.18.0-553.143.1.el8_10.x86_64	python3-perf-4.18.0-553.150.1.el8_10.x86_64
kernel-modules-4.18.0-553.144.1.el8_10.x86_64	python3-perf-4.18.0-553.151.1.el8_10.x86_64
kernel-modules-4.18.0-553.146.1.el8_10.x86_64	python3-perf-4.18.0-553.153.1.el8_10.x86_64
kernel-modules-4.18.0-553.147.1.el8_10.x86_64	python3-perf-4.18.0-553.154.1.el8_10.x86_64
kernel-modules-4.18.0-553.148.1.el8_10.x86_64	python3-perf-4.18.0-553.155.1.el8_10.x86_64
kernel-modules-4.18.0-553.150.1.el8_10.x86_64	python3-perf-4.18.0-553.156.1.el8_10.x86_64
kernel-modules-4.18.0-553.151.1.el8_10.x86_64	python3-perf-4.18.0-553.157.1.el8_10.x86_64
kernel-modules-4.18.0-553.153.1.el8_10.x86_64	python3-perf-4.18.0-553.158.1.el8_10.x86_64
kernel-modules-4.18.0-553.154.1.el8_10.x86_64	python3-perf-4.18.0-553.159.1.el8_10.x86_64
kernel-modules-4.18.0-553.155.1.el8_10.x86_64	python3-perf-4.18.0-553.160.1.el8_10.x86_64
kernel-modules-4.18.0-553.156.1.el8_10.x86_64	python3-perf-4.18.0-553.162.1.el8_10.x86_64
kernel-modules-4.18.0-553.157.1.el8_10.x86_64	python3-perf-4.18.0-553.163.1.el8_10.x86_64
kernel-modules-4.18.0-553.158.1.el8_10.x86_64	python3-perf-4.18.0-553.164.1.el8_10.x86_64
kernel-modules-4.18.0-553.159.1.el8_10.x86_64	python3-perf-4.18.0-553.166.1.el8_10.x86_64
kernel-modules-4.18.0-553.160.1.el8_10.x86_64	python3-perf-4.18.0-553.167.1.el8_10.x86_64
kernel-modules-4.18.0-553.162.1.el8_10.x86_64	python3-perf-4.18.0-553.168.1.el8_10.x86_64
kernel-modules-4.18.0-553.163.1.el8_10.x86_64	python3-unbound-1.16.2-5.12.el8_10.x86_64
kernel-modules-4.18.0-553.164.1.el8_10.x86_64	python3-unbound-1.16.2-5.14.el8_10.2.x86_64
kernel-modules-4.18.0-553.166.1.el8_10.x86_64	python3-unbound-1.16.2-5.14.el8_10.4.x86_64
kernel-modules-4.18.0-553.167.1.el8_10.x86_64	python3-unbound-1.16.2-5.14.el8_10.x86_64
kernel-modules-4.18.0-553.168.1.el8_10.x86_64	qt5-qtbase-5.15.3-9.el8_10.x86_64
kernel-tools-4.18.0-553.139.1.el8_10.x86_64	qt5-qtbase-common-5.15.3-9.el8_10.noarch
kernel-tools-4.18.0-553.140.1.el8_10.x86_64	qt5-qtbase-gui-5.15.3-9.el8_10.x86_64
kernel-tools-4.18.0-553.141.1.el8_10.x86_64	sqlite-3.26.0-21.el8_10.x86_64
kernel-tools-4.18.0-553.143.1.el8_10.x86_64	sqlite-libs-3.26.0-21.el8_10.x86_64
kernel-tools-4.18.0-553.144.1.el8_10.x86_64	tar-2:1.30-13.el8_10.x86_64
kernel-tools-4.18.0-553.146.1.el8_10.x86_64	unbound-libs-1.16.2-5.12.el8_10.x86_64
kernel-tools-4.18.0-553.147.1.el8_10.x86_64	unbound-libs-1.16.2-5.14.el8_10.2.x86_64
kernel-tools-4.18.0-553.148.1.el8_10.x86_64	unbound-libs-1.16.2-5.14.el8_10.4.x86_64
kernel-tools-4.18.0-553.150.1.el8_10.x86_64	unbound-libs-1.16.2-5.14.el8_10.x86_64
kernel-tools-4.18.0-553.151.1.el8_10.x86_64	vim-minimal-2:8.0.1763-27.el8_10.x86_64
kernel-tools-4.18.0-553.153.1.el8_10.x86_64	vim-minimal-2:8.0.1763-31.el8_10.7.x86_64
	vim-minimal-2:8.0.1763-31.el8_10.x86_64
	wget-1.19.5-16.el8_10.x86_64

Security vulnerabilities resolved in ADS 4.0 OVA OS Upgrade Bundle:

Updated Package	RHSA Number	CVE	RHSA Severity
libpng-2:1.6.34-11.el8_10.x86_64	RHSA-2026:29898	CVE-2026-33416	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

glibc-2.28-251.el8_10.38.x86_64 glibc-all-langpacks-2.28-251.el8_10.38.x86_64 glibc-common-2.28-251.el8_10.38.x86_64 glibc-gconv-extra-2.28-251.el8_10.38.x86_64 glibc-langpack-en-2.28-251.el8_10.38.x86_64 libnsl-2.28-251.el8_10.38.x86_64	RHSA-2026:33126	CVE-2026-5450	Moderate/Sec.
giflib-5.1.4-5.el8_10.x86_64	RHSA-2026:33503	CVE-2026-26740	Important/Sec.
kernel-4.18.0-553.139.1.el8_10.x86_64 kernel-core-4.18.0-553.139.1.el8_10.x86_64 kernel-modules-4.18.0-553.139.1.el8_10.x86_64 kernel-tools-4.18.0-553.139.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.139.1.el8_10.x86_64 python3-perf-4.18.0-553.139.1.el8_10.x86_64	RHSA-2026:33743	CVE-2026-23216 CVE-2026-45984 CVE-2026-46189	Important/Sec.
compat-openssl10-1:1.0.2o-4.el8_10.3.x86_64	RHSA-2026:36215	CVE-2026-45447	Important/Sec.
kernel-4.18.0-553.140.1.el8_10.x86_64 kernel-core-4.18.0-553.140.1.el8_10.x86_64 kernel-modules-4.18.0-553.140.1.el8_10.x86_64 kernel-tools-4.18.0-553.140.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.140.1.el8_10.x86_64 python3-perf-4.18.0-553.140.1.el8_10.x86_64	RHSA-2026:36349	CVE-2025-10263 CVE-2026-43198 CVE-2026-43450 CVE-2026-46209 CVE-2026-46227 CVE-2026-46259	Important/Sec.
kernel-4.18.0-553.141.1.el8_10.x86_64 kernel-core-4.18.0-553.141.1.el8_10.x86_64 kernel-modules-4.18.0-553.141.1.el8_10.x86_64 kernel-tools-4.18.0-553.141.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.141.1.el8_10.x86_64 python3-perf-4.18.0-553.141.1.el8_10.x86_64	RHSA-2026:36366	CVE-2026-43112	Important/Sec.
libtasn1-4.13-6.el8_10.x86_64	RHSA-2026:36728	CVE-2025-13151	Low/Sec.
libsolv-0.7.20-7.el8_10.x86_64	RHSA-2026:36730	CVE-2026-48864	Moderate/Sec.
cups-libs-1:2.2.6-68.el8_10.x86_64	RHSA-2026:36733	CVE-2026-34980	Moderate/Sec.
libxml2-2.9.7-21.el8_10.6.x86_64 python3-libxml2-2.9.7-21.el8_10.6.x86_64	RHSA-2026:36734	CVE-2025-6170	Low/Sec.
gstreamer1-plugins-bad-free-1.16.1-8.el8_10.x86_64	RHSA-2026:37130	CVE-2026-52720 CVE-2026-52722	Important/Sec.
python3-unbound-1.16.2-5.12.el8_10.x86_64 unbound-libs-1.16.2-5.12.el8_10.x86_64	RHSA-2026:37282	CVE-2026-40622 CVE-2026-41292 CVE-2026-42534 CVE-2026-44390	Important/Sec.
openssl-1:1.1.1k-17.el8_6.x86_64 openssl-libs-1:1.1.1k-17.el8_6.x86_64 openssl-perl-1:1.1.1k-17.el8_6.x86_64	RHSA-2026:38503	CVE-2026-28390	Moderate/Sec.
vim-minimal-2:8.0.1763-27.el8_10.x86_64	RHSA-2026:38510	CVE-2026-46483 CVE-2026-47162 CVE-2026-47167	Important/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

		CVE-2026-52858	
kernel-4.18.0-553.143.1.el8_10.x86_64 kernel-core-4.18.0-553.143.1.el8_10.x86_64 kernel-modules-4.18.0-553.143.1.el8_10.x86_64 kernel-tools-4.18.0-553.143.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.143.1.el8_10.x86_64 python3-perf-4.18.0-553.143.1.el8_10.x86_64	RHSA-2026:39083	CVE-2025-71066 CVE-2025-71089 CVE-2026-31411 CVE-2026-43499 CVE-2026-46113 CVE-2026-53166 CVE-2026-53266 CVE-2026-53359	Important/Sec.
kernel-4.18.0-553.144.1.el8_10.x86_64 kernel-core-4.18.0-553.144.1.el8_10.x86_64 kernel-modules-4.18.0-553.144.1.el8_10.x86_64 kernel-tools-4.18.0-553.144.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.144.1.el8_10.x86_64 python3-perf-4.18.0-553.144.1.el8_10.x86_64	RHSA-2026:39179	CVE-2026-46086 CVE-2026-46116	Important/Sec.
platform-python-3.6.8-77.el8_10.x86_64 platform-python-devel-3.6.8-77.el8_10.x86_64 python3-libs-3.6.8-77.el8_10.x86_64	RHSA-2026:39320	CVE-2026-15308	Important/Sec.
glib2-2.56.4-170.el8_10.x86_64	RHSA-2026:42090	CVE-2026-58016	Important/Sec.
kernel-4.18.0-553.146.1.el8_10.x86_64 kernel-core-4.18.0-553.146.1.el8_10.x86_64 kernel-modules-4.18.0-553.146.1.el8_10.x86_64 kernel-tools-4.18.0-553.146.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.146.1.el8_10.x86_64 python3-perf-4.18.0-553.146.1.el8_10.x86_64	RHSA-2026:42552	CVE-2026-46117 CVE-2026-53071	Important/Sec.
glibc-2.28-251.el8_10.40.x86_64 glibc-all-langpacks-2.28-251.el8_10.40.x86_64 glibc-common-2.28-251.el8_10.40.x86_64 glibc-gconv-extra-2.28-251.el8_10.40.x86_64 glibc-langpack-en-2.28-251.el8_10.40.x86_64 libnsl-2.28-251.el8_10.40.x86_64	RHSA-2026:42733	CVE-2026-5435 CVE-2026-5928 CVE-2026-6238	Moderate/Sec.
java-1.8.0-openjdk-1:1.8.0.502.b07-1.1.el8.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.502.b07-1.1.el8.x86_64	RHSA-2026:42877	CVE-2026-41254 CVE-2026-46968 CVE-2026-47010 CVE-2026-47021 CVE-2026-47027 CVE-2026-47057 CVE-2026-47058 CVE-2026-47059 CVE-2026-47063 CVE-2026-60147	Important/Sec.
java-17-openjdk-1:17.0.20.0.8-1.1.el8.x86_64 java-17-openjdk-headless-1:17.0.20.0.8-1.1.el8.x86_64	RHSA-2026:42887	CVE-2026-41254 CVE-2026-46917 CVE-2026-46968 CVE-2026-47010 CVE-2026-47021 CVE-2026-47027 CVE-2026-47059 CVE-2026-47063 CVE-2026-60147	Important/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

acl-2.4.0-1.el8_10.x86_64 libacl-2.4.0-1.el8_10.x86_64	RHSA-2026:43420	CVE-2026-54369 CVE-2026-54370	Important/Sec.
vim-minimal-2:8.0.1763-22.el8_10.x86_64	RHSA-2026:4442		Moderate/Sec.
kernel-4.18.0-553.147.1.el8_10.x86_64 kernel-core-4.18.0-553.147.1.el8_10.x86_64 kernel-modules-4.18.0-553.147.1.el8_10.x86_64 kernel-tools-4.18.0-553.147.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.147.1.el8_10.x86_64 python3-perf-4.18.0-553.147.1.el8_10.x86_64	RHSA-2026:45115	CVE-2025-40026 CVE-2026-52993 CVE-2026-53059	Important/Sec.
grub2-common-1:2.02-170.el8_10.1.noarch grub2-efi-x64-1:2.02-170.el8_10.1.x86_64 grub2-tools-1:2.02-170.el8_10.1.x86_64 grub2-tools-efi-1:2.02-170.el8_10.1.x86_64 grub2-tools-extra-1:2.02-170.el8_10.1.x86_64 grub2-tools-minimal-1:2.02-170.el8_10.1.x86_64	RHSA-2026:4648		Moderate/Sec.
kernel-4.18.0-553.148.1.el8_10.x86_64 kernel-core-4.18.0-553.148.1.el8_10.x86_64 kernel-modules-4.18.0-553.148.1.el8_10.x86_64 kernel-tools-4.18.0-553.148.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.148.1.el8_10.x86_64 python3-perf-4.18.0-553.148.1.el8_10.x86_64	RHSA-2026:47011	CVE-2026-53006	Important/Sec.
libgcrypt-1.8.5-8.el8_10.x86_64	RHSA-2026:47117	CVE-2026-41989	Moderate/Sec.
libtiff-4.0.9-38.el8_10.x86_64	RHSA-2026:47184	CVE-2026-12912	Important/Sec.
libpng-2:1.6.34-10.el8_10.x86_64	RHSA-2026:4728		Important/Sec.
glibc-2.28-251.el8_10.31.x86_64 glibc-all-langpacks-2.28-251.el8_10.31.x86_64 glibc-common-2.28-251.el8_10.31.x86_64 glibc-gconv-extra-2.28-251.el8_10.31.x86_64 glibc-langpack-en-2.28-251.el8_10.31.x86_64 libnsl-2.28-251.el8_10.31.x86_64	RHSA-2026:4772		Moderate/Sec.
gstreamer1-plugins-bad-free-1.16.1-9.el8_10.1.x86_64	RHSA-2026:47731	CVE-2026-59691 CVE-2026-59692	Important/Sec.
openssh-8.0p1-30.el8_10.x86_64 openssh-clients-8.0p1-30.el8_10.x86_64 openssh-server-8.0p1-30.el8_10.x86_64	RHSA-2026:47755	CVE-2026-55653 CVE-2026-55655	Moderate/Sec.
vim-minimal-2:8.0.1763-31.el8_10.x86_64	RHSA-2026:48703	CVE-2026-55693 CVE-2026-57455 CVE-2026-57456 CVE-2026-59858	Important/Sec.
kernel-4.18.0-553.150.1.el8_10.x86_64 kernel-core-4.18.0-553.150.1.el8_10.x86_64 kernel-modules-4.18.0-553.150.1.el8_10.x86_64 kernel-tools-4.18.0-553.150.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.150.1.el8_10.x86_64 python3-perf-4.18.0-553.150.1.el8_10.x86_64	RHSA-2026:49214	CVE-2026-31692 CVE-2026-43116 CVE-2026-46150 CVE-2026-64530	Important/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

kernel-4.18.0-553.151.1.el8_10.x86_64 kernel-core-4.18.0-553.151.1.el8_10.x86_64 kernel-modules-4.18.0-553.151.1.el8_10.x86_64 kernel-tools-4.18.0-553.151.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.151.1.el8_10.x86_64 python3-perf-4.18.0-553.151.1.el8_10.x86_64	RHSA-2026:49857	CVE-2026-52923	Moderate/Sec.
kernel-4.18.0-553.153.1.el8_10.x86_64 kernel-core-4.18.0-553.153.1.el8_10.x86_64 kernel-modules-4.18.0-553.153.1.el8_10.x86_64 kernel-tools-4.18.0-553.153.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.153.1.el8_10.x86_64 python3-perf-4.18.0-553.153.1.el8_10.x86_64	RHSA-2026:50978	CVE-2025-54518	Important/Sec.
kernel-4.18.0-553.154.1.el8_10.x86_64 kernel-core-4.18.0-553.154.1.el8_10.x86_64 kernel-modules-4.18.0-553.154.1.el8_10.x86_64 kernel-tools-4.18.0-553.154.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.154.1.el8_10.x86_64 python3-perf-4.18.0-553.154.1.el8_10.x86_64	RHSA-2026:52765	CVE-2026-64496	Moderate/Sec.
kernel-4.18.0-553.155.1.el8_10.x86_64 kernel-core-4.18.0-553.155.1.el8_10.x86_64 kernel-modules-4.18.0-553.155.1.el8_10.x86_64 kernel-tools-4.18.0-553.155.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.155.1.el8_10.x86_64 python3-perf-4.18.0-553.155.1.el8_10.x86_64	RHSA-2026:54246	CVE-2026-45991 CVE-2026-53009	Moderate/Sec.
dracut-049-246.git20260728.el8_10.x86_64 dracut-config-rescue-049-246.git20260728.el8_10.x86_64 dracut-network-049-246.git20260728.el8_10.x86_64 dracut-squash-049-246.git20260728.el8_10.x86_64	RHSA-2026:54575	CVE-2026-15816	Important/Sec.
bind-export-libs-32:9.11.36-16.el8_10.14.x86_64	RHSA-2026:54654	CVE-2026-10723 CVE-2026-11622 CVE-2026-11721 CVE-2026-13204 CVE-2026-13321	Important/Sec.
kernel-4.18.0-553.156.1.el8_10.x86_64 kernel-core-4.18.0-553.156.1.el8_10.x86_64 kernel-modules-4.18.0-553.156.1.el8_10.x86_64 kernel-tools-4.18.0-553.156.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.156.1.el8_10.x86_64 python3-perf-4.18.0-553.156.1.el8_10.x86_64	RHSA-2026:55764	CVE-2025-39902 CVE-2026-17523 CVE-2026-43206 CVE-2026-53016 CVE-2026-53136 CVE-2026-53329 CVE-2026-53374 CVE-2026-63879 CVE-2026-63884 CVE-2026-64219	Important/Sec.
java-1.8.0-openjdk-1:1.8.0.504.b01-1.1.el8.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.504.b01-1.1.el8.x86_64	RHSA-2026:55775	CVE-2026-60589 CVE-2026-61308 CVE-2026-70907	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

qemu-guest-agent-15:6.2.0-53.module+el8.10.0+23760+c0926e61.6.x86_64	RHSA-2026:5578		Moderate/Sec.
java-17-openjdk-1:17.0.20.1.1-1.1.el8.x86_64 java-17-openjdk-headless-1:17.0.20.1.1-1.1.el8.x86_64	RHSA-2026:55781	CVE-2026-60589 CVE-2026-61308 CVE-2026-70907	Moderate/Sec.
python3-unbound-1.16.2-5.14.el8_10.x86_64 unbound-libs-1.16.2-5.14.el8_10.x86_64	RHSA-2026:55784	CVE-2026-44690	Important/Sec.
libnghttp2-1.33.0-6.el8_10.3.x86_64	RHSA-2026:55804	CVE-2026-58055	Moderate/Sec.
gnutls-3.6.16-8.el8_10.5.x86_64	RHSA-2026:5585		Moderate/Sec.
platform-python-3.6.8-74.el8_10.x86_64 platform-python-devel-3.6.8-74.el8_10.x86_64 python3-libs-3.6.8-74.el8_10.x86_64	RHSA-2026:5588		Moderate/Sec.
pam-1.3.1-40.el8_10.x86_64	RHSA-2026:56131	CVE-2026-54411	Moderate/Sec.
libattr-2.6.0-1.el8_10.x86_64	RHSA-2026:56133	CVE-2026-54371	Moderate/Sec.
platform-python-3.6.8-78.el8_10.x86_64 platform-python-devel-3.6.8-78.el8_10.x86_64 python3-libs-3.6.8-78.el8_10.x86_64	RHSA-2026:56219	CVE-2026-11940	Important/Sec.
gstreamer1-plugins-bad-free-1.16.1-9.el8_10.2.x86_64	RHSA-2026:56521	CVE-2026-19387	Important/Sec.
kernel-4.18.0-553.157.1.el8_10.x86_64 kernel-core-4.18.0-553.157.1.el8_10.x86_64 kernel-modules-4.18.0-553.157.1.el8_10.x86_64 kernel-tools-4.18.0-553.157.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.157.1.el8_10.x86_64 python3-perf-4.18.0-553.157.1.el8_10.x86_64	RHSA-2026:57253	CVE-2024-56602 CVE-2026-46120 CVE-2026-52991 CVE-2026-53189 CVE-2026-63887 CVE-2026-63888 CVE-2026-64048 CVE-2026-64379 CVE-2026-68388	Important/Sec.
curl-7.61.1-34.el8_10.13.x86_64 libcurl-7.61.1-34.el8_10.13.x86_64	RHSA-2026:57462	CVE-2026-8286	Important/Sec.
sqlite-3.26.0-21.el8_10.x86_64 sqlite-libs-3.26.0-21.el8_10.x86_64	RHSA-2026:58938	CVE-2026-11822 CVE-2026-11824	Important/Sec.
gstreamer1-plugins-base-1.16.1-6.el8_10.1.x86_64	RHSA-2026:59487	CVE-2026-18297	Important/Sec.
kernel-4.18.0-553.158.1.el8_10.x86_64 kernel-core-4.18.0-553.158.1.el8_10.x86_64 kernel-modules-4.18.0-553.158.1.el8_10.x86_64 kernel-tools-4.18.0-553.158.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.158.1.el8_10.x86_64 python3-perf-4.18.0-553.158.1.el8_10.x86_64	RHSA-2026:59821	CVE-2026-52924 CVE-2026-63886 CVE-2026-63913 CVE-2026-64189 CVE-2026-64191 CVE-2026-64276 CVE-2026-64277 CVE-2026-64320	Important/Sec.
kernel-4.18.0-553.115.1.el8_10.x86_64	RHSA-202		Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

kernel-core-4.18.0-553.115.1.el8_10.x86_64 kernel-modules-4.18.0-553.115.1.el8_10.x86_64 kernel-tools-4.18.0-553.115.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.115.1.el8_10.x86_64 python3-perf-4.18.0-553.115.1.el8_10.x86_64	6:6037		
libxml2-2.9.7-21.el8_10.7.x86_64 python3-libxml2-2.9.7-21.el8_10.7.x86_64	RHSA-2026:61248	CVE-2026-11979	Moderate/Sec.
glib2-2.56.4-177.el8_10.x86_64	RHSA-2026:61766	CVE-2026-15588 CVE-2026-58010 CVE-2026-58011 CVE-2026-58012 CVE-2026-58013 CVE-2026-58014 CVE-2026-58015	Moderate/Sec.
wget-1.19.5-16.el8_10.x86_64	RHSA-2026:62144	CVE-2026-58469 CVE-2026-58471 CVE-2026-58472	Moderate/Sec.
libssh-0.9.6-17.el8_10.x86_64 libssh-config-0.9.6-17.el8_10.noarch	RHSA-2026:62218	CVE-2026-59843 CVE-2026-59844 CVE-2026-59845 CVE-2026-59846 CVE-2026-59847 CVE-2026-59848 CVE-2026-59850	Moderate/Sec.
kernel-4.18.0-553.159.1.el8_10.x86_64 kernel-core-4.18.0-553.159.1.el8_10.x86_64 kernel-modules-4.18.0-553.159.1.el8_10.x86_64 kernel-tools-4.18.0-553.159.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.159.1.el8_10.x86_64 python3-perf-4.18.0-553.159.1.el8_10.x86_64	RHSA-2026:63014	CVE-2024-57849 CVE-2025-71132 CVE-2026-45970 CVE-2026-53185 CVE-2026-53391 CVE-2026-53392 CVE-2026-53397 CVE-2026-53399 CVE-2026-63800 CVE-2026-64018 CVE-2026-64268 CVE-2026-64298 CVE-2026-68480 CVE-2026-74581	Important/Sec.
openssh-8.0p1-28.el8_10.x86_64 openssh-clients-8.0p1-28.el8_10.x86_64 openssh-server-8.0p1-28.el8_10.x86_64	RHSA-2026:6461		Important/Sec.
platform-python-3.6.8-75.el8_10.x86_64 platform-python-devel-3.6.8-75.el8_10.x86_64 python3-libs-3.6.8-75.el8_10.x86_64	RHSA-2026:6473		Important/Sec.
expat-2.5.0-2.el8_10.2.x86_64	RHSA-2026:64809	CVE-2026-50219 CVE-2026-56132	Moderate/Sec.
microcode_ctl-4:20260812-1.el8_10.x86_64	RHSA-2026:65147	CVE-2025-31936 CVE-2025-35973	Important/Sec.
kernel-4.18.0-553.117.1.el8_10.x86_64 kernel-core-4.18.0-553.117.1.el8_10.x86_64	RHSA-2026:6571		Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

kernel-modules-4.18.0-553.117.1.el8_10.x86_64 kernel-tools-4.18.0-553.117.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.117.1.el8_10.x86_64 python3-perf-4.18.0-553.117.1.el8_10.x86_64			
qt5-qtbase-5.15.3-9.el8_10.x86_64 qt5-qtbase-common-5.15.3-9.el8_10.noarch qt5-qtbase-gui-5.15.3-9.el8_10.x86_64	RHSA-2026:65897	CVE-2026-9499	Important/Sec.
gzip-1.9-15.el8_10.x86_64	RHSA-2026:65998	CVE-2026-41991 CVE-2026-41992	Moderate/Sec.
kernel-4.18.0-553.160.1.el8_10.x86_64 kernel-core-4.18.0-553.160.1.el8_10.x86_64 kernel-modules-4.18.0-553.160.1.el8_10.x86_64 kernel-tools-4.18.0-553.160.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.160.1.el8_10.x86_64 python3-perf-4.18.0-553.160.1.el8_10.x86_64	RHSA-2026:66000	CVE-2026-43493 CVE-2026-53002 CVE-2026-64007 CVE-2026-64563 CVE-2026-68343 CVE-2026-72129 CVE-2026-74480	Important/Sec.
kernel-4.18.0-553.162.1.el8_10.x86_64 kernel-core-4.18.0-553.162.1.el8_10.x86_64 kernel-modules-4.18.0-553.162.1.el8_10.x86_64 kernel-tools-4.18.0-553.162.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.162.1.el8_10.x86_64 python3-perf-4.18.0-553.162.1.el8_10.x86_64	RHSA-2026:66325	CVE-2025-68745 CVE-2026-46149 CVE-2026-52917 CVE-2026-52942 CVE-2026-52986 CVE-2026-53091 CVE-2026-53246 CVE-2026-63801 CVE-2026-63971 CVE-2026-64015 CVE-2026-64113 CVE-2026-68117 CVE-2026-68300 CVE-2026-68315 CVE-2026-68376	Important/Sec.
vim-minimal-2:8.0.1763-31.el8_10.7.x86_64	RHSA-2026:66348	CVE-2026-28420 CVE-2026-52859 CVE-2026-55892 CVE-2026-59857 CVE-2026-73072 CVE-2026-73076 CVE-2026-73078	Important/Sec.
glib2-2.56.4-178.el8_10.x86_64	RHSA-2026:66451	CVE-2026-16118	Moderate/Sec.
gstreamer1-plugins-base-1.16.1-7.el8_10.x86_64	RHSA-2026:67145	CVE-2026-85150	Moderate/Sec.
perl-Errno-1.28-423.el8_10.1.x86_64 perl-IO-1.38-423.el8_10.1.x86_64 perl-SelfLoader-1.23-423.el8_10.1.noarch perl-interpreter-4:5.26.3-423.el8_10.1.x86_64 perl-libs-4:5.26.3-423.el8_10.1.x86_64 perl-macros-4:5.26.3-423.el8_10.1.x86_64	RHSA-2026:67162	CVE-2026-13221	Moderate/Sec.
libkcapi-1.4.0-3.el8_10.x86_64 libkcapi-hmaccalc-1.4.0-3.el8_10.x86_64	RHSA-2026:67266	CVE-2026-71225 CVE-2026-71226	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

		CVE-2026-71227	
kernel-4.18.0-553.163.1.el8_10.x86_64 kernel-core-4.18.0-553.163.1.el8_10.x86_64 kernel-modules-4.18.0-553.163.1.el8_10.x86_64 kernel-tools-4.18.0-553.163.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.163.1.el8_10.x86_64 python3-perf-4.18.0-553.163.1.el8_10.x86_64	RHSA-2026:67468	CVE-2024-53161 CVE-2025-71127 CVE-2026-43133 CVE-2026-52947 CVE-2026-53182 CVE-2026-63802 CVE-2026-63889 CVE-2026-64117 CVE-2026-68363 CVE-2026-72098 CVE-2026-74556	Important/Sec.
gstreamer1-plugins-bad-free-1.16.1-6.el8_10.x86_64 gstreamer1-plugins-base-1.16.1-6.el8_10.x86_64	RHSA-2026:6750		Important/Sec.
libevent-2.1.8-11.el8_10.x86_64	RHSA-2026:67908	CVE-2026-63382 CVE-2026-63383 CVE-2026-63384 CVE-2026-63385 CVE-2026-63387 CVE-2026-63388	Important/Sec.
libsoup-2.62.3-15.el8_10.x86_64	RHSA-2026:68266	CVE-2026-15711	Moderate/Sec.
kernel-4.18.0-553.164.1.el8_10.x86_64 kernel-core-4.18.0-553.164.1.el8_10.x86_64 kernel-modules-4.18.0-553.164.1.el8_10.x86_64 kernel-tools-4.18.0-553.164.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.164.1.el8_10.x86_64 python3-perf-4.18.0-553.164.1.el8_10.x86_64	RHSA-2026:68531	CVE-2026-23103 CVE-2026-31663 CVE-2026-43233 CVE-2026-43339 CVE-2026-46266 CVE-2026-46306 CVE-2026-52920 CVE-2026-53075 CVE-2026-53131 CVE-2026-53176 CVE-2026-53192 CVE-2026-53223 CVE-2026-53228 CVE-2026-53239 CVE-2026-53268 CVE-2026-53275 CVE-2026-63917 CVE-2026-63919 CVE-2026-63921 CVE-2026-64002 CVE-2026-68143 CVE-2026-68426	Important/Sec.
libtiff-4.0.9-39.el8_10.x86_64	RHSA-2026:69095	CVE-2026-52490	Important/Sec.
python3-unbound-1.16.2-5.14.el8_10.2.x86_64 unbound-libs-1.16.2-5.14.el8_10.2.x86_64	RHSA-2026:69120	CVE-2026-50252	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

vim-minimal-2:8.0.1763-22.el8_10.1.x86_64	RHSA-2026:6915		Important/Sec.
openssh-8.0p1-33.el8_10.x86_64 openssh-clients-8.0p1-33.el8_10.x86_64 openssh-server-8.0p1-33.el8_10.x86_64	RHSA-2026:69266	CVE-2026-59995 CVE-2026-59999 CVE-2026-73282	Important/Sec.
libxml2-2.9.7-21.el8_10.8.x86_64 python3-libxml2-2.9.7-21.el8_10.8.x86_64	RHSA-2026:69655	CVE-2026-6653	Moderate/Sec.
coreutils-8.30-21.el8_10.x86_64	RHSA-2026:69964	CVE-2025-5278	Moderate/Sec.
tar-2:1.30-13.el8_10.x86_64	RHSA-2026:70390	CVE-2025-45582 CVE-2026-18477 CVE-2026-18508 CVE-2026-5704	Moderate/Sec.
kernel-4.18.0-553.166.1.el8_10.x86_64 kernel-core-4.18.0-553.166.1.el8_10.x86_64 kernel-modules-4.18.0-553.166.1.el8_10.x86_64 kernel-tools-4.18.0-553.166.1.el8_10.x86_64 kernel-tools-4.18.0-553.166.1.el8_10.x86_64 python3-perf-4.18.0-553.166.1.el8_10.x86_64	RHSA-2026:70402	CVE-2023-54120 CVE-2023-54214 CVE-2025-39964 CVE-2025-71082 CVE-2026-43334 CVE-2026-45894 CVE-2026-46043 CVE-2026-46133 CVE-2026-52918 CVE-2026-53053 CVE-2026-53062 CVE-2026-53254 CVE-2026-53256 CVE-2026-63823 CVE-2026-63947 CVE-2026-63975 CVE-2026-64534 CVE-2026-64582 CVE-2026-68188 CVE-2026-68293	Important/Sec.
python3-unbound-1.16.2-5.14.el8_10.4.x86_64 unbound-libs-1.16.2-5.14.el8_10.4.x86_64	RHSA-2026:70754	CVE-2026-81634 CVE-2026-81642 CVE-2026-82717	Critical/Sec.
kernel-4.18.0-553.167.1.el8_10.x86_64 kernel-core-4.18.0-553.167.1.el8_10.x86_64 kernel-modules-4.18.0-553.167.1.el8_10.x86_64 kernel-tools-4.18.0-553.167.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.167.1.el8_10.x86_64 python3-perf-4.18.0-553.167.1.el8_10.x86_64	RHSA-2026:71213	CVE-2026-43370 CVE-2026-63831 CVE-2026-64564 CVE-2026-72261 CVE-2026-80844 CVE-2026-81000 CVE-2026-89846	Important/Sec.
kernel-4.18.0-553.168.1.el8_10.x86_64 kernel-core-4.18.0-553.168.1.el8_10.x86_64 kernel-modules-4.18.0-553.168.1.el8_10.x86_64 kernel-tools-4.18.0-553.168.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.168.1.el8_10.x86_64 python3-perf-4.18.0-553.168.1.el8_10.x86_64	RHSA-2026:71329	CVE-2026-31566 CVE-2026-52912 CVE-2026-68121 CVE-2026-80714 CVE-2026-89480	Important/Sec.
libxml2-2.9.7-21.el8_10.9.x86_64	RHSA-202	CVE-2026-74860	Important/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

python3-libxml2-2.9.7-21.el8_10.9.x86_64	6:71641	CVE-2026-86138 CVE-2026-86140 CVE-2026-86143 CVE-2026-86144	
kernel-4.18.0-553.120.1.el8_10.x86_64 kernel-core-4.18.0-553.120.1.el8_10.x86_64 kernel-modules-4.18.0-553.120.1.el8_10.x86_64 kernel-tools-4.18.0-553.120.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.120.1.el8_10.x86_64 python3-perf-4.18.0-553.120.1.el8_10.x86_64	RHSA-2026:9131		Important/Sec.
java-1.8.0-openjdk-1:1.8.0.492.b09-1.el8.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.492.b09-1.el8.x86_64	RHSA-2026:9683		Important/Sec.
java-17-openjdk-1:17.0.19.0.10-1.el8.x86_64 java-17-openjdk-headless-1:17.0.19.0.10-1.el8.x86_64	RHSA-2026:9686		Important/Sec.

ADS-4.0 OVA Security Service Pack 14 includes the following rpm updates:

gdk-pixbuf2-2.36.12-8.el8_10.x86_64	kernel-modules-4.18.0-553.134.1.el8_10.x86_64
gdk-pixbuf2-modules-2.36.12-8.el8_10.x86_64	kernel-tools-4.18.0-553.134.1.el8_10.x86_64
platform-python-3.6.8-76.el8_10.x86_64	kernel-tools-libs-4.18.0-553.134.1.el8_10.x86_64
platform-python-devel-3.6.8-76.el8_10.x86_64	python3-perf-4.18.0-553.134.1.el8_10.x86_64
python3-libs-3.6.8-76.el8_10.x86_64	dracut-049-244.git20260529.el8_10.x86_64
libxml2-2.9.7-21.el8_10.4.x86_64	dracut-config-rescue-049-244.git20260529.el8_10.x86_64
python3-libxml2-2.9.7-21.el8_10.4.x86_64	dracut-network-049-244.git20260529.el8_10.x86_64
vim-minimal-2:8.0.1763-22.el8_10.3.x86_64	dracut-squash-049-244.git20260529.el8_10.x86_64
sudo-1.9.5p2-1.el8_10.5.x86_64	kernel-4.18.0-553.136.1.el8_10.x86_64
libcap-2.48-6.el8_10.1.x86_64	kernel-core-4.18.0-553.136.1.el8_10.x86_64
openssh-8.0p1-29.el8_10.x86_64	kernel-modules-4.18.0-553.136.1.el8_10.x86_64
openssh-clients-8.0p1-29.el8_10.x86_64	kernel-tools-4.18.0-553.136.1.el8_10.x86_64
openssh-server-8.0p1-29.el8_10.x86_64	kernel-tools-libs-4.18.0-553.136.1.el8_10.x86_64
kernel-4.18.0-553.123.1.el8_10.x86_64	python3-perf-4.18.0-553.136.1.el8_10.x86_64
kernel-core-4.18.0-553.123.1.el8_10.x86_64	kernel-4.18.0-553.137.1.el8_10.x86_64
kernel-modules-4.18.0-553.123.1.el8_10.x86_64	kernel-core-4.18.0-553.137.1.el8_10.x86_64
kernel-tools-4.18.0-553.123.1.el8_10.x86_64	kernel-modules-4.18.0-553.137.1.el8_10.x86_64
kernel-tools-libs-4.18.0-553.123.1.el8_10.x86_64	kernel-tools-4.18.0-553.137.1.el8_10.x86_64
python3-perf-4.18.0-553.123.1.el8_10.x86_64	kernel-tools-libs-4.18.0-553.137.1.el8_10.x86_64
libsoup-2.62.3-14.el8_10.x86_64	python3-perf-4.18.0-553.137.1.el8_10.x86_64
glib2-2.56.4-169.el8_10.x86_64	vim-minimal-2:8.0.1763-24.el8_10.x86_64
libtiff-4.0.9-37.el8_10.x86_64	vim-minimal-2:8.0.1763-22.el8_10.x86_64
kernel-4.18.0-553.124.1.el8_10.x86_64	grub2-common-1:2.02-170.el8_10.1.noarch
kernel-core-4.18.0-553.124.1.el8_10.x86_64	grub2-efi-x64-1:2.02-170.el8_10.1.x86_64
kernel-modules-4.18.0-553.124.1.el8_10.x86_64	grub2-tools-1:2.02-170.el8_10.1.x86_64
kernel-tools-4.18.0-553.124.1.el8_10.x86_64	grub2-tools-efi-1:2.02-170.el8_10.1.x86_64
kernel-tools-libs-4.18.0-553.124.1.el8_10.x86_64	grub2-tools-extra-1:2.02-170.el8_10.1.x86_64
python3-perf-4.18.0-553.124.1.el8_10.x86_64	grub2-tools-minimal-1:2.02-170.el8_10.1.x86_64
krb5-libs-1.18.2-34.el8_10.x86_64	libpng-2:1.6.34-10.el8_10.x86_64
libsndfile-1.0.28-17.el8_10.x86_64	glibc-2.28-251.el8_10.31.x86_64

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

kernel-4.18.0-553.125.1.el8_10.x86_64	glibc-all-langpacks-2.28-251.el8_10.31.x86_64
kernel-core-4.18.0-553.125.1.el8_10.x86_64	glibc-common-2.28-251.el8_10.31.x86_64
kernel-modules-4.18.0-553.125.1.el8_10.x86_64	glibc-gconv-extra-2.28-251.el8_10.31.x86_64
kernel-tools-4.18.0-553.125.1.el8_10.x86_64	glibc-langpack-en-2.28-251.el8_10.31.x86_64
kernel-tools-libs-4.18.0-553.125.1.el8_10.x86_64	libnsl-2.28-251.el8_10.31.x86_64
python3-perf-4.18.0-553.125.1.el8_10.x86_64	qemu-guest-agent-15:6.2.0-53.module+el8.10.0+23760+c0926e61.6.x86_64
glibc-2.28-251.el8_10.37.x86_64	gnutls-3.6.16-8.el8_10.5.x86_64
glibc-all-langpacks-2.28-251.el8_10.37.x86_64	platform-python-3.6.8-74.el8_10.x86_64
glibc-common-2.28-251.el8_10.37.x86_64	platform-python-devel-3.6.8-74.el8_10.x86_64
glibc-gconv-extra-2.28-251.el8_10.37.x86_64	python3-libs-3.6.8-74.el8_10.x86_64
glibc-langpack-en-2.28-251.el8_10.37.x86_64	kernel-4.18.0-553.115.1.el8_10.x86_64
libnsl-2.28-251.el8_10.37.x86_64	kernel-core-4.18.0-553.115.1.el8_10.x86_64
gnutls-3.6.16-8.el8_10.6.x86_64	kernel-modules-4.18.0-553.115.1.el8_10.x86_64
kernel-4.18.0-553.126.1.el8_10.x86_64	kernel-tools-4.18.0-553.115.1.el8_10.x86_64
kernel-core-4.18.0-553.126.1.el8_10.x86_64	kernel-tools-libs-4.18.0-553.115.1.el8_10.x86_64
kernel-modules-4.18.0-553.126.1.el8_10.x86_64	python3-perf-4.18.0-553.115.1.el8_10.x86_64
kernel-tools-4.18.0-553.126.1.el8_10.x86_64	openssh-8.0p1-28.el8_10.x86_64
kernel-tools-libs-4.18.0-553.126.1.el8_10.x86_64	openssh-clients-8.0p1-28.el8_10.x86_64
python3-perf-4.18.0-553.126.1.el8_10.x86_64	openssh-server-8.0p1-28.el8_10.x86_64
compat-openssl10-1:1.0.2o-4.el8_10.2.x86_64	platform-python-3.6.8-75.el8_10.x86_64
expat-2.5.0-2.el8_10.x86_64	platform-python-devel-3.6.8-75.el8_10.x86_64
vim-minimal-2:8.0.1763-23.el8_10.x86_64	python3-libs-3.6.8-75.el8_10.x86_64
kernel-4.18.0-553.129.1.el8_10.x86_64	kernel-4.18.0-553.117.1.el8_10.x86_64
kernel-core-4.18.0-553.129.1.el8_10.x86_64	kernel-core-4.18.0-553.117.1.el8_10.x86_64
kernel-modules-4.18.0-553.129.1.el8_10.x86_64	kernel-modules-4.18.0-553.117.1.el8_10.x86_64
kernel-tools-4.18.0-553.129.1.el8_10.x86_64	kernel-tools-4.18.0-553.117.1.el8_10.x86_64
kernel-tools-libs-4.18.0-553.129.1.el8_10.x86_64	kernel-tools-libs-4.18.0-553.117.1.el8_10.x86_64
python3-perf-4.18.0-553.129.1.el8_10.x86_64	python3-perf-4.18.0-553.117.1.el8_10.x86_64
bind-export-libs-32:9.11.36-16.el8_10.8.x86_64	gstreamer1-plugins-bad-free-1.16.1-6.el8_10.x86_64
python3-unbound-1.16.2-5.11.el8_10.x86_64	gstreamer1-plugins-base-1.16.1-6.el8_10.x86_64
unbound-libs-1.16.2-5.11.el8_10.x86_64	vim-minimal-2:8.0.1763-22.el8_10.1.x86_64
kernel-4.18.0-553.132.1.el8_10.x86_64	libnghttp2-1.33.0-6.el8_10.2.x86_64
kernel-core-4.18.0-553.132.1.el8_10.x86_64	bind-export-libs-32:9.11.36-16.el8_10.7.x86_64
kernel-modules-4.18.0-553.132.1.el8_10.x86_64	libarchive-3.3.3-7.el8_10.x86_64
kernel-tools-4.18.0-553.132.1.el8_10.x86_64	giflib-5.1.4-4.el8_10.x86_64
kernel-tools-libs-4.18.0-553.132.1.el8_10.x86_64	kernel-4.18.0-553.120.1.el8_10.x86_64
python3-perf-4.18.0-553.132.1.el8_10.x86_64	kernel-core-4.18.0-553.120.1.el8_10.x86_64
openssl-1:1.1.1k-16.el8_6.x86_64	kernel-modules-4.18.0-553.120.1.el8_10.x86_64
openssl-libs-1:1.1.1k-16.el8_6.x86_64	kernel-tools-4.18.0-553.120.1.el8_10.x86_64
openssl-perl-1:1.1.1k-16.el8_6.x86_64	kernel-tools-libs-4.18.0-553.120.1.el8_10.x86_64
libxml2-2.9.7-21.el8_10.5.x86_64	python3-perf-4.18.0-553.120.1.el8_10.x86_64
python3-libxml2-2.9.7-21.el8_10.5.x86_64	java-1.8.0-openjdk-1:1.8.0.492.b09-1.el8.x86_64
libxslt-1.1.32-6.4.el8_10.x86_64	java-1.8.0-openjdk-headless-1:1.8.0.492.b09-1.el8.x86_64
kernel-4.18.0-553.134.1.el8_10.x86_64	java-17-openjdk-1:17.0.19.0.10-1.el8.x86_64
kernel-core-4.18.0-553.134.1.el8_10.x86_64	java-17-openjdk-headless-1:17.0.19.0.10-1.el8.x86_64ss

Security vulnerabilities resolved in ADS 4.0 OVA OS Upgrade Bundle:

Updated Package	RHSA Number	CVE	RHSA Severity
gdk-pixbuf2-2.36.12-8.el8_10.x86_64	RHSA-202	CVE-2026-5201	Important/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

gdk-pixbuf2-modules-2.36.12-8.el8_10.x86_64	6:10741		
platform-python-3.6.8-76.el8_10.x86_64 platform-python-devel-3.6.8-76.el8_10.x86_64 python3-libs-3.6.8-76.el8_10.x86_64	RHSA-202 6:11077	CVE-2026-4786 CVE-2026-6100	Important/Sec.
libxml2-2.9.7-21.el8_10.4.x86_64 python3-libxml2-2.9.7-21.el8_10.4.x86_64	RHSA-202 6:11349	CVE-2025-9714	Moderate/Sec.
vim-minimal-2:8.0.1763-22.el8_10.3.x86_64	RHSA-202 6:11509	CVE-2026-34982	Important/Sec.
sudo-1.9.5p2-1.el8_10.5.x86_64	RHSA-202 6:11521	CVE-2026-35535	Important/Sec.
libcap-2.48-6.el8_10.1.x86_64	RHSA-202 6:13285	CVE-2026-4878	Important/Sec.
openssh-8.0p1-29.el8_10.x86_64 openssh-clients-8.0p1-29.el8_10.x86_64 openssh-server-8.0p1-29.el8_10.x86_64	RHSA-202 6:13383	CVE-2026-35385 CVE-2026-35386 CVE-2026-35387 CVE-2026-35388 CVE-2026-35414	Important/Sec.
kernel-4.18.0-553.123.1.el8_10.x86_64 kernel-core-4.18.0-553.123.1.el8_10.x86_64 kernel-modules-4.18.0-553.123.1.el8_10.x86_64 kernel-tools-4.18.0-553.123.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.123.1.el8_10.x86_64 python3-perf-4.18.0-553.123.1.el8_10.x86_64	RHSA-202 6:13577	CVE-2024-41073 CVE-2025-40252 CVE-2025-68724 CVE-2026-23401 CVE-2026-31402 CVE-2026-31431	Important/Sec.
libsoup-2.62.3-14.el8_10.x86_64	RHSA-202 6:14087	CVE-2026-5119	Moderate/Sec.
glib2-2.56.4-169.el8_10.x86_64	RHSA-202 6:15953	CVE-2025-14087 CVE-2025-14512	Moderate/Sec.
libtiff-4.0.9-37.el8_10.x86_64	RHSA-202 6:16055	CVE-2026-4775	Important/Sec.
kernel-4.18.0-553.124.1.el8_10.x86_64 kernel-core-4.18.0-553.124.1.el8_10.x86_64 kernel-modules-4.18.0-553.124.1.el8_10.x86_64 kernel-tools-4.18.0-553.124.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.124.1.el8_10.x86_64 python3-perf-4.18.0-553.124.1.el8_10.x86_64	RHSA-202 6:16195	CVE-2026-43284	Important/Sec.
krb5-libs-1.18.2-34.el8_10.x86_64	RHSA-202 6:16799	CVE-2026-40355 CVE-2026-40356	Important/Sec.
libsndfile-1.0.28-17.el8_10.x86_64	RHSA-202 6:19559	CVE-2026-37555	Important/Sec.
kernel-4.18.0-553.125.1.el8_10.x86_64 kernel-core-4.18.0-553.125.1.el8_10.x86_64 kernel-modules-4.18.0-553.125.1.el8_10.x86_64 kernel-tools-4.18.0-553.125.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.125.1.el8_10.x86_64 python3-perf-4.18.0-553.125.1.el8_10.x86_64	RHSA-202 6:19666	CVE-2026-46300 CVE-2026-46333	Important/Sec.
glibc-2.28-251.el8_10.37.x86_64 glibc-all-langpacks-2.28-251.el8_10.37.x86_64	RHSA-202 6:20587	CVE-2026-4046	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

glibc-common-2.28-251.el8_10.37.x86_64 glibc-gconv-extra-2.28-251.el8_10.37.x86_64 glibc-langpack-en-2.28-251.el8_10.37.x86_64 libnsl-2.28-251.el8_10.37.x86_64			
gnutls-3.6.16-8.el8_10.6.x86_64	RHSA-2026:20611	CVE-2026-33845 CVE-2026-33846 CVE-2026-3833 CVE-2026-42009 CVE-2026-42010 CVE-2026-42011	Important/Sec.
kernel-4.18.0-553.126.1.el8_10.x86_64 kernel-core-4.18.0-553.126.1.el8_10.x86_64 kernel-modules-4.18.0-553.126.1.el8_10.x86_64 kernel-tools-4.18.0-553.126.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.126.1.el8_10.x86_64 python3-perf-4.18.0-553.126.1.el8_10.x86_64	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	Important/Sec.
compat-openssl10-1:1.0.2o-4.el8_10.2.x86_64	RHSA-2026:22315	CVE-2026-28390	Moderate/Sec.
expat-2.5.0-2.el8_10.x86_64	RHSA-2026:22721	CVE-2026-45186	Important/Sec.
vim-minimal-2:8.0.1763-23.el8_10.x86_64	RHSA-2026:22730	CVE-2026-35177	Moderate/Sec.
kernel-4.18.0-553.129.1.el8_10.x86_64 kernel-core-4.18.0-553.129.1.el8_10.x86_64 kernel-modules-4.18.0-553.129.1.el8_10.x86_64 kernel-tools-4.18.0-553.129.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.129.1.el8_10.x86_64 python3-perf-4.18.0-553.129.1.el8_10.x86_64	RHSA-2026:23258	CVE-2026-46243	Important/Sec.
bind-export-libs-32:9.11.36-16.el8_10.8.x86_64	RHSA-2026:24339	CVE-2026-3039 CVE-2026-5946	Important/Sec.
python3-unbound-1.16.2-5.11.el8_10.x86_64 unbound-libs-1.16.2-5.11.el8_10.x86_64	RHSA-2026:24365	CVE-2026-42944 CVE-2026-42959	Important/Sec.
kernel-4.18.0-553.132.1.el8_10.x86_64 kernel-core-4.18.0-553.132.1.el8_10.x86_64 kernel-modules-4.18.0-553.132.1.el8_10.x86_64 kernel-tools-4.18.0-553.132.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.132.1.el8_10.x86_64 python3-perf-4.18.0-553.132.1.el8_10.x86_64	RHSA-2026:25121	CVE-2023-53781 CVE-2025-21858 CVE-2025-68366 CVE-2026-22984 CVE-2026-22990 CVE-2026-23392	Critical/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

		CVE-2026-31581 CVE-2026-31613 CVE-2026-43037 CVE-2026-43038 CVE-2026-43125 CVE-2026-45852 sCVE-2026-46181	
openssl-1:1.1.1k-16.el8_6.x86_64 openssl-libs-1:1.1.1k-16.el8_6.x86_64 openssl-perl-1:1.1.1k-16.el8_6.x86_64	RHSA-2026:26275	CVE-2024-4741 CVE-2026-45447	Important/Sec.
libxml2-2.9.7-21.el8_10.5.x86_64 python3-libxml2-2.9.7-21.el8_10.5.x86_64	RHSA-2026:26354	CVE-2024-34459	Low/Sec.
libxslt-1.1.32-6.4.el8_10.x86_64	RHSA-2026:26355	CVE-2025-10911	Moderate/Sec.
kernel-4.18.0-553.134.1.el8_10.x86_64 kernel-core-4.18.0-553.134.1.el8_10.x86_64 kernel-modules-4.18.0-553.134.1.el8_10.x86_64 kernel-tools-4.18.0-553.134.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.134.1.el8_10.x86_64 python3-perf-4.18.0-553.134.1.el8_10.x86_64	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/Sec.
dracut-049-244.git20260529.el8_10.x86_64 dracut-config-rescue-049-244.git20260529.el8_10.x86_64 dracut-network-049-244.git20260529.el8_10.x86_64 dracut-squash-049-244.git20260529.el8_10.x86_64	RHSA-2026:26534	CVE-2026-6893	Important/Sec.
kernel-4.18.0-553.136.1.el8_10.x86_64 kernel-core-4.18.0-553.136.1.el8_10.x86_64 kernel-modules-4.18.0-553.136.1.el8_10.x86_64 kernel-tools-4.18.0-553.136.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.136.1.el8_10.x86_64 python3-perf-4.18.0-553.136.1.el8_10.x86_64	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/Sec.
kernel-4.18.0-553.137.1.el8_10.x86_64 kernel-core-4.18.0-553.137.1.el8_10.x86_64 kernel-modules-4.18.0-553.137.1.el8_10.x86_64 kernel-tools-4.18.0-553.137.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.137.1.el8_10.x86_64 python3-perf-4.18.0-553.137.1.el8_10.x86_64	RHSA-2026:27811	CVE-2026-46054	Important/Sec.
vim-minimal-2:8.0.1763-24.el8_10.x86_64	RHSA-2026:28553	CVE-2026-41411	Moderate/Sec.
vim-minimal-2:8.0.1763-22.el8_10.x86_64	RHSA-2026:4442	CVE-2026-25749	Moderate/Sec.
grub2-common-1:2.02-170.el8_10.1.noarch grub2-efi-x64-1:2.02-170.el8_10.1.x86_64 grub2-tools-1:2.02-170.el8_10.1.x86_64	RHSA-2026:4648	CVE-2025-61662	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

grub2-tools-efi-1:2.02-170.el8_10.1.x86_64 grub2-tools-extra-1:2.02-170.el8_10.1.x86_64 grub2-tools-minimal-1:2.02-170.el8_10.1.x86_64			
libpng-2:1.6.34-10.el8_10.x86_64	RHSA-2026:4728	CVE-2026-22695 CVE-2026-22801 CVE-2026-25646	Important/Sec.
glibc-2.28-251.el8_10.31.x86_64 glibc-all-langpacks-2.28-251.el8_10.31.x86_64 glibc-common-2.28-251.el8_10.31.x86_64 glibc-gconv-extra-2.28-251.el8_10.31.x86_64 glibc-langpack-en-2.28-251.el8_10.31.x86_64 libnsl-2.28-251.el8_10.31.x86_64	RHSA-2026:4772	CVE-2025-15281 CVE-2026-0915	Moderate/Sec.
qemu-guest-agent-15:6.2.0-53.module+el8.10.0+23760+c0926e61.6.x86_64	RHSA-2026:5578	CVE-2025-11234	Moderate/Sec.
gnutls-3.6.16-8.el8_10.5.x86_64	RHSA-2026:5585	CVE-2025-14831 CVE-2025-9820	Moderate/Sec.
platform-python-3.6.8-74.el8_10.x86_64 platform-python-devel-3.6.8-74.el8_10.x86_64 python3-libs-3.6.8-74.el8_10.x86_64	RHSA-2026:5588	CVE-2025-0938	Moderate/Sec.
kernel-4.18.0-553.115.1.el8_10.x86_64 kernel-core-4.18.0-553.115.1.el8_10.x86_64 kernel-modules-4.18.0-553.115.1.el8_10.x86_64 kernel-tools-4.18.0-553.115.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.115.1.el8_10.x86_64 python3-perf-4.18.0-553.115.1.el8_10.x86_64	RHSA-2026:6037	CVE-2025-38180 CVE-2026-23204 CVE-2026-23209	Moderate/Sec.
openssh-8.0p1-28.el8_10.x86_64 openssh-clients-8.0p1-28.el8_10.x86_64 openssh-server-8.0p1-28.el8_10.x86_64	RHSA-2026:6461	CVE-2026-3497	Important/Sec.
platform-python-3.6.8-75.el8_10.x86_64 platform-python-devel-3.6.8-75.el8_10.x86_64 python3-libs-3.6.8-75.el8_10.x86_64	RHSA-2026:6473	CVE-2026-4519	Important/Sec.
kernel-4.18.0-553.117.1.el8_10.x86_64 kernel-core-4.18.0-553.117.1.el8_10.x86_64 kernel-modules-4.18.0-553.117.1.el8_10.x86_64 kernel-tools-4.18.0-553.117.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.117.1.el8_10.x86_64 python3-perf-4.18.0-553.117.1.el8_10.x86_64	RHSA-2026:6571	CVE-2024-26984 CVE-2025-71238 CVE-2026-23193 CVE-2026-23231	Moderate/Sec.
gstreamer1-plugins-bad-free-1.16.1-6.el8_10.x86_64 gstreamer1-plugins-base-1.16.1-6.el8_10.x86_64	RHSA-2026:6750	CVE-2026-2920 CVE-2026-2921 CVE-2026-2923 CVE-2026-3082 CVE-2026-3083 CVE-2026-3085	Important/Sec.
vim-minimal-2:8.0.1763-22.el8_10.1.x86_64	RHSA-2026:6915	CVE-2026-28417 CVE-2026-28421 CVE-2026-33412	Important/Sec.
libnghttp2-1.33.0-6.el8_10.2.x86_64	RHSA-2026:7667	CVE-2026-27135	Important/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

bind-export-libs-32:9.11.36-16.el8_10.7.x86_64	RHSA-2026:8352	CVE-2026-1519	Important/Sec.
libarchive-3.3.3-7.el8_10.x86_64	RHSA-2026:8534	CVE-2026-4424 CVE-2026-5121	Important/Sec.
giflib-5.1.4-4.el8_10.x86_64	RHSA-2026:8861	CVE-2026-23868	Important/Sec.
kernel-4.18.0-553.120.1.el8_10.x86_64 kernel-core-4.18.0-553.120.1.el8_10.x86_64 kernel-modules-4.18.0-553.120.1.el8_10.x86_64 kernel-tools-4.18.0-553.120.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.120.1.el8_10.x86_64 python3-perf-4.18.0-553.120.1.el8_10.x86_64	RHSA-2026:9131	CVE-2025-68741 CVE-2026-23191	Important/Sec.
java-1.8.0-openjdk-1:1.8.0.492.b09-1.el8.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.492.b09-1.el8.x86_64	RHSA-2026:9683	CVE-2026-22007 CVE-2026-22013 CVE-2026-22016 CVE-2026-22018 CVE-2026-22021 CVE-2026-23865 CVE-2026-34268	Important/Sec.
java-17-openjdk-1:17.0.19.0.10-1.el8.x86_64 java-17-openjdk-headless-1:17.0.19.0.10-1.el8.x86_64	RHSA-2026:9686	CVE-2026-22007 CVE-2026-22013 CVE-2026-22016 CVE-2026-22018 CVE-2026-22021 CVE-2026-23865 CVE-2026-34268 CVE-2026-34282	Important/Sec.

ADS-4.0 OVA OS Upgrade Bundle includes the following rpm updates:

brotli-1.0.6-4.el8_10.x86_64	kernel-tools-4.18.0-553.94.1.el8_10.x86_64
cups-libs-1:2.2.6-66.el8_10.x86_64	kernel-tools-4.18.0-553.97.1.el8_10.x86_64
glib2-2.56.4-168.el8_10.x86_64	kernel-tools-libs-4.18.0-553.100.1.el8_10.x86_64
gnupg2-2.2.20-4.el8_10.x86_64	kernel-tools-libs-4.18.0-553.104.1.el8_10.x86_64
gnupg2-smime-2.2.20-4.el8_10.x86_64	kernel-tools-libs-4.18.0-553.105.1.el8_10.x86_64
java-1.8.0-openjdk-1:1.8.0.482.b08-1.el8.x86_64	kernel-tools-libs-4.18.0-553.107.1.el8_10.x86_64
java-1.8.0-openjdk-headless-1:1.8.0.482.b08-1.el8.x86_64	kernel-tools-libs-4.18.0-553.109.1.el8_10.x86_64
java-17-openjdk-1:17.0.15.0.6-2.el8.x86_64	kernel-tools-libs-4.18.0-553.111.1.el8_10.x86_64
java-17-openjdk-1:17.0.18.0.8-1.el8.x86_64	kernel-tools-libs-4.18.0-553.92.1.el8_10.x86_64
java-17-openjdk-headless-1:17.0.15.0.6-2.el8.x86_64	kernel-tools-libs-4.18.0-553.94.1.el8_10.x86_64
java-17-openjdk-headless-1:17.0.18.0.8-1.el8.x86_64	kernel-tools-libs-4.18.0-553.97.1.el8_10.x86_64
kernel-4.18.0-553.100.1.el8_10.x86_64	libblkid-2.32.1-48.el8_10.x86_64
kernel-4.18.0-553.104.1.el8_10.x86_64	libfdisk-2.32.1-48.el8_10.x86_64
kernel-4.18.0-553.105.1.el8_10.x86_64	libmount-2.32.1-48.el8_10.x86_64
kernel-4.18.0-553.107.1.el8_10.x86_64	libpng-2:1.6.34-9.el8_10.x86_64
kernel-4.18.0-553.109.1.el8_10.x86_64	libsmartcols-2.32.1-48.el8_10.x86_64
	libsoup-2.62.3-11.el8_10.x86_64

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

kernel-4.18.0-553.111.1.el8_10.x86_64	libsoup-2.62.3-13.el8_10.x86_64
kernel-4.18.0-553.92.1.el8_10.x86_64	libuuid-2.32.1-48.el8_10.x86_64
kernel-4.18.0-553.94.1.el8_10.x86_64	net-snmp-1:5.8-33.el8_10.x86_64
kernel-4.18.0-553.97.1.el8_10.x86_64	net-snmp-agent-libs-1:5.8-33.el8_10.x86_64
kernel-core-4.18.0-553.100.1.el8_10.x86_64	net-snmp-libs-1:5.8-33.el8_10.x86_64
kernel-core-4.18.0-553.104.1.el8_10.x86_64	net-snmp-utils-1:5.8-33.el8_10.x86_64
kernel-core-4.18.0-553.105.1.el8_10.x86_64	openssl-1:1.1.1k-14.el8_10.x86_64
kernel-core-4.18.0-553.107.1.el8_10.x86_64	openssl-1:1.1.1k-15.el8_6.x86_64
kernel-core-4.18.0-553.109.1.el8_10.x86_64	openssl-libs-1:1.1.1k-14.el8_10.x86_64
kernel-core-4.18.0-553.111.1.el8_10.x86_64	openssl-libs-1:1.1.1k-15.el8_6.x86_64
kernel-core-4.18.0-553.92.1.el8_10.x86_64	openssl-perl-1:1.1.1k-14.el8_10.x86_64
kernel-core-4.18.0-553.94.1.el8_10.x86_64	openssl-perl-1:1.1.1k-15.el8_6.x86_64
kernel-core-4.18.0-553.97.1.el8_10.x86_64	platform-python-3.6.8-72.el8_10.x86_64
kernel-modules-4.18.0-553.100.1.el8_10.x86_64	platform-python-3.6.8-73.el8_10.x86_64
kernel-modules-4.18.0-553.104.1.el8_10.x86_64	platform-python-devel-3.6.8-72.el8_10.x86_64
kernel-modules-4.18.0-553.105.1.el8_10.x86_64	platform-python-devel-3.6.8-73.el8_10.x86_64
kernel-modules-4.18.0-553.107.1.el8_10.x86_64	python3-libs-3.6.8-72.el8_10.x86_64
kernel-modules-4.18.0-553.109.1.el8_10.x86_64	python3-libs-3.6.8-73.el8_10.x86_64
kernel-modules-4.18.0-553.111.1.el8_10.x86_64	python3-perf-4.18.0-553.100.1.el8_10.x86_64
kernel-modules-4.18.0-553.92.1.el8_10.x86_64	python3-perf-4.18.0-553.104.1.el8_10.x86_64
kernel-modules-4.18.0-553.94.1.el8_10.x86_64	python3-perf-4.18.0-553.105.1.el8_10.x86_64
kernel-modules-4.18.0-553.97.1.el8_10.x86_64	python3-perf-4.18.0-553.107.1.el8_10.x86_64
kernel-tools-4.18.0-553.100.1.el8_10.x86_64	python3-perf-4.18.0-553.109.1.el8_10.x86_64
kernel-tools-4.18.0-553.104.1.el8_10.x86_64	python3-perf-4.18.0-553.111.1.el8_10.x86_64
kernel-tools-4.18.0-553.105.1.el8_10.x86_64	python3-perf-4.18.0-553.92.1.el8_10.x86_64
kernel-tools-4.18.0-553.107.1.el8_10.x86_64	python3-perf-4.18.0-553.94.1.el8_10.x86_64
kernel-tools-4.18.0-553.109.1.el8_10.x86_64	python3-perf-4.18.0-553.97.1.el8_10.x86_64
kernel-tools-4.18.0-553.111.1.el8_10.x86_64	util-linux-2.32.1-48.el8_10.x86_64
kernel-tools-4.18.0-553.92.1.el8_10.x86_64	

Security vulnerabilities resolved in ADS 4.0 OVA OS Upgrade Bundle:

Updated Package	RHSA Number	CVE	RHSA Severity
java-17-openjdk-1:17.0.15.0.6-2.el8.x86_64 java-17-openjdk-headless-1:17.0.15.0.6-2.el8.x86_64	RHSA-2025:3852		Moderate/Sec.
libpng-2:1.6.34-9.el8_10.x86_64	RHSA-2026:0241	CVE-2025-64720 CVE-2025-65018 CVE-2025-66293	Important/Sec.
openssl-1:1.1.1k-14.el8_10.x86_64 openssl-libs-1:1.1.1k-14.el8_10.x86_64 openssl-perl-1:1.1.1k-14.el8_10.x86_64	RHSA-2026:0337	CVE-2025-9230	Moderate/Sec.
libsoup-2.62.3-11.el8_10.x86_64	RHSA-2026:0421	CVE-2025-14523	Important/Sec.
kernel-4.18.0-553.92.1.el8_10.x86_64 kernel-core-4.18.0-553.92.1.el8_10.x86_64 kernel-modules-4.18.0-553.92.1.el8_10.x86_64 kernel-tools-4.18.0-553.92.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.92.1.el8_10.x86_64 python3-perf-4.18.0-553.92.1.el8_10.x86_64	RHSA-2026:0444	CVE-2025-39993 CVE-2025-40240 CVE-2025-68285	Important/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

cups-libs-1:2.2.6-66.el8_10.x86_64	RHSA-2026:0596	CVE-2025-58436 CVE-2025-61915	Moderate/Sec.
gnupg2-2.2.20-4.el8_10.x86_64 gnupg2-smime-2.2.20-4.el8_10.x86_64	RHSA-2026:0728	CVE-2025-68973	Important/Sec.
net-snmp-1:5.8-33.el8_10.x86_64 net-snmp-agent-libs-1:5.8-33.el8_10.x86_64 net-snmp-libs-1:5.8-33.el8_10.x86_64 net-snmp-utils-1:5.8-33.el8_10.x86_64	RHSA-2026:0750	CVE-2025-68615	Important/Sec.
kernel-4.18.0-553.94.1.el8_10.x86_64 kernel-core-4.18.0-553.94.1.el8_10.x86_64 kernel-modules-4.18.0-553.94.1.el8_10.x86_64 kernel-tools-4.18.0-553.94.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.94.1.el8_10.x86_64 python3-perf-4.18.0-553.94.1.el8_10.x86_64	RHSA-2026:0759	CVE-2023-53552 CVE-2025-38051 CVE-2025-39933 CVE-2025-40096 CVE-2025-68301	Important/Sec.
java-17-openjdk-1:17.0.18.0.8-1.el8.x86_64 java-17-openjdk-headless-1:17.0.18.0.8-1.el8.x86_64 java-1.8.0-openjdk-1:1.8.0.482.b08-1.el8.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.482.b08-1.el8.x86_64	RHSA-2026:0927	CVE-2025-64720 CVE-2025-65018 CVE-2026-21925 CVE-2026-21933 CVE-2026-21945	Important/Sec.
glib2-2.56.4-168.el8_10.x86_64	RHSA-2026:0991	CVE-2025-13601	Moderate/Sec.
kernel-4.18.0-553.97.1.el8_10.x86_64 kernel-core-4.18.0-553.97.1.el8_10.x86_64 kernel-modules-4.18.0-553.97.1.el8_10.x86_64 kernel-tools-4.18.0-553.97.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.97.1.el8_10.x86_64 python3-perf-4.18.0-553.97.1.el8_10.x86_64	RHSA-2026:1142	CVE-2023-53673 CVE-2025-40154 CVE-2025-40248 CVE-2025-40277	Important/Sec.
platform-python-3.6.8-72.el8_10.x86_64 platform-python-devel-3.6.8-72.el8_10.x86_64 python3-libs-3.6.8-72.el8_10.x86_64	RHSA-2026:1631	CVE-2025-12084	Moderate/Sec.
kernel-4.18.0-553.100.1.el8_10.x86_64 kernel-core-4.18.0-553.100.1.el8_10.x86_64 kernel-modules-4.18.0-553.100.1.el8_10.x86_64 kernel-tools-4.18.0-553.100.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.100.1.el8_10.x86_64 python3-perf-4.18.0-553.100.1.el8_10.x86_64	RHSA-2026:1662	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/Sec.
libblkid-2.32.1-48.el8_10.x86_64 libfdisk-2.32.1-48.el8_10.x86_64 libmount-2.32.1-48.el8_10.x86_64 libsmartcols-2.32.1-48.el8_10.x86_64 libuuid-2.32.1-48.el8_10.x86_64 util-linux-2.32.1-48.el8_10.x86_64	RHSA-2026:1852	CVE-2025-14104	Moderate/Sec.
platform-python-3.6.8-73.el8_10.x86_64 platform-python-devel-3.6.8-73.el8_10.x86_64	RHSA-2026:2128	CVE-2025-15366 CVE-2025-15367	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

python3-libs-3.6.8-73.el8_10.x86_64		CVE-2026-0865 CVE-2026-1299	
libsoup-2.62.3-13.el8_10.x86_64	RHSA-2026:2215	CVE-2026-0719 CVE-2026-1761	Important/Sec.
kernel-4.18.0-553.104.1.el8_10.x86_64 kernel-core-4.18.0-553.104.1.el8_10.x86_64 kernel-modules-4.18.0-553.104.1.el8_10.x86_64 kernel-tools-4.18.0-553.104.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.104.1.el8_10.x86_64 python3-perf-4.18.0-553.104.1.el8_10.x86_64	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/Sec.
brotli-1.0.6-4.el8_10.x86_64	RHSA-2026:2389	CVE-2025-6176	Important/Sec.
kernel-4.18.0-553.105.1.el8_10.x86_64 kernel-core-4.18.0-553.105.1.el8_10.x86_64 kernel-modules-4.18.0-553.105.1.el8_10.x86_64 kernel-tools-4.18.0-553.105.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.105.1.el8_10.x86_64 python3-perf-4.18.0-553.105.1.el8_10.x86_64	RHSA-2026:2720	CVE-2023-53762 CVE-2025-40168 CVE-2025-40304	Moderate/Sec.
openssl-1:1.1.1k-15.el8_6.x86_64 openssl-libs-1:1.1.1k-15.el8_6.x86_64 openssl-perl-1:1.1.1k-15.el8_6.x86_64	RHSA-2026:3042	CVE-2025-69419	Moderate/Sec.
kernel-4.18.0-553.107.1.el8_10.x86_64 kernel-core-4.18.0-553.107.1.el8_10.x86_64 kernel-modules-4.18.0-553.107.1.el8_10.x86_64 kernel-tools-4.18.0-553.107.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.107.1.el8_10.x86_64 python3-perf-4.18.0-553.107.1.el8_10.x86_64	RHSA-2026:3083	CVE-2025-38129 CVE-2025-38248 CVE-2025-40064 CVE-2025-68800 CVE-2026-23074	Important/Sec.
kernel-4.18.0-553.109.1.el8_10.x86_64 kernel-core-4.18.0-553.109.1.el8_10.x86_64 kernel-modules-4.18.0-553.109.1.el8_10.x86_64 kernel-tools-4.18.0-553.109.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.109.1.el8_10.x86_64 python3-perf-4.18.0-553.109.1.el8_10.x86_64	RHSA-2026:3464	CVE-2026-23097	Moderate/Sec.
kernel-4.18.0-553.111.1.el8_10.x86_64 kernel-core-4.18.0-553.111.1.el8_10.x86_64 kernel-modules-4.18.0-553.111.1.el8_10.x86_64 kernel-tools-4.18.0-553.111.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.111.1.el8_10.x86_64 python3-perf-4.18.0-553.111.1.el8_10.x86_64	RHSA-2026:3963	CVE-2025-71085 CVE-2026-23001	Moderate/Sec.

ADS-4.0 OVA Security Service Pack #13 includes the following rpm updates:

pam-1.3.1-37.el8_10.x86_64 sudo-1.9.5p2-1.el8_10.1.x86_64 platform-python-3.6.8-70.el8_10.x86_64 platform-python-devel-3.6.8-70.el8_10.x86_64	kernel-tools-4.18.0-553.71.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.71.1.el8_10.x86_64 python3-perf-4.18.0-553.71.1.el8_10.x86_64 pam-1.3.1-38.el8_10.x86_64

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

python3-libs-3.6.8-70.el8_10.x86_64	platform-python-3.6.8-71.el8_10.x86_64
kernel-4.18.0-553.60.1.el8_10.x86_64	platform-python-devel-3.6.8-71.el8_10.x86_64
kernel-core-4.18.0-553.60.1.el8_10.x86_64	python3-libs-3.6.8-71.el8_10.x86_64
kernel-modules-4.18.0-553.60.1.el8_10.x86_64	kernel-4.18.0-553.72.1.el8_10.x86_64
kernel-tools-4.18.0-553.60.1.el8_10.x86_64	kernel-core-4.18.0-553.72.1.el8_10.x86_64
kernel-tools-libs-4.18.0-553.60.1.el8_10.x86_64	kernel-modules-4.18.0-553.72.1.el8_10.x86_64
python3-perf-4.18.0-553.60.1.el8_10.x86_64	kernel-tools-4.18.0-553.72.1.el8_10.x86_64
libxml2-2.9.7-21.el8_10.1.x86_64	kernel-tools-libs-4.18.0-553.72.1.el8_10.x86_64
python3-libxml2-2.9.7-21.el8_10.1.x86_64	python3-perf-4.18.0-553.72.1.el8_10.x86_64
java-1.8.0-openjdk-1:1.8.0.462.b08-2.el8.x86_64	libudisks2-2.9.0-16.el8_10.1.x86_64
java-1.8.0-openjdk-headless-1:1.8.0.462.b08-2.el8.x86_64	udisks2-2.9.0-16.el8_10.1.x86_64
java-17-openjdk-1:17.0.16.0.8-2.el8.x86_64	kernel-4.18.0-553.74.1.el8_10.x86_64
java-17-openjdk-headless-1:17.0.16.0.8-2.el8.x86_64	kernel-core-4.18.0-553.74.1.el8_10.x86_64
microcode_ctl-4:20250512-1.el8_10.x86_64	kernel-modules-4.18.0-553.74.1.el8_10.x86_64
lz4-libs-1.8.3-5.el8_10.x86_64	kernel-tools-4.18.0-553.74.1.el8_10.x86_64
platform-python-setuptools-39.2.0-9.el8_10.noarch	kernel-tools-libs-4.18.0-553.74.1.el8_10.x86_64
python3-setuptools-39.2.0-9.el8_10.noarch	python3-perf-4.18.0-553.74.1.el8_10.x86_64
python3-setuptools-wheel-39.2.0-9.el8_10.noarch	cups-libs-1:2.2.6-63.el8_10.x86_64
kernel-4.18.0-553.62.1.el8_10.x86_64	kernel-4.18.0-553.75.1.el8_10.x86_64
kernel-core-4.18.0-553.62.1.el8_10.x86_64	kernel-core-4.18.0-553.75.1.el8_10.x86_64
kernel-modules-4.18.0-553.62.1.el8_10.x86_64	kernel-modules-4.18.0-553.75.1.el8_10.x86_64
kernel-tools-4.18.0-553.62.1.el8_10.x86_64	kernel-tools-4.18.0-553.75.1.el8_10.x86_64
kernel-tools-libs-4.18.0-553.62.1.el8_10.x86_64	kernel-tools-libs-4.18.0-553.75.1.el8_10.x86_64
python3-perf-4.18.0-553.62.1.el8_10.x86_64	python3-perf-4.18.0-553.75.1.el8_10.x86_64
glib2-2.56.4-166.el8_10.x86_64	kernel-4.18.0-553.76.1.el8_10.x86_64
kernel-4.18.0-553.63.1.el8_10.x86_64	kernel-core-4.18.0-553.76.1.el8_10.x86_64
kernel-core-4.18.0-553.63.1.el8_10.x86_64	kernel-modules-4.18.0-553.76.1.el8_10.x86_64
kernel-modules-4.18.0-553.63.1.el8_10.x86_64	kernel-tools-4.18.0-553.76.1.el8_10.x86_64
kernel-tools-4.18.0-553.63.1.el8_10.x86_64	kernel-tools-libs-4.18.0-553.76.1.el8_10.x86_64
kernel-tools-libs-4.18.0-553.63.1.el8_10.x86_64	python3-perf-4.18.0-553.76.1.el8_10.x86_64
python3-perf-4.18.0-553.63.1.el8_10.x86_64	openssh-8.0p1-26.el8_10.x86_64
perl-Errno-1.28-423.el8_10.x86_64	openssh-clients-8.0p1-26.el8_10.x86_64
perl-IO-1.38-423.el8_10.x86_64	openssh-server-8.0p1-26.el8_10.x86_64
perl-SelfLoader-1.23-423.el8_10.noarch	kernel-4.18.0-553.77.1.el8_10.x86_64
perl-interpreter-4:5.26.3-423.el8_10.x86_64	kernel-core-4.18.0-553.77.1.el8_10.x86_64
perl-libs-4:5.26.3-423.el8_10.x86_64	kernel-modules-4.18.0-553.77.1.el8_10.x86_64
perl-macros-4:5.26.3-423.el8_10.x86_64	kernel-tools-4.18.0-553.77.1.el8_10.x86_64
kernel-4.18.0-553.64.1.el8_10.x86_64	kernel-tools-libs-4.18.0-553.77.1.el8_10.x86_64
kernel-core-4.18.0-553.64.1.el8_10.x86_64	python3-perf-4.18.0-553.77.1.el8_10.x86_64
kernel-modules-4.18.0-553.64.1.el8_10.x86_64	kernel-4.18.0-553.78.1.el8_10.x86_64
kernel-tools-4.18.0-553.64.1.el8_10.x86_64	kernel-core-4.18.0-553.78.1.el8_10.x86_64
kernel-tools-libs-4.18.0-553.64.1.el8_10.x86_64	kernel-modules-4.18.0-553.78.1.el8_10.x86_64
python3-perf-4.18.0-553.64.1.el8_10.x86_64	kernel-tools-4.18.0-553.78.1.el8_10.x86_64
python3-unbound-1.16.2-5.9.el8_10.x86_64	kernel-tools-libs-4.18.0-553.78.1.el8_10.x86_64
unbound-libs-1.16.2-5.9.el8_10.x86_64	python3-perf-4.18.0-553.78.1.el8_10.x86_64
sqlite-3.26.0-20.el8_10.x86_64	gnutls-3.6.16-8.el8_10.4.x86_64
sqlite-libs-3.26.0-20.el8_10.x86_64	open-vm-tools-12.3.5-2.el8_10.1.x86_64
libxml2-2.9.7-21.el8_10.2.x86_64	vim-minimal-2:8.0.1763-21.el8_10.x86_64
python3-libxml2-2.9.7-21.el8_10.2.x86_64	kernel-4.18.0-553.79.1.el8_10.x86_64
qemu-guest-agent-15:6.2.0-53.module+el8.10.0+23081+c18b1ee3.4.x86_64	kernel-core-4.18.0-553.79.1.el8_10.x86_64
	kernel-modules-4.18.0-553.79.1.el8_10.x86_64
	kernel-tools-4.18.0-553.79.1.el8_10.x86_64

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

kernel-4.18.0-553.66.1.el8_10.x86_64 kernel-core-4.18.0-553.66.1.el8_10.x86_64 kernel-modules-4.18.0-553.66.1.el8_10.x86_64 kernel-tools-4.18.0-553.66.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.66.1.el8_10.x86_64 python3-perf-4.18.0-553.66.1.el8_10.x86_64 glibc-2.28-251.el8_10.25.x86_64 glibc-all-langpacks-2.28-251.el8_10.25.x86_64 glibc-common-2.28-251.el8_10.25.x86_64 glibc-langpack-en-2.28-251.el8_10.25.x86_64 libnsl-2.28-251.el8_10.25.x86_64 libxml2-2.9.7-21.el8_10.3.x86_64 python3-libxml2-2.9.7-21.el8_10.3.x86_64 gdk-pixbuf2-2.36.12-7.el8_10.x86_64 gdk-pixbuf2-modules-2.36.12-7.el8_10.x86_64 kernel-4.18.0-553.69.1.el8_10.x86_64 kernel-core-4.18.0-553.69.1.el8_10.x86_64 kernel-modules-4.18.0-553.69.1.el8_10.x86_64 kernel-tools-4.18.0-553.69.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.69.1.el8_10.x86_64 python3-perf-4.18.0-553.69.1.el8_10.x86_64 kernel-4.18.0-553.70.1.el8_10.x86_64 kernel-core-4.18.0-553.70.1.el8_10.x86_64 kernel-modules-4.18.0-553.70.1.el8_10.x86_64 kernel-tools-4.18.0-553.70.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.70.1.el8_10.x86_64 python3-perf-4.18.0-553.70.1.el8_10.x86_64 libarchive-3.3.3-6.el8_10.x86_64 kernel-4.18.0-553.71.1.el8_10.x86_64 kernel-core-4.18.0-553.71.1.el8_10.x86_64 kernel-modules-4.18.0-553.71.1.el8_10.x86_64	kernel-tools-libs-4.18.0-553.79.1.el8_10.x86_64 python3-perf-4.18.0-553.79.1.el8_10.x86_64 libssh-0.9.6-15.el8_10.x86_64 libssh-config-0.9.6-15.el8_10.noarch kernel-4.18.0-553.80.1.el8_10.x86_64 kernel-core-4.18.0-553.80.1.el8_10.x86_64 kernel-modules-4.18.0-553.80.1.el8_10.x86_64 kernel-tools-4.18.0-553.80.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.80.1.el8_10.x86_64 python3-perf-4.18.0-553.80.1.el8_10.x86_64 java-1.8.0-openjdk-1:1.8.0.472.b08-1.el8.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.472.b08-1.el8.x86_64 java-17-openjdk-1:17.0.17.0.10-1.el8.x86_64 java-17-openjdk-headless-1:17.0.17.0.10-1.el8.x86_64 kernel-4.18.0-553.81.1.el8_10.x86_64 kernel-core-4.18.0-553.81.1.el8_10.x86_64 kernel-modules-4.18.0-553.81.1.el8_10.x86_64 kernel-tools-4.18.0-553.81.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.81.1.el8_10.x86_64 python3-perf-4.18.0-553.81.1.el8_10.x86_64 kernel-4.18.0-553.58.1.el8_10.x86_64 kernel-core-4.18.0-553.58.1.el8_10.x86_64 kernel-modules-4.18.0-553.58.1.el8_10.x86_64 kernel-tools-4.18.0-553.58.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.58.1.el8_10.x86_64 python3-perf-4.18.0-553.58.1.el8_10.x86_64 libblockdev-2.28-7.el8_10.x86_64 libblockdev-crypto-2.28-7.el8_10.x86_64 libblockdev-fs-2.28-7.el8_10.x86_64 libblockdev-loop-2.28-7.el8_10.x86_64 libblockdev-mdraid-2.28-7.el8_10.x86_64 libblockdev-part-2.28-7.el8_10.x86_64 libblockdev-swap-2.28-7.el8_10.x86_64 libblockdev-utils-2.28-7.el8_10.x86_64

Security vulnerabilities resolved in ADS 4.0 OVA Security Service Pack #13:

Updated Package	RHSA Number	CVE	RHSA Severity
pam-1.3.1-37.el8_10.x86_64	RHSA-2025:10027	CVE-2025-6020	Important/Sec.
sudo-1.9.5p2-1.el8_10.1.x86_64	RHSA-2025:10110	CVE-2025-32462	Important/Sec.
platform-python-3.6.8-70.el8_10.x86_64 platform-python-devel-3.6.8-70.el8_10.x86_64 python3-libs-3.6.8-70.el8_10.x86_64	RHSA-2025:10128	CVE-2024-12718 CVE-2025-4138 CVE-2025-4330 CVE-2025-4435 CVE-2025-4517	Important/Sec.
kernel-4.18.0-553.60.1.el8_10.x86_64 kernel-core-4.18.0-553.60.1.el8_10.x86_64 kernel-modules-4.18.0-553.60.1.el8_10.x86_64	RHSA-2025:10669	CVE-2022-49111 CVE-2022-49136 CVE-2022-49846	Important/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

kernel-tools-4.18.0-553.60.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.60.1.el8_10.x86_64 python3-perf-4.18.0-553.60.1.el8_10.x86_64			
libxml2-2.9.7-21.el8_10.1.x86_64 python3-libxml2-2.9.7-21.el8_10.1.x86_64	RHSA-2025:10698	CVE-2025-49794 CVE-2025-49796 CVE-2025-6021	Important/Sec.
java-1.8.0-openjdk-1:1.8.0.462.b08-2.el8.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.462.b08-2.el8.x86_64	RHSA-2025:10862	CVE-2025-30749 CVE-2025-30754 CVE-2025-30761 CVE-2025-50106	Important/Sec.
java-17-openjdk-1:17.0.16.0.8-2.el8.x86_64 java-17-openjdk-headless-1:17.0.16.0.8-2.el8.x86_64	RHSA-2025:10867	CVE-2025-30749 CVE-2025-30754 CVE-2025-50059 CVE-2025-50106	Important/Sec.
microcode_ctl-4:20250512-1.el8_10.x86_64	RHSA-2025:10991	CVE-2024-28956	Moderate/Sec.
lz4-libs-1.8.3-5.el8_10.x86_64	RHSA-2025:11035	CVE-2019-17543	Moderate/Sec.
platform-python-setuptools-39.2.0-9.el8_10.noarch python3-setuptools-39.2.0-9.el8_10.noarch python3-setuptools-wheel-39.2.0-9.el8_10.noarch	RHSA-2025:11036	CVE-2025-47273	Moderate/Sec.
kernel-4.18.0-553.62.1.el8_10.x86_64 kernel-core-4.18.0-553.62.1.el8_10.x86_64 kernel-modules-4.18.0-553.62.1.el8_10.x86_64 kernel-tools-4.18.0-553.62.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.62.1.el8_10.x86_64 python3-perf-4.18.0-553.62.1.el8_10.x86_64	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/Sec.
glib2-2.56.4-166.el8_10.x86_64	RHSA-2025:11327	CVE-2024-34397 CVE-2024-52533 CVE-2025-4373	Moderate/Sec.
kernel-4.18.0-553.63.1.el8_10.x86_64 kernel-core-4.18.0-553.63.1.el8_10.x86_64 kernel-modules-4.18.0-553.63.1.el8_10.x86_64 kernel-tools-4.18.0-553.63.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.63.1.el8_10.x86_64 python3-perf-4.18.0-553.63.1.el8_10.x86_64	RHSA-2025:11455	CVE-2024-50154 CVE-2025-38086	Moderate/Sec.
perl-Errno-1.28-423.el8_10.x86_64 perl-IO-1.38-423.el8_10.x86_64 perl-SelfLoader-1.23-423.el8_10.noarch perl-interpreter-4:5.26.3-423.el8_10.x86_64 perl-libs-4:5.26.3-423.el8_10.x86_64 perl-macros-4:5.26.3-423.el8_10.x86_64	RHSA-2025:11805	CVE-2025-40909	Moderate/Sec.
kernel-4.18.0-553.64.1.el8_10.x86_64 kernel-core-4.18.0-553.64.1.el8_10.x86_64 kernel-modules-4.18.0-553.64.1.el8_10.x86_64 kernel-tools-4.18.0-553.64.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.64.1.el8_10.x86_64 python3-perf-4.18.0-553.64.1.el8_10.x86_64	RHSA-2025:11850	CVE-2022-49977 CVE-2025-21905 CVE-2025-21919	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

python3-unbound-1.16.2-5.9.el8_10.x86_64 unbound-libs-1.16.2-5.9.el8_10.x86_64	RHSA-2025:11884	CVE-2025-5994	Important/Sec.
sqlite-3.26.0-20.el8_10.x86_64 sqlite-libs-3.26.0-20.el8_10.x86_64	RHSA-2025:12010	CVE-2025-6965	Important/Sec.
libxml2-2.9.7-21.el8_10.2.x86_64 python3-libxml2-2.9.7-21.el8_10.2.x86_64	RHSA-2025:12450	CVE-2025-7425	Important/Sec.
qemu-guest-agent-15:6.2.0-53.module+el8.10.0+23081+c18b1ee3.4.x86_64	RHSA-2025:12527	CVE-2025-49133	Moderate/Sec.
kernel-4.18.0-553.66.1.el8_10.x86_64 kernel-core-4.18.0-553.66.1.el8_10.x86_64 kernel-modules-4.18.0-553.66.1.el8_10.x86_64 kernel-tools-4.18.0-553.66.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.66.1.el8_10.x86_64 python3-perf-4.18.0-553.66.1.el8_10.x86_64	RHSA-2025:12752	CVE-2022-50020 CVE-2025-21928 CVE-2025-22020 CVE-2025-37890 CVE-2025-38052 CVE-2025-38079	Important/Sec.
glibc-2.28-251.el8_10.25.x86_64 glibc-all-langpacks-2.28-251.el8_10.25.x86_64 glibc-common-2.28-251.el8_10.25.x86_64 glibc-langpack-en-2.28-251.el8_10.25.x86_64 libnsl-2.28-251.el8_10.25.x86_64	RHSA-2025:12980	CVE-2025-8058	Moderate/Sec.
libxml2-2.9.7-21.el8_10.3.x86_64 python3-libxml2-2.9.7-21.el8_10.3.x86_64	RHSA-2025:13203	CVE-2025-32415	Moderate/Sec.
gdk-pixbuf2-2.36.12-7.el8_10.x86_64 gdk-pixbuf2-modules-2.36.12-7.el8_10.x86_64	RHSA-2025:13315	CVE-2025-7345	Moderate/Sec.
kernel-4.18.0-553.69.1.el8_10.x86_64 kernel-core-4.18.0-553.69.1.el8_10.x86_64 kernel-modules-4.18.0-553.69.1.el8_10.x86_64 kernel-tools-4.18.0-553.69.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.69.1.el8_10.x86_64 python3-perf-4.18.0-553.69.1.el8_10.x86_64	RHSA-2025:13589	CVE-2021-47670 CVE-2024-56644 CVE-2025-21727 CVE-2025-21759 CVE-2025-38085 CVE-2025-38159	Moderate/Sec.
kernel-4.18.0-553.70.1.el8_10.x86_64 kernel-core-4.18.0-553.70.1.el8_10.x86_64 kernel-modules-4.18.0-553.70.1.el8_10.x86_64 kernel-tools-4.18.0-553.70.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.70.1.el8_10.x86_64 python3-perf-4.18.0-553.70.1.el8_10.x86_64	RHSA-2025:13960	CVE-2025-22097 CVE-2025-37914 CVE-2025-38250 sCVE-2025-38380	Important/Sec.
libarchive-3.3.3-6.el8_10.x86_64	RHSA-2025:14135	CVE-2025-5914	Important/Sec.
kernel-4.18.0-553.71.1.el8_10.x86_64 kernel-core-4.18.0-553.71.1.el8_10.x86_64 kernel-modules-4.18.0-553.71.1.el8_10.x86_64 kernel-tools-4.18.0-553.71.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.71.1.el8_10.x86_64 python3-perf-4.18.0-553.71.1.el8_10.x86_64	RHSA-2025:14438	CVE-2025-22058 CVE-2025-38200	Moderate/Sec.
pam-1.3.1-38.el8_10.x86_64	RHSA-2025:14557	CVE-2025-6020	Important/Sec.
platform-python-3.6.8-71.el8_10.x86_64 platform-python-devel-3.6.8-71.el8_10.x86_64 python3-libs-3.6.8-71.el8_10.x86_64	RHSA-2025:14560	CVE-2025-8194	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

kernel-4.18.0-553.72.1.el8_10.x86_64 kernel-core-4.18.0-553.72.1.el8_10.x86_64 kernel-modules-4.18.0-553.72.1.el8_10.x86_64 kernel-tools-4.18.0-553.72.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.72.1.el8_10.x86_64 python3-perf-4.18.0-553.72.1.el8_10.x86_64	RHSA-2025:15008	CVE-2025-38211 CVE-2025-38332 CVE-2025-38464 CVE-2025-38477	Moderate/Sec.
libudisks2-2.9.0-16.el8_10.1.x86_64 udisks2-2.9.0-16.el8_10.1.x86_64	RHSA-2025:15017	CVE-2025-8067	Important/Sec.
kernel-4.18.0-553.74.1.el8_10.x86_64 kernel-core-4.18.0-553.74.1.el8_10.x86_64 kernel-modules-4.18.0-553.74.1.el8_10.x86_64 kernel-tools-4.18.0-553.74.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.74.1.el8_10.x86_64 python3-perf-4.18.0-553.74.1.el8_10.x86_64	RHSA-2025:15471	CVE-2022-49985 CVE-2025-38352	Important/Sec.
cups-libs-1:2.2.6-63.el8_10.x86_64	RHSA-2025:15702	CVE-2025-58060	Important/Sec.
kernel-4.18.0-553.75.1.el8_10.x86_64 kernel-core-4.18.0-553.75.1.el8_10.x86_64 kernel-modules-4.18.0-553.75.1.el8_10.x86_64 kernel-tools-4.18.0-553.75.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.75.1.el8_10.x86_64 python3-perf-4.18.0-553.75.1.el8_10.x86_64	RHSA-2025:15785	CVE-2023-53125 CVE-2025-38350 CVE-2025-38392 CVE-2025-38449	Important/Sec.
kernel-4.18.0-553.76.1.el8_10.x86_64 kernel-core-4.18.0-553.76.1.el8_10.x86_64 kernel-modules-4.18.0-553.76.1.el8_10.x86_64 kernel-tools-4.18.0-553.76.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.76.1.el8_10.x86_64 python3-perf-4.18.0-553.76.1.el8_10.x86_64	RHSA-2025:16372	CVE-2025-38461 CVE-2025-38498 CVE-2025-38556	Moderate/Sec.
openssh-8.0p1-26.el8_10.x86_64 openssh-clients-8.0p1-26.el8_10.x86_64 openssh-server-8.0p1-26.el8_10.x86_64	RHSA-2025:16823	CVE-2025-26465	Moderate/Sec.
kernel-4.18.0-553.77.1.el8_10.x86_64 kernel-core-4.18.0-553.77.1.el8_10.x86_64 kernel-modules-4.18.0-553.77.1.el8_10.x86_64 kernel-tools-4.18.0-553.77.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.77.1.el8_10.x86_64 python3-perf-4.18.0-553.77.1.el8_10.x86_64	RHSA-2025:16919	CVE-2022-50087 CVE-2025-22026 CVE-2025-37797 CVE-2025-38718	Moderate/Sec.
kernel-4.18.0-553.78.1.el8_10.x86_64 kernel-core-4.18.0-553.78.1.el8_10.x86_64 kernel-modules-4.18.0-553.78.1.el8_10.x86_64 kernel-tools-4.18.0-553.78.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.78.1.el8_10.x86_64 python3-perf-4.18.0-553.78.1.el8_10.x86_64	RHSA-2025:17397	CVE-2025-38527 CVE-2025-39730	Moderate/Sec.
gnutls-3.6.16-8.el8_10.4.x86_64	RHSA-2025:17415	CVE-2025-32988 CVE-2025-32990 CVE-2025-6395	Moderate/Sec.
open-vm-tools-12.3.5-2.el8_10.1.x86_64	RHSA-2025:17509	CVE-2025-41244	Important/Sec.
vim-minimal-2:8.0.1763-21.el8_10.x86_64	RHSA-2025:17715	CVE-2025-53905 CVE-2025-53906	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

kernel-4.18.0-553.79.1.el8_10.x86_64 kernel-core-4.18.0-553.79.1.el8_10.x86_64 kernel-modules-4.18.0-553.79.1.el8_10.x86_64 kernel-tools-4.18.0-553.79.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.79.1.el8_10.x86_64 python3-perf-4.18.0-553.79.1.el8_10.x86_64	RHSA-2025:17797	CVE-2022-50228 CVE-2023-53305	Moderate/Sec.
libssh-0.9.6-15.el8_10.x86_64 libssh-config-0.9.6-15.el8_10.noarch	RHSA-2025:18286	CVE-2025-5318	Moderate/Sec.
kernel-4.18.0-553.80.1.el8_10.x86_64 kernel-core-4.18.0-553.80.1.el8_10.x86_64 kernel-modules-4.18.0-553.80.1.el8_10.x86_64 kernel-tools-4.18.0-553.80.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.80.1.el8_10.x86_64 python3-perf-4.18.0-553.80.1.el8_10.x86_64	RHSA-2025:18297	CVE-2023-53373 CVE-2025-39751 CVE-2025-39757	Moderate/Sec.
java-1.8.0-openjdk-1:1.8.0.472.b08-1.el8.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.472.b08-1.el8.x86_64	RHSA-2025:18815	CVE-2025-53057 CVE-2025-53066	Moderate/Sec.
java-17-openjdk-1:17.0.17.0.10-1.el8.x86_64 java-17-openjdk-headless-1:17.0.17.0.10-1.el8.x86_64	RHSA-2025:18821	CVE-2025-53057 CVE-2025-53066	Moderate/Sec.
kernel-4.18.0-553.81.1.el8_10.x86_64 kernel-core-4.18.0-553.81.1.el8_10.x86_64 kernel-modules-4.18.0-553.81.1.el8_10.x86_64 kernel-tools-4.18.0-553.81.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.81.1.el8_10.x86_64 python3-perf-4.18.0-553.81.1.el8_10.x86_64	RHSA-2025:19102	CVE-2022-50386 CVE-2023-53297 CVE-2023-53386 CVE-2025-39817 CVE-2025-39841 CVE-2025-39849	Moderate/Sec.
kernel-4.18.0-553.58.1.el8_10.x86_64 kernel-core-4.18.0-553.58.1.el8_10.x86_64 kernel-modules-4.18.0-553.58.1.el8_10.x86_64 kernel-tools-4.18.0-553.58.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.58.1.el8_10.x86_64 python3-perf-4.18.0-553.58.1.el8_10.x86_64	RHSA-2025:9580	CVE-2022-48919 CVE-2024-50301 CVE-2024-53064 CVE-2025-21764	Moderate/Sec.
libblockdev-2.28-7.el8_10.x86_64 libblockdev-crypto-2.28-7.el8_10.x86_64 libblockdev-fs-2.28-7.el8_10.x86_64 libblockdev-loop-2.28-7.el8_10.x86_64 libblockdev-mdraid-2.28-7.el8_10.x86_64 libblockdev-part-2.28-7.el8_10.x86_64 libblockdev-swap-2.28-7.el8_10.x86_64 libblockdev-utils-2.28-7.el8_10.x86_64	RHSA-2025:9878	CVE-2025-6019	Important/Sec.

ADS-4.0 OVA Security Service Pack #12 includes the following rpm updates:

grub2-common-1:2.02-162.el8_10.noarch grub2-efi-x64-1:2.02-162.el8_10.x86_64 grub2-tools-1:2.02-162.el8_10.x86_64 grub2-tools-extra-1:2.02-162.el8_10.x86_64 grub2-tools-minimal-1:2.02-162.el8_10.x86_64 freetype-2.9.1-10.el8_10.x86_64 libxslt-1.1.32-6.1.el8_10.x86_64	python3-perf-4.18.0-553.52.1.el8_10.x86_64 libjpeg-turbo-1.5.3-14.el8_10.x86_64 compat-openssl10-1:1.0.2o-4.el8_10.1.x86_64 kernel-4.18.0-553.53.1.el8_10.x86_64 kernel-core-4.18.0-553.53.1.el8_10.x86_64 kernel-modules-4.18.0-553.53.1.el8_10.x86_64 kernel-tools-4.18.0-553.53.1.el8_10.x86_64

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

glibc-2.28-251.el8_10.16.x86_64 glibc-all-langpacks-2.28-251.el8_10.16.x86_64 glibc-common-2.28-251.el8_10.16.x86_64 glibc-langpack-en-2.28-251.el8_10.16.x86_64 libnsl-2.28-251.el8_10.16.x86_64 java-1.8.0-openjdk-1:1.8.0.452.b09-2.el8.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.452.b09-2.el8.x86_64 java-17-openjdk-1:17.0.15.0.6-2.el8.x86_64 java-17-openjdk-headless-1:17.0.15.0.6-2.el8.x86_64 kernel-4.18.0-553.50.1.el8_10.x86_64 kernel-core-4.18.0-553.50.1.el8_10.x86_64 kernel-modules-4.18.0-553.50.1.el8_10.x86_64 kernel-tools-4.18.0-553.50.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.50.1.el8_10.x86_64 python3-perf-4.18.0-553.50.1.el8_10.x86_64 expat-2.2.5-17.el8_10.x86_64 bluez-libs-5.63-5.el8_10.x86_64 libtasn1-4.13-5.el8_10.x86_64 gnutls-3.6.16-8.el8_10.3.x86_64 libsoup-2.62.3-8.el8_10.x86_64 libtiff-4.0.9-34.el8_10.x86_64 kernel-4.18.0-553.52.1.el8_10.x86_64 kernel-core-4.18.0-553.52.1.el8_10.x86_64 kernel-modules-4.18.0-553.52.1.el8_10.x86_64 kernel-tools-4.18.0-553.52.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.52.1.el8_10.x86_64	kernel-tools-libs-4.18.0-553.53.1.el8_10.x86_64 python3-perf-4.18.0-553.53.1.el8_10.x86_64 libsoup-2.62.3-9.el8_10.x86_64 gstreamer1-plugins-bad-free-1.16.1-5.el8_10.x86_64 kernel-4.18.0-553.54.1.el8_10.x86_64 kernel-core-4.18.0-553.54.1.el8_10.x86_64 kernel-modules-4.18.0-553.54.1.el8_10.x86_64 kernel-tools-4.18.0-553.54.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.54.1.el8_10.x86_64 python3-perf-4.18.0-553.54.1.el8_10.x86_64 krb5-libs-1.18.2-32.el8_10.x86_64 libxslt-1.1.32-6.2.el8_10.x86_64 glibc-2.28-251.el8_10.22.x86_64 glibc-all-langpacks-2.28-251.el8_10.22.x86_64 glibc-common-2.28-251.el8_10.22.x86_64 glibc-langpack-en-2.28-251.el8_10.22.x86_64 libnsl-2.28-251.el8_10.22.x86_64 kernel-4.18.0-553.56.1.el8_10.x86_64 kernel-core-4.18.0-553.56.1.el8_10.x86_64 kernel-modules-4.18.0-553.56.1.el8_10.x86_64 kernel-tools-4.18.0-553.56.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.56.1.el8_10.x86_64 python3-perf-4.18.0-553.56.1.el8_10.x86_64 libxml2-2.9.7-20.el8_10.x86_64 python3-libxml2-2.9.7-20.el8_10.x86_64

Security vulnerabilities resolved in ADS 4.0 OVA Security Service Pack #12:

Updated Package	RHSA Number	CVE	RHSA Severity
grub2-common-1:2.02-162.el8_10.noarch grub2-efi-x64-1:2.02-162.el8_10.x86_64 grub2-tools-1:2.02-162.el8_10.x86_64 grub2-tools-extra-1:2.02-162.el8_10.x86_64 grub2-tools-minimal-1:2.02-162.el8_10.x86_64	RHSA-2025:3367	CVE-2025-0624	Important/Sec
freetype-2.9.1-10.el8_10.x86_64	RHSA-2025:3421	CVE-2025-27363	Important/Sec
libxslt-1.1.32-6.1.el8_10.x86_64	RHSA-2025:3615	CVE-2024-55549 CVE-2025-24855	Important/Sec
glibc-2.28-251.el8_10.16.x86_64 glibc-all-langpacks-2.28-251.el8_10.16.x86_64 glibc-common-2.28-251.el8_10.16.x86_64 glibc-langpack-en-2.28-251.el8_10.16.x86_64 libnsl-2.28-251.el8_10.16.x86_64	RHSA-2025:3828	CVE-2025-0395	Moderate/Sec.
java-1.8.0-openjdk-1:1.8.0.452.b09-2.el8.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.452.b09-2.el8.x86_64	RHSA-2025:3845	CVE-2025-21587 CVE-2025-30691 CVE-2025-30698	Moderate/Sec.
java-17-openjdk-1:17.0.15.0.6-2.el8.x86_64	RHSA-20	CVE-2025-21587	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

java-17-openjdk-headless-1:17.0.15.0.6-2.el8.x86_64	25:3852	CVE-2025-30691 CVE-2025-30698	
kernel-4.18.0-553.50.1.el8_10.x86_64 kernel-core-4.18.0-553.50.1.el8_10.x86_64 kernel-modules-4.18.0-553.50.1.el8_10.x86_64 kernel-tools-4.18.0-553.50.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.50.1.el8_10.x86_64 python3-perf-4.18.0-553.50.1.el8_10.x86_64	RHSA-2025:3893	CVE-2024-53150 CVE-2024-53241	Moderate/Sec.
expat-2.2.5-17.el8_10.x86_64	RHSA-2025:3913	CVE-2024-8176	Moderate/Sec
bluez-libs-5.63-5.el8_10.x86_64	RHSA-2025:4043	CVE-2023-27349 CVE-2023-51589	Moderate/Sec.
libtasn1-4.13-5.el8_10.x86_64	RHSA-2025:4049	CVE-2024-12133	Moderate/Sec.
gnutls-3.6.16-8.el8_10.3.x86_64	RHSA-2025:4051	CVE-2024-12243	Moderate/Sec
libsoup-2.62.3-8.el8_10.x86_64	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/Sec
libtiff-4.0.9-34.el8_10.x86_64	RHSA-2025:4658	CVE-2017-17095	Moderate/Sec
kernel-4.18.0-553.52.1.el8_10.x86_64 kernel-core-4.18.0-553.52.1.el8_10.x86_64 kernel-modules-4.18.0-553.52.1.el8_10.x86_64 kernel-tools-4.18.0-553.52.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.52.1.el8_10.x86_64 python3-perf-4.18.0-553.52.1.el8_10.x86_64	RHSA-2025:7531	CVE-2022-49011 CVE-2024-53141	Important/Sec
libjpeg-turbo-1.5.3-14.el8_10.x86_64	RHSA-2025:7540	CVE-2020-13790	Moderate/Sec
compat-openssl10-1:1.0.2o-4.el8_10.1.x86_64	RHSA-2025:7895	CVE-2023-0286	Important/Sec
kernel-4.18.0-553.53.1.el8_10.x86_64 kernel-core-4.18.0-553.53.1.el8_10.x86_64 kernel-modules-4.18.0-553.53.1.el8_10.x86_64 kernel-tools-4.18.0-553.53.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.53.1.el8_10.x86_64 python3-perf-4.18.0-553.53.1.el8_10.x86_64	RHSA-2025:8056	CVE-2024-40906 CVE-2024-44970 CVE-2025-21756	Important/Sec
libsoup-2.62.3-9.el8_10.x86_64	RHSA-2025:8132	CVE-2025-2784 CVE-2025-32049 CVE-2025-32914 CVE-2025-4948	Important/Sec
gstreamer1-plugins-bad-free-1.16.1-5.el8_10.x86_64	RHSA-2025:8201	CVE-2025-3887	Important/Sec

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

kernel-4.18.0-553.54.1.el8_10.x86_64 kernel-core-4.18.0-553.54.1.el8_10.x86_64 kernel-modules-4.18.0-553.54.1.el8_10.x86_64 kernel-tools-4.18.0-553.54.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.54.1.el8_10.x86_64 python3-perf-4.18.0-553.54.1.el8_10.x86_64	RHSA-2025:8246	CVE-2024-43842	Moderate/Sec
krb5-libs-1.18.2-32.el8_10.x86_64	RHSA-2025:8411	CVE-2025-3576	Moderate/Sec
libxslt-1.1.32-6.2.el8_10.x86_64	RHSA-2025:8676	CVE-2023-40403	Moderate/Sec
glibc-2.28-251.el8_10.22.x86_64 glibc-all-langpacks-2.28-251.el8_10.22.x86_64 glibc-common-2.28-251.el8_10.22.x86_64 glibc-langpack-en-2.28-251.el8_10.22.x86_64 libnsl-2.28-251.el8_10.22.x86_64	RHSA-2025:8686	CVE-2025-4802	Moderate/Sec
kernel-4.18.0-553.56.1.el8_10.x86_64 kernel-core-4.18.0-553.56.1.el8_10.x86_64 kernel-modules-4.18.0-553.56.1.el8_10.x86_64 kernel-tools-4.18.0-553.56.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.56.1.el8_10.x86_64 python3-perf-4.18.0-553.56.1.el8_10.x86_64	RHSA-2025:8743	CVE-2022-49395	Moderate/Sec
libxml2-2.9.7-20.el8_10.x86_64 python3-libxml2-2.9.7-20.el8_10.x86_64	RHSA-2025:8958	CVE-2025-32414	Moderate/Sec

ADS-4.0 OVA Security Service Pack #11 includes the following rpm updates:

libgcc-8.5.0-23.el8_10.x86_64 libgfortran-8.5.0-23.el8_10.x86_64 libgomp-8.5.0-23.el8_10.x86_64 libquadmath-8.5.0-23.el8_10.x86_64 libstdc++-8.5.0-23.el8_10.x86_64 libxml2-2.9.7-18.el8_10.2.x86_64 python3-libxml2-2.9.7-18.el8_10.2.x86_64 bind-export-libs-32:9.11.36-16.el8_10.4.x86_64 kernel-4.18.0-553.44.1.el8_10.x86_64 kernel-core-4.18.0-553.44.1.el8_10.x86_64 kernel-modules-4.18.0-553.44.1.el8_10.x86_64 kernel-tools-4.18.0-553.44.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.44.1.el8_10.x86_64 python3-perf-4.18.0-553.44.1.el8_10.x86_64 libxml2-2.9.7-19.el8_10.x86_64	python3-libxml2-2.9.7-19.el8_10.x86_64 krb5-libs-1.18.2-31.el8_10.x86_64 kernel-4.18.0-553.45.1.el8_10.x86_64 kernel-core-4.18.0-553.45.1.el8_10.x86_64 kernel-modules-4.18.0-553.45.1.el8_10.x86_64 kernel-tools-4.18.0-553.45.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.45.1.el8_10.x86_64 python3-perf-4.18.0-553.45.1.el8_10.x86_64 kernel-4.18.0-553.46.1.el8_10.x86_64 kernel-core-4.18.0-553.46.1.el8_10.x86_64 kernel-modules-4.18.0-553.46.1.el8_10.x86_64 kernel-tools-4.18.0-553.46.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.46.1.el8_10.x86_64 python3-perf-4.18.0-553.46.1.el8_10.x86_64

Security vulnerabilities resolved in ADS 4.0 OVA Security Service Pack #11:

Updated Package	RHSA Number	CVE	RHSA Severity
libgcc-8.5.0-23.el8_10.x86_64 libgfortran-8.5.0-23.el8_10.x86_64	RHSA-2025:1301	CVE-2020-11023	Moderate/Sec

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

libgomp-8.5.0-23.el8_10.x86_64 libquadmath-8.5.0-23.el8_10.x86_64 libstdc++-8.5.0-23.el8_10.x86_64			
libxml2-2.9.7-18.el8_10.2.x86_64 python3-libxml2-2.9.7-18.el8_10.2.x86_64	RHSA-2025:1517	CVE-2022-49043	Moderate/Sec
bind-export-libs-32:9.11.36-16.el8_10.4.x86_64	RHSA-2025:1675	CVE-2024-11187	Important/Sec
kernel-4.18.0-553.44.1.el8_10.x86_64 kernel-core-4.18.0-553.44.1.el8_10.x86_64 kernel-modules-4.18.0-553.44.1.el8_10.x86_64 kernel-tools-4.18.0-553.44.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.44.1.el8_10.x86_64 python3-perf-4.18.0-553.44.1.el8_10.x86_64	RHSA-2025:2473	CVE-2024-50302 CVE-2024-53197 CVE-2024-57807 CVE-2024-57979	Important/Sec
libxml2-2.9.7-19.el8_10.x86_64 python3-libxml2-2.9.7-19.el8_10.x86_64	RHSA-2025:2686	CVE-2024-56171 CVE-2025-24928	Important/Sec
krb5-libs-1.18.2-31.el8_10.x86_64	RHSA-2025:2722		Moderate/Sec
kernel-4.18.0-553.45.1.el8_10.x86_64 kernel-core-4.18.0-553.45.1.el8_10.x86_64 kernel-modules-4.18.0-553.45.1.el8_10.x86_64 kernel-tools-4.18.0-553.45.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.45.1.el8_10.x86_64 python3-perf-4.18.0-553.45.1.el8_10.x86_64	RHSA-2025:3026	CVE-2023-52922	Important/Sec
kernel-4.18.0-553.46.1.el8_10.x86_64 kernel-core-4.18.0-553.46.1.el8_10.x86_64 kernel-modules-4.18.0-553.46.1.el8_10.x86_64 kernel-tools-4.18.0-553.46.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.46.1.el8_10.x86_64 python3-perf-4.18.0-553.46.1.el8_10.x86_64	RHSA-2025:3260	CVE-2025-21785	Important/Sec

ADS-4.0 OVA Security Service Pack #10 includes the following rpm updates:

kernel-4.18.0-553.30.1.el8_10.x86_64	python3-perf-4.18.0-553.27.1.el8_10.x86_64
kernel-core-4.18.0-553.30.1.el8_10.x86_64	krb5-libs-1.18.2-30.el8_10.x86_64
kernel-modules-4.18.0-553.30.1.el8_10.x86_64	bzip2-1.0.6-27.el8_10.x86_64
kernel-tools-4.18.0-553.30.1.el8_10.x86_64	bzip2-libs-1.0.6-27.el8_10.x86_64
kernel-tools-libs-4.18.0-553.30.1.el8_10.x86_64	gstreamer1-plugins-base-1.16.1-4.el8_10.x86_64
python3-perf-4.18.0-553.30.1.el8_10.x86_64	expat-2.2.5-16.el8_10.x86_64
pam-1.3.1-36.el8_10.x86_64	kernel-4.18.0-553.34.1.el8_10.x86_64
platform-python-3.6.8-69.el8_10.x86_64	kernel-core-4.18.0-553.34.1.el8_10.x86_64
platform-python-devel-3.6.8-69.el8_10.x86_64	kernel-modules-4.18.0-553.34.1.el8_10.x86_64
python3-libs-3.6.8-69.el8_10.x86_64	kernel-tools-4.18.0-553.34.1.el8_10.x86_64
kernel-4.18.0-553.32.1.el8_10.x86_64	kernel-tools-libs-4.18.0-553.34.1.el8_10.x86_64
kernel-core-4.18.0-553.32.1.el8_10.x86_64	python3-perf-4.18.0-553.34.1.el8_10.x86_64
kernel-modules-4.18.0-553.32.1.el8_10.x86_64	cups-libs-1:2.2.6-62.el8_10.x86_64
kernel-tools-4.18.0-553.32.1.el8_10.x86_64	bzip2-1.0.6-28.el8_10.x86_64
kernel-tools-libs-4.18.0-553.32.1.el8_10.x86_64	bzip2-libs-1.0.6-28.el8_10.x86_64
python3-perf-4.18.0-553.32.1.el8_10.x86_64	python3-unbound-1.16.2-5.8.el8_10.x86_64
python3-scipy-1.0.0-	unbound-libs-1.16.2-5.8.el8_10.x86_64

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

21.module+el8.10.0+20784+edafcd43.x86_64 python36-3.6.8- 39.module+el8.10.0+20784+edafcd43.x86_64 bluez-libs-5.63-3.el8_10.x86_64 tuned-2.22.1-5.el8_10.noarch libsndfile-1.0.28-16.el8_10.x86_64 gstreamer1-plugins-base-1.16.1-5.el8_10.x86_64 java-1.8.0-openjdk-1:1.8.0.432.b06-2.el8.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.432.b06- 2.el8.x86_64 libtiff-4.0.9-33.el8_10.x86_64 kernel-4.18.0-553.27.1.el8_10.x86_64 kernel-core-4.18.0-553.27.1.el8_10.x86_64 kernel-modules-4.18.0-553.27.1.el8_10.x86_64 kernel-tools-4.18.0-553.27.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.27.1.el8_10.x86_64	kernel-4.18.0-553.37.1.el8_10.x86_64 kernel-core-4.18.0-553.37.1.el8_10.x86_64 kernel-modules-4.18.0-553.37.1.el8_10.x86_64 kernel-tools-4.18.0-553.37.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.37.1.el8_10.x86_64 python3-perf-4.18.0-553.37.1.el8_10.x86_64 kernel-4.18.0-553.40.1.el8_10.x86_64 kernel-core-4.18.0-553.40.1.el8_10.x86_64 kernel-modules-4.18.0-553.40.1.el8_10.x86_64 kernel-tools-4.18.0-553.40.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.40.1.el8_10.x86_64 python3-perf-4.18.0-553.40.1.el8_10.x86_64

Security vulnerabilities resolved in ADS 4.0 OVA Security Service Pack #10:

Updated Package	RHSA Number	CVE	RHSA Severity
kernel-4.18.0-553.30.1.el8_10.x86_64 kernel-core-4.18.0-553.30.1.el8_10.x86_64 kernel-modules-4.18.0-553.30.1.el8_10.x86_64 kernel-tools-4.18.0-553.30.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.30.1.el8_10.x86_64 python3-perf-4.18.0-553.30.1.el8_10.x86_64	RHSA-2024:10281	CVE-2024-27043 CVE-2024-27399 CVE-2024-38564 CVE-2024-46858	Moderate/Sec
pam-1.3.1-36.el8_10.x86_64	RHSA-2024:10379	CVE-2024-10041 CVE-2024-10963	Important/Sec.
platform-python-3.6.8-69.el8_10.x86_64 platform-python-devel-3.6.8-69.el8_10.x86_64 python3-libs-3.6.8-69.el8_10.x86_64	RHSA-2024:10779	CVE-2024-11168 CVE-2024-9287	Important/Sec.
kernel-4.18.0-553.32.1.el8_10.x86_64 kernel-core-4.18.0-553.32.1.el8_10.x86_64 kernel-modules-4.18.0-553.32.1.el8_10.x86_64 kernel-tools-4.18.0-553.32.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.32.1.el8_10.x86_64 python3-perf-4.18.0-553.32.1.el8_10.x86_64	RHSA-2024:10943	CVE-2024-46695 CVE-2024-49949 CVE-2024-50082 CVE-2024-50099 CVE-2024-50110 CVE-2024-50142 CVE-2024-50192 CVE-2024-50256 CVE-2024-50264	Moderate/Sec.
python3-scipy-1.0.0- 21.module+el8.10.0+20784+edafcd43.x86_64 python36-3.6.8- 39.module+el8.10.0+20784+edafcd43.x86_64	RHSA-2024:10953	CVE-2024-53899	Important/Sec.
bluez-libs-5.63-3.el8_10.x86_64	RHSA-2024:11154	CVE-2023-45866	Moderate/Sec.
tuned-2.22.1-5.el8_10.noarch	RHSA-2024:11161	CVE-2024-52337	Moderate/Sec.
libsndfile-1.0.28-16.el8_10.x86_64	RHSA-20	CVE-2024-50612	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

	24:11192		
gstreamer1-plugins-base-1.16.1-5.el8_10.x86_64	RHSA-2024:11345	CVE-2024-47538 CVE-2024-47607 CVE-2024-47615	Important/Sec.
java-1.8.0-openjdk-1:1.8.0.432.b06-2.el8.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.432.b06-2.el8.x86_64	RHSA-2024:8117	CVE-2023-48161 CVE-2024-21208 CVE-2024-21210 CVE-2024-21217 CVE-2024-21235	Moderate/Sec.
libtiff-4.0.9-33.el8_10.x86_64	RHSA-2024:8833	CVE-2024-7006	Moderate/Sec.
kernel-4.18.0-553.27.1.el8_10.x86_64 kernel-core-4.18.0-553.27.1.el8_10.x86_64 kernel-modules-4.18.0-553.27.1.el8_10.x86_64 kernel-tools-4.18.0-553.27.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.27.1.el8_10.x86_64 python3-perf-4.18.0-553.27.1.el8_10.x86_64	RHSA-2024:8856	CVE-2022-48773 CVE-2022-48936 CVE-2023-52492 CVE-2024-24857 CVE-2024-26851 CVE-2024-26924 CVE-2024-26976 CVE-2024-27017 CVE-2024-27062 CVE-2024-35839 CVE-2024-35898 CVE-2024-35939 CVE-2024-38540 CVE-2024-38541 CVE-2024-38586 CVE-2024-38608 CVE-2024-39503 CVE-2024-40924 CVE-2024-40961 CVE-2024-40983 CVE-2024-40984 CVE-2024-41009 CVE-2024-41042 CVE-2024-41066 CVE-2024-41092 CVE-2024-41093 CVE-2024-42070 CVE-2024-42079 CVE-2024-42244 CVE-2024-42284 CVE-2024-42292 CVE-2024-42301 CVE-2024-43854 CVE-2024-43880 CVE-2024-43889 CVE-2024-43892 CVE-2024-44935 CVE-2024-44989 CVE-2024-44990 CVE-2024-45018	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

		CVE-2024-46826 CVE-2024-47668	
krb5-libs-1.18.2-30.el8_10.x86_64	RHSA-2024:8860	CVE-2024-3596	Important/Sec.
bzip2-1.0.6-27.el8_10.x86_64 bzip2-libs-1.0.6-27.el8_10.x86_64	RHSA-2024:8922	CVE-2019-12900	Low/Sec.
gstreamer1-plugins-base-1.16.1-4.el8_10.x86_64	RHSA-2024:9056	CVE-2024-4453	Moderate/Sec.
expat-2.2.5-16.el8_10.x86_64	RHSA-2024:9502	CVE-2024-50602	Moderate/Sec.
kernel-4.18.0-553.34.1.el8_10.x86_64 kernel-core-4.18.0-553.34.1.el8_10.x86_64 kernel-modules-4.18.0-553.34.1.el8_10.x86_64 kernel-tools-4.18.0-553.34.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.34.1.el8_10.x86_64 python3-perf-4.18.0-553.34.1.el8_10.x86_64	RHSA-2025:0065	CVE-2024-53088 CVE-2024-53122	Important/Sec.
cups-libs-1:2.2.6-62.el8_10.x86_64	RHSA-2025:0083	CVE-2024-47175	Low/Sec.
bzip2-1.0.6-28.el8_10.x86_64 bzip2-libs-1.0.6-28.el8_10.x86_64	RHSA-2025:0733	CVE-2019-12900	Moderate/Sec.
python3-unbound-1.16.2-5.8.el8_10.x86_64 unbound-libs-1.16.2-5.8.el8_10.x86_64	RHSA-2025:0837	CVE-2024-1488 CVE-2024-8508	Important/Sec.
kernel-4.18.0-553.37.1.el8_10.x86_64 kernel-core-4.18.0-553.37.1.el8_10.x86_64 kernel-modules-4.18.0-553.37.1.el8_10.x86_64 kernel-tools-4.18.0-553.37.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.37.1.el8_10.x86_64 python3-perf-4.18.0-553.37.1.el8_10.x86_64	RHSA-2025:1068	CVE-2024-26935 CVE-2024-50275	Moderate/Sec.
kernel-4.18.0-553.40.1.el8_10.x86_64 kernel-core-4.18.0-553.40.1.el8_10.x86_64 kernel-modules-4.18.0-553.40.1.el8_10.x86_64 kernel-tools-4.18.0-553.40.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.40.1.el8_10.x86_64 python3-perf-4.18.0-553.40.1.el8_10.x86_64	RHSA-2025:1266	CVE-2024-53104	Important/Sec.

ADS-4.0 OVA Security Service Pack #9 includes the following rpm updates:

kernel-4.18.0-553.8.1.el8_10.x86_64	python3-perf-4.18.0-553.16.1.el8_10.x86_64
kernel-core-4.18.0-553.8.1.el8_10.x86_64	wget-1.19.5-12.el8_10.x86_64
kernel-modules-4.18.0-553.8.1.el8_10.x86_64	orc-0.4.28-4.el8_10.x86_64
kernel-tools-4.18.0-553.8.1.el8_10.x86_64	krb5-libs-1.18.2-29.el8_10.x86_64
kernel-tools-libs-4.18.0-553.8.1.el8_10.x86_64	bind-export-libs-32:9.11.36-16.el8_10.2.x86_64
python3-perf-4.18.0-553.8.1.el8_10.x86_64	platform-python-setuptools-39.2.0-8.el8_10.noarch
libnghttp2-1.33.0-6.el8_10.1.x86_64	python3-setuptools-39.2.0-8.el8_10.noarch
less-530-3.el8_10.x86_64	python3-setuptools-wheel-39.2.0-8.el8_10.noarch
linux-firmware-20240610-122.git90df68d2.el8_10.noarch	curl-7.61.1-34.el8_10.2.x86_64
openldap-2.4.46-19.el8_10.x86_64	libcurl-7.61.1-34.el8_10.2.x86_64
	bubblewrap-0.4.0-2.el8_10.x86_64

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

cups-libs-1:2.2.6-60.el8_10.x86_64 qemu-guest-agent-15:6.2.0-49.module+el8.10.0+21533+3df3c4b6.x86_64 qemu-guest-agent-15:6.2.0-50.module+el8.10.0+22027+db0a70a4.x86_64 java-1.8.0-openjdk-1:1.8.0.422.b05-2.el8.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.422.b05-2.el8.x86_64 qt5-qtbase-5.15.3-8.el8_10.x86_64 qt5-qtbase-common-5.15.3-8.el8_10.noarch qt5-qtbase-gui-5.15.3-8.el8_10.x86_64 libtiff-4.0.9-32.el8_10.x86_64 kernel-4.18.0-553.16.1.el8_10.x86_64 kernel-core-4.18.0-553.16.1.el8_10.x86_64 kernel-modules-4.18.0-553.16.1.el8_10.x86_64 kernel-tools-4.18.0-553.16.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.16.1.el8_10.x86_64	gtk-update-icon-cache-3.22.30-12.el8_10.x86_64 qemu-guest-agent-15:6.2.0-53.module+el8.10.0+22268+f82ccd96.x86_64 platform-python-3.6.8-67.el8_10.x86_64 platform-python-devel-3.6.8-67.el8_10.x86_64 python3-libs-3.6.8-67.el8_10.x86_64 expat-2.2.5-15.el8_10.x86_64 kernel-4.18.0-553.22.1.el8_10.x86_64 kernel-core-4.18.0-553.22.1.el8_10.x86_64 kernel-modules-4.18.0-553.22.1.el8_10.x86_64 kernel-tools-4.18.0-553.22.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.22.1.el8_10.x86_64 python3-perf-4.18.0-553.22.1.el8_10.x86_64 linux-firmware-20240827-124.git3cff7109.el8_10.noarch openssl-1:1.1.1k-14.el8_6.x86_64 openssl-libs-1:1.1.1k-14.el8_6.x86_64 openssl-perl-1:1.1.1k-14.el8_6.x86_64

Security vulnerabilities resolved in ADS 4.0 OVA Security Service Pack #9:

Updated Package	RHSA Number	CVE	RHSA Severity
kernel-4.18.0-553.8.1.el8_10.x86_64 kernel-core-4.18.0-553.8.1.el8_10.x86_64 kernel-modules-4.18.0-553.8.1.el8_10.x86_64 kernel-tools-4.18.0-553.8.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.8.1.el8_10.x86_64 python3-perf-4.18.0-553.8.1.el8_10.x86_64	RHSA-2024:4211	CVE-2020-26555 CVE-2021-46909 CVE-2021-46972 CVE-2021-47069 CVE-2021-47073 CVE-2021-47353 CVE-2021-47356 CVE-2023-5090 CVE-2023-52464 CVE-2023-52560 CVE-2023-52615 CVE-2023-52700 CVE-2023-52835 CVE-2024-26656 CVE-2024-26675 CVE-2024-26735 CVE-2024-26801 CVE-2024-26826 CVE-2024-26907 CVE-2024-26982 CVE-2024-27397 CVE-2024-35888 CVE-2024-35890 CVE-2024-36004	Important/Sec.
libnghttp2-1.33.0-6.el8_10.1.x86_64	RHSA-2024:4252	CVE-2024-28182	Moderate/Sec.
less-530-3.el8_10.x86_64	RHSA-20	CVE-2022-48624	Important/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

	24:4256	CVE-2024-32487	
linux-firmware-20240610-122.git90df68d2.el8_10.noarch	RHSA-2024:4262	CVE-2023-31346	Moderate/Sec.
openldap-2.4.46-19.el8_10.x86_64	RHSA-2024:4264	CVE-2023-2953	Low/Sec.
cups-libs-1:2.2.6-60.el8_10.x86_64	RHSA-2024:4265	CVE-2024-35235	Moderate/Sec.
qemu-guest-agent-15:6.2.0-49.module+el8.10.0+21533+3df3c4b6.x86_64	RHSA-2024:4351	CVE-2024-4418	Low/Sec.
qemu-guest-agent-15:6.2.0-50.module+el8.10.0+22027+db0a70a4.x86_64	RHSA-2024:4420	CVE-2024-4467	Important/Sec.
java-1.8.0-openjdk-1:1.8.0.422.b05-2.el8.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.422.b05-2.el8.x86_64	RHSA-2024:4563	CVE-2024-21131 CVE-2024-21138 CVE-2024-21140 CVE-2024-21144 CVE-2024-21145 CVE-2024-21147	Important/Sec.
qt5-qtbase-5.15.3-8.el8_10.x86_64 qt5-qtbase-common-5.15.3-8.el8_10.noarch qt5-qtbase-gui-5.15.3-8.el8_10.x86_64	RHSA-2024:4617	CVE-2024-39936	Important/Sec.
libtiff-4.0.9-32.el8_10.x86_64	RHSA-2024:5079	CVE-2018-15209 CVE-2023-25433 CVE-2023-52356 CVE-2023-6228	Moderate/Sec.
kernel-4.18.0-553.16.1.el8_10.x86_64 kernel-core-4.18.0-553.16.1.el8_10.x86_64 kernel-modules-4.18.0-553.16.1.el8_10.x86_64 kernel-tools-4.18.0-553.16.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.16.1.el8_10.x86_64 python3-perf-4.18.0-553.16.1.el8_10.x86_64	RHSA-2024:5101	CVE-2021-46939 CVE-2021-47548 CVE-2021-47579 CVE-2022-48743 CVE-2023-28746 CVE-2023-52451 CVE-2023-52463 CVE-2023-52619 CVE-2023-52622 CVE-2023-52653 CVE-2023-52658 CVE-2023-52845 CVE-2023-52847 CVE-2023-52864 CVE-2024-21823 CVE-2024-26586 CVE-2024-26669 CVE-2024-26698 CVE-2024-26733 CVE-2024-26802 CVE-2024-26843 CVE-2024-26878 CVE-2024-26921	Important/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

		CVE-2024-26960 CVE-2024-27010 CVE-2024-33621 CVE-2024-35801 CVE-2024-35807 CVE-2024-35876 CVE-2024-35893 CVE-2024-35947 CVE-2024-36886 CVE-2024-36921 CVE-2024-36927 CVE-2024-38596 CVE-2024-39276	
wget-1.19.5-12.el8_10.x86_64	RHSA-2024:5299	CVE-2024-38428	Moderate/Sec.
orc-0.4.28-4.el8_10.x86_64	RHSA-2024:5306	CVE-2024-40897	Moderate/Sec.
krb5-libs-1.18.2-29.el8_10.x86_64	RHSA-2024:5312	CVE-2024-37370 CVE-2024-37371	Moderate/Sec.
bind-export-libs-32:9.11.36-16.el8_10.2.x86_64	RHSA-2024:5524	CVE-2024-1737 CVE-2024-1975	Important/Sec.
platform-python-setuptools-39.2.0-8.el8_10.noarch python3-setuptools-39.2.0-8.el8_10.noarch python3-setuptools-wheel-39.2.0-8.el8_10.noarch	RHSA-2024:5530	CVE-2024-6345	Important/Sec.
curl-7.61.1-34.el8_10.2.x86_64	RHSA-2024:5654	CVE-2024-2398	Moderate/Sec.
bubblewrap-0.4.0-2.el8_10.x86_64	RHSA-2024:6422	CVE-2024-42472	Important/Sec.
gtk-update-icon-cache-3.22.30-12.el8_10.x86_64	RHSA-2024:6963	CVE-2024-6655	Moderate/Sec.
qemu-guest-agent-15:6.2.0-53.module+el8.10.0+22268+f82ccd96.x86_64	RHSA-2024:6964	CVE-2024-3446 CVE-2024-7383 CVE-2024-7409	Moderate/Sec.
platform-python-3.6.8-67.el8_10.x86_64 platform-python-devel-3.6.8-67.el8_10.x86_64 python3-libs-3.6.8-67.el8_10.x86_64	RHSA-2024:6975	CVE-2024-4032 CVE-2024-6232 CVE-2024-6923	Moderate/Sec.
expat-2.2.5-15.el8_10.x86_64	RHSA-2024:6989	CVE-2024-45490 CVE-2024-45491 CVE-2024-45492	Moderate/Sec.
kernel-4.18.0-553.22.1.el8_10.x86_64 kernel-core-4.18.0-553.22.1.el8_10.x86_64 kernel-modules-4.18.0-553.22.1.el8_10.x86_64 kernel-tools-4.18.0-553.22.1.el8_10.x86_64	RHSA-2024:7000		Important/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

kernel-tools-libs-4.18.0-553.22.1.el8_10.x86_64 python3-perf-4.18.0-553.22.1.el8_10.x86_64			
linux-firmware-20240827-124.git3cff7109.el8_10.noarch	RHSA-2024:7481	CVE-2023-20584 CVE-2023-31356	Important/Sec.
openssl-1:1.1.1k-14.el8_6.x86_64 openssl-libs-1:1.1.1k-14.el8_6.x86_64 openssl-perl-1:1.1.1k-14.el8_6.x86_64	RHSA-2024:7848	CVE-2024-5535	Low/Sec.

ADS-4.0 OVA Security Service Pack #8 includes the following rpm updates:

libmaxminddb-1.2.0-10.el8_9.1.x86_64	kernel-modules-4.18.0-553.el8_10.x86_64
tcpdump-14:4.9.3-3.el8_9.1.x86_64	kernel-tools-4.18.0-553.el8_10.x86_64
nss-3.90.0-6.el8_9.x86_64	kernel-tools-libs-4.18.0-553.el8_10.x86_64
nss-softokn-3.90.0-6.el8_9.x86_64	python3-perf-4.18.0-553.el8_10.x86_64
nss-softokn-freebl-3.90.0-6.el8_9.x86_64	squashfs-tools-4.3-21.el8.x86_64
nss-sysinit-3.90.0-6.el8_9.x86_64	pam-1.3.1-33.el8.x86_64
nss-util-3.90.0-6.el8_9.x86_64	openssh-8.0p1-24.el8.x86_64
sudo-1.9.5p2-1.el8_9.x86_64	openssh-clients-8.0p1-24.el8.x86_64
kernel-4.18.0-513.18.1.el8_9.x86_64	openssh-server-8.0p1-24.el8.x86_64
kernel-core-4.18.0-513.18.1.el8_9.x86_64	linux-firmware-20240111-121.gitb3132c18.el8.noarch
kernel-modules-4.18.0-513.18.1.el8_9.x86_64	grub2-common-1:2.02-156.el8.noarch
kernel-tools-4.18.0-513.18.1.el8_9.x86_64	grub2-efi-x64-1:2.02-156.el8.x86_64
kernel-tools-libs-4.18.0-513.18.1.el8_9.x86_64	grub2-tools-1:2.02-156.el8.x86_64
python3-perf-4.18.0-513.18.1.el8_9.x86_64	grub2-tools-extra-1:2.02-156.el8.x86_64
python3-unbound-1.16.2-5.el8_9.2.x86_64	grub2-tools-minimal-1:2.02-156.el8.x86_64
unbound-libs-1.16.2-5.el8_9.2.x86_64	systemd-239-82.el8.x86_64
curl-7.61.1-33.el8_9.5.x86_64	systemd-libs-239-82.el8.x86_64
libcurl-7.61.1-33.el8_9.5.x86_64	systemd-pam-239-82.el8.x86_64
kernel-4.18.0-513.24.1.el8_9.x86_64	systemd-udev-239-82.el8.x86_64
kernel-core-4.18.0-513.24.1.el8_9.x86_64	traceroute-3:2.1.0-8.el8.x86_64
kernel-modules-4.18.0-513.24.1.el8_9.x86_64	gmp-1:6.1.2-11.el8.x86_64
kernel-tools-4.18.0-513.24.1.el8_9.x86_64	libssh-0.9.6-14.el8.x86_64
kernel-tools-libs-4.18.0-513.24.1.el8_9.x86_64	libssh-config-0.9.6-14.el8.noarch
python3-perf-4.18.0-513.24.1.el8_9.x86_64	qemu-guest-agent-15:6.2.0-49.module+el8.10.0+21533+3df3c4b6.x86_64
less-530-2.el8_9.x86_64	krb5-libs-1.18.2-27.el8_10.x86_64
expat-2.2.5-11.el8_9.1.x86_64	glibc-2.28-251.el8_10.1.x86_64
python3-unbound-1.16.2-5.el8_9.6.x86_64	glibc-all-langpacks-2.28-251.el8_10.1.x86_64
unbound-libs-1.16.2-5.el8_9.6.x86_64	glibc-common-2.28-251.el8_10.1.x86_64
bind-export-libs-32:9.11.36-11.el8_9.1.x86_64	glibc-langpack-en-2.28-251.el8_10.1.x86_64
dhcp-client-12:4.3.6-49.el8_9.1.x86_64	libnsl-2.28-251.el8_10.1.x86_64
dhcp-common-12:4.3.6-49.el8_9.1.noarch	bind-export-libs-32:9.11.36-14.el8_10.x86_64
dhcp-libs-12:4.3.6-49.el8_9.1.x86_64	dhcp-client-12:4.3.6-50.el8_10.x86_64
gnutls-3.6.16-8.el8_9.3.x86_64	dhcp-common-12:4.3.6-50.el8_10.noarch
java-1.8.0-openjdk-1:1.8.0.412.b08-2.el8.x86_64	dhcp-libs-12:4.3.6-50.el8_10.x86_64
java-1.8.0-openjdk-headless-1:1.8.0.412.b08-2.el8.x86_64	gdk-pixbuf2-2.36.12-6.el8_10.x86_64
shim-x64-15.8-4.el8_9.x86_64	gdk-pixbuf2-modules-2.36.12-6.el8_10.x86_64
glibc-2.28-236.el8_9.13.x86_64	glibc-2.28-251.el8_10.2.x86_64
glibc-all-langpacks-2.28-236.el8_9.13.x86_64	glibc-all-langpacks-2.28-251.el8_10.2.x86_64
glibc-common-2.28-236.el8_9.13.x86_64	glibc-common-2.28-251.el8_10.2.x86_64
glibc-langpack-en-2.28-236.el8_9.13.x86_64	glibc-langpack-en-2.28-251.el8_10.2.x86_64

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

libnsl-2.28-236.el8_9.13.x86_64 qemu-guest-agent-15:6.2.0-49.module+el8.10.0+21533+3df3c4b6.x86_64 libX11-1.6.8-8.el8.x86_64 libX11-common-1.6.8-8.el8.noarch libX11-xcb-1.6.8-8.el8.x86_64 harfbuzz-1.7.5-4.el8.x86_64 libsndfile-1.0.28-14.el8.x86_64 libtiff-4.0.9-31.el8.x86_64 gstreamer1-plugins-bad-free-1.16.1-4.el8.x86_64 gstreamer1-plugins-base-1.16.1-3.el8.x86_64 kernel-4.18.0-553.el8_10.x86_64 kernel-core-4.18.0-553.el8_10.x86_64	libnsl-2.28-251.el8_10.2.x86_64 platform-python-3.6.8-62.el8_10.x86_64 platform-python-devel-3.6.8-62.el8_10.x86_64 python3-libs-3.6.8-62.el8_10.x86_64 kernel-4.18.0-553.5.1.el8_10.x86_64 kernel-core-4.18.0-553.5.1.el8_10.x86_64 kernel-modules-4.18.0-553.5.1.el8_10.x86_64 kernel-tools-4.18.0-553.5.1.el8_10.x86_64 kernel-tools-libs-4.18.0-553.5.1.el8_10.x86_64 python3-perf-4.18.0-553.5.1.el8_10.x86_64 libxml2-2.9.7-18.el8_10.1.x86_64 python3-libxml2-2.9.7-18.el8_10.1.x86_64

Security vulnerabilities resolved in ADS 4.0 OVA Security Service Pack #8:

Updated Package	RHSA Number	CVE	RHSA Severity
libmaxminddb-1.2.0-10.el8_9.1.x86_64	RHSA-2024:0768	CVE-2020-28241	Moderate/Sec.
tcpdump-14:4.9.3-3.el8_9.1.x86_64	RHSA-2024:0769	CVE-2021-41043	Moderate/Sec.
nss-3.90.0-6.el8_9.x86_64 nss-softokn-3.90.0-6.el8_9.x86_64 nss-softokn-freebl-3.90.0-6.el8_9.x86_64 nss-sysinit-3.90.0-6.el8_9.x86_64 nss-util-3.90.0-6.el8_9.x86_64	RHSA-2024:0786	CVE-2023-6135	Moderate/Sec.
sudo-1.9.5p2-1.el8_9.x86_64	RHSA-2024:0811		Moderate/Sec.
kernel-4.18.0-513.18.1.el8_9.x86_64 kernel-core-4.18.0-513.18.1.el8_9.x86_64 kernel-modules-4.18.0-513.18.1.el8_9.x86_64 kernel-tools-4.18.0-513.18.1.el8_9.x86_64 kernel-tools-libs-4.18.0-513.18.1.el8_9.x86_64 python3-perf-4.18.0-513.18.1.el8_9.x86_64	RHSA-2024:0897	CVE-2022-3545 CVE-2022-41858 CVE-2023-1073 CVE-2023-1838 CVE-2023-2166 CVE-2023-2176 CVE-2023-40283 CVE-2023-45871 CVE-2023-4623 CVE-2023-46813 CVE-2023-4921 CVE-2023-5717 CVE-2023-6356 CVE-2023-6535 CVE-2023-6536 CVE-2023-6606 CVE-2023-6610 CVE-2023-6817 CVE-2024-0646	Important/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

python3-unbound-1.16.2-5.el8_9.2.x86_64 unbound-libs-1.16.2-5.el8_9.2.x86_64	RHSA-2024:0965	CVE-2023-50387 CVE-2023-50868	Important/Sec.
curl-7.61.1-33.el8_9.5.x86_64 libcurl-7.61.1-33.el8_9.5.x86_64	RHSA-2024:1601	CVE-2023-28322 CVE-2023-38546 CVE-2023-46218	Moderate/Sec.
kernel-4.18.0-513.24.1.el8_9.x86_64 kernel-core-4.18.0-513.24.1.el8_9.x86_64 kernel-modules-4.18.0-513.24.1.el8_9.x86_64 kernel-tools-4.18.0-513.24.1.el8_9.x86_64 kernel-tools-libs-4.18.0-513.24.1.el8_9.x86_64 python3-perf-4.18.0-513.24.1.el8_9.x86_64	RHSA-2024:1607	CVE-2021-33631 CVE-2022-38096 CVE-2023-51042 CVE-2023-6931 CVE-2024-0565 CVE-2024-1086	Important/Sec.
less-530-2.el8_9.x86_64	RHSA-2024:1610	CVE-2022-48624	Moderate/Sec.
expat-2.2.5-11.el8_9.1.x86_64	RHSA-2024:1615	CVE-2023-52425	Moderate/Sec.
python3-unbound-1.16.2-5.el8_9.6.x86_64 unbound-libs-1.16.2-5.el8_9.6.x86_64	RHSA-2024:1751	CVE-2024-1488	Important/Sec.
bind-export-libs-32:9.11.36-11.el8_9.1.x86_64 dhcp-client-12:4.3.6-49.el8_9.1.x86_64 dhcp-common-12:4.3.6-49.el8_9.1.noarch dhcp-libs-12:4.3.6-49.el8_9.1.x86_64	RHSA-2024:1782	CVE-2023-4408 CVE-2023-50387 CVE-2023-50868	Important/Sec.
gnutls-3.6.16-8.el8_9.3.x86_64	RHSA-2024:1784	CVE-2024-28834	Moderate/Sec.
java-1.8.0-openjdk-1:1.8.0.412.b08-2.el8.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.412.b08-2.el8.x86_64	RHSA-2024:1818	CVE-2024-21011 CVE-2024-21068 CVE-2024-21085 CVE-2024-21094	Moderate/Sec.
shim-x64-15.8-4.el8_9.x86_64	RHSA-2024:1902	CVE-2023-40546 CVE-2023-40547 CVE-2023-40548 CVE-2023-40549 CVE-2023-40550 CVE-2023-40551	Important/Sec.
glibc-2.28-236.el8_9.13.x86_64 glibc-all-langpacks-2.28-236.el8_9.13.x86_64 glibc-common-2.28-236.el8_9.13.x86_64	RHSA-2024:2722	CVE-2024-2961	Important/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

glibc-langpack-en-2.28-236.el8_9.13.x86_64 libnsl-2.28-236.el8_9.13.x86_64			
qemu-guest-agent-15:6.2.0-49.module+el8.10.0+21533+3df3c4b6.x86_64	RHSA-2024:2962	CVE-2023-3255 CVE-2023-5088 CVE-2023-6683 CVE-2023-6693	Moderate/Sec.
libX11-1.6.8-8.el8.x86_64 libX11-common-1.6.8-8.el8.noarch libX11-xcb-1.6.8-8.el8.x86_64	RHSA-2024:2973	CVE-2023-43785 CVE-2023-43786 CVE-2023-43787	Moderate/Sec.
harfbuzz-1.7.5-4.el8.x86_64	RHSA-2024:2980	CVE-2023-25193	Moderate/Sec.
libsndfile-1.0.28-14.el8.x86_64	RHSA-2024:3030	CVE-2022-33065	Moderate/Sec.
libtiff-4.0.9-31.el8.x86_64	RHSA-2024:3059	CVE-2022-4645	Moderate/Sec.
gstreamer1-plugins-bad-free-1.16.1-4.el8.x86_64	RHSA-2024:3060	CVE-2023-40474 CVE-2023-40475 CVE-2023-40476	Moderate/Sec.
gstreamer1-plugins-base-1.16.1-3.el8.x86_64	RHSA-2024:3088	CVE-2023-37328	Moderate/Sec.
kernel-4.18.0-553.el8_10.x86_64 kernel-core-4.18.0-553.el8_10.x86_64 kernel-modules-4.18.0-553.el8_10.x86_64 kernel-tools-4.18.0-553.el8_10.x86_64 kernel-tools-libs-4.18.0-553.el8_10.x86_64 python3-perf-4.18.0-553.el8_10.x86_64	RHSA-2024:3138		Moderate/Sec.
squashfs-tools-4.3-21.el8.x86_64	RHSA-2024:3139	CVE-2021-40153 CVE-2021-41072	Moderate/Sec.
pam-1.3.1-33.el8.x86_64	RHSA-2024:3163	CVE-2024-22365	Moderate/Sec.
openssh-8.0p1-24.el8.x86_64 openssh-clients-8.0p1-24.el8.x86_64 openssh-server-8.0p1-24.el8.x86_64	RHSA-2024:3166	CVE-2020-15778	Moderate/Sec.
linux-firmware-20240111-121.gitb3132c18.el8.noarch	RHSA-2024:3178	CVE-2022-46329 CVE-2023-20592	Important/Sec.
grub2-common-1:2.02-156.el8.noarch grub2-efi-x64-1:2.02-156.el8.x86_64 grub2-tools-1:2.02-156.el8.x86_64 grub2-tools-extra-1:2.02-156.el8.x86_64 grub2-tools-minimal-1:2.02-156.el8.x86_64	RHSA-2024:3184	CVE-2023-4692 CVE-2023-4693 CVE-2024-1048	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

systemd-239-82.el8.x86_64 systemd-libs-239-82.el8.x86_64 systemd-pam-239-82.el8.x86_64 systemd-udev-239-82.el8.x86_64	RHSA-2024:3203	CVE-2023-7008	Moderate/Sec.
traceroute-3:2.1.0-8.el8.x86_64	RHSA-2024:3211	CVE-2023-46316	Moderate/Sec.
gmp-1:6.1.2-11.el8.x86_64	RHSA-2024:3214	CVE-2021-43618	Moderate/Sec.
libssh-0.9.6-14.el8.x86_64 libssh-config-0.9.6-14.el8.noarch	RHSA-2024:3233	CVE-2023-6004 CVE-2023-6918	Low/Sec.
qemu-guest-agent-15:6.2.0-49.module+el8.10.0+21533+3df3c4b6.x86_64	RHSA-2024:3253	CVE-2024-2494	Moderate/Sec.
krb5-libs-1.18.2-27.el8_10.x86_64	RHSA-2024:3268	CVE-2024-26458 CVE-2024-26461	Low/Sec.
glibc-2.28-251.el8_10.1.x86_64 glibc-all-langpacks-2.28-251.el8_10.1.x86_64 glibc-common-2.28-251.el8_10.1.x86_64 glibc-langpack-en-2.28-251.el8_10.1.x86_64 libnsl-2.28-251.el8_10.1.x86_64	RHSA-2024:3269	CVE-2024-2961	Important/Sec.
bind-export-libs-32:9.11.36-14.el8_10.x86_64 dhcp-client-12:4.3.6-50.el8_10.x86_64 dhcp-common-12:4.3.6-50.el8_10.noarch dhcp-libs-12:4.3.6-50.el8_10.x86_64	RHSA-2024:3271	CVE-2023-4408 CVE-2023-50387 CVE-2023-50868	Important/Sec.
gdk-pixbuf2-2.36.12-6.el8_10.x86_64 gdk-pixbuf2-modules-2.36.12-6.el8_10.x86_64	RHSA-2024:3341	CVE-2022-48622	Moderate/Sec.
glibc-2.28-251.el8_10.2.x86_64 glibc-all-langpacks-2.28-251.el8_10.2.x86_64 glibc-common-2.28-251.el8_10.2.x86_64 glibc-langpack-en-2.28-251.el8_10.2.x86_64 libnsl-2.28-251.el8_10.2.x86_64	RHSA-2024:3344	CVE-2024-33599 CVE-2024-33600 CVE-2024-33601 CVE-2024-33602	Important/Sec.
platform-python-3.6.8-62.el8_10.x86_64 platform-python-devel-3.6.8-62.el8_10.x86_64 python3-libs-3.6.8-62.el8_10.x86_64	RHSA-2024:3347	CVE-2023-6597 CVE-2024-0450	Important/Sec.
kernel-4.18.0-553.5.1.el8_10.x86_64 kernel-core-4.18.0-553.5.1.el8_10.x86_64 kernel-modules-4.18.0-553.5.1.el8_10.x86_64 kernel-tools-4.18.0-553.5.1.el8_10.x86_64 kernel-tools-libs-4.18.0-	RHSA-2024:3618	CVE-2019-25162 CVE-2020-36777 CVE-2021-46934 CVE-2021-47013 CVE-2021-47055 CVE-2021-47118 CVE-2021-47153 CVE-2021-47171	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

553.5.1.el8_10.x86_64 python3-perf-4.18.0- 553.5.1.el8_10.x86_64		CVE-2021-47185 CVE-2022-48627 CVE-2022-48669 CVE-2023-52439 CVE-2023-52445 CVE-2023-52477 CVE-2023-52513 CVE-2023-52520 CVE-2023-52528 CVE-2023-52565 CVE-2023-52578 CVE-2023-52594 CVE-2023-52595 CVE-2023-52610 CVE-2023-6240 CVE-2024-0340 CVE-2024-23307 CVE-2024-25744 CVE-2024-26593 CVE-2024-26603 CVE-2024-26615 CVE-2024-26642 CVE-2024-26643 CVE-2024-26659 CVE-2024-26664 CVE-2024-26743 CVE-2024-26744 CVE-2024-26779 CVE-2024-26872 CVE-2024-26901 CVE-2024-26919 CVE-2024-26933 CVE-2024-26934 CVE-2024-26964 CVE-2024-26973 CVE-2024-26993 CVE-2024-27059	
libxml2-2.9.7-18.el8_10.1.x86_64 python3-libxml2-2.9.7- 18.el8_10.1.x86_64	RHSA-2024:3626	CVE-2024-25062	Moderate/Sec.

ADS-4.0 OVA Security Service Pack #7 includes the following rpm updates:

avahi-libs-0.7-21.el8.x86_64 avahi-libs-0.7-21.el8_9.1.x86_64 bind-export-libs-32:9.11.36-11.el8_9.x86_64 bind-export-libs-32:9.11.36-8.el8_8.2.x86_64 cups-libs-1:2.2.6-54.el8_9.x86_64 fwupd-1.7.8-2.el8.x86_64 glibc-2.28-225.el8_8.6.x86_64	nss-util-3.90.0-4.el8_9.x86_64 open-vm-tools-12.2.5-3.el8_9.1.x86_64 openssh-8.0p1-19.el8_9.2.x86_64 openssh-clients-8.0p1-19.el8_9.2.x86_64 openssh-server-8.0p1-19.el8_9.2.x86_64 openssl-1:1.1.1k-12.el8_9.x86_64 openssl-libs-1:1.1.1k-12.el8_9.x86_64

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

glibc-all-langpacks-2.28-225.el8_8.6.x86_64	openssl-perl-1:1.1.1k-12.el8_9.x86_64
glibc-common-2.28-225.el8_8.6.x86_64	perl-HTTP-Tiny-0.074-2.el8.noarch
glibc-langpack-en-2.28-225.el8_8.6.x86_64	pixman-0.38.4-3.el8_9.x86_64
gnutls-3.6.16-8.el8_9.1.x86_64	platform-python-3.6.8-51.el8_8.2.x86_64
gnutls-3.6.16-8.el8_9.x86_64	platform-python-3.6.8-56.el8_9.2.x86_64
gstreamer1-plugins-bad-free-1.16.1-2.el8_9.x86_64	platform-python-3.6.8-56.el8_9.3.x86_64
java-1.8.0-openjdk-1:1.8.0.392.b08-4.el8.x86_64	platform-python-3.6.8-56.el8_9.x86_64
java-1.8.0-openjdk-1:1.8.0.402.b06-2.el8.x86_64	platform-python-devel-3.6.8-51.el8_8.2.x86_64
java-1.8.0-openjdk-headless-1:1.8.0.392.b08-4.el8.x86_64	platform-python-devel-3.6.8-56.el8_9.2.x86_64
	platform-python-devel-3.6.8-56.el8_9.3.x86_64
java-1.8.0-openjdk-headless-1:1.8.0.402.b06-2.el8.x86_64	platform-python-devel-3.6.8-56.el8_9.x86_64
	platform-python-pip-9.0.3-23.el8.noarch
kernel-4.18.0-513.11.1.el8_9.x86_64	procps-ng-3.3.15-14.el8.x86_64
kernel-4.18.0-513.5.1.el8_9.x86_64	python3-libs-3.6.8-51.el8_8.2.x86_64
kernel-4.18.0-513.9.1.el8_9.x86_64	python3-libs-3.6.8-56.el8_9.2.x86_64
kernel-core-4.18.0-513.11.1.el8_9.x86_64	python3-libs-3.6.8-56.el8_9.3.x86_64
kernel-core-4.18.0-513.5.1.el8_9.x86_64	python3-libs-3.6.8-56.el8_9.x86_64
kernel-core-4.18.0-513.9.1.el8_9.x86_64	python3-libxml2-2.9.7-18.el8_9.x86_64
kernel-modules-4.18.0-513.11.1.el8_9.x86_64	python3-perf-4.18.0-513.11.1.el8_9.x86_64
kernel-modules-4.18.0-513.5.1.el8_9.x86_64	python3-perf-4.18.0-513.5.1.el8_9.x86_64
kernel-modules-4.18.0-513.9.1.el8_9.x86_64	python3-perf-4.18.0-513.9.1.el8_9.x86_64
kernel-tools-4.18.0-513.11.1.el8_9.x86_64	python3-pip-9.0.3-23.el8.noarch
kernel-tools-4.18.0-513.5.1.el8_9.x86_64	python3-pip-wheel-9.0.3-23.el8.noarch
kernel-tools-4.18.0-513.9.1.el8_9.x86_64	python3-rpm-4.14.3-28.el8_9.x86_64
kernel-tools-libs-4.18.0-513.11.1.el8_9.x86_64	qemu-guest-agent-15:6.2.0-40.module+el8.9.0+20056+d9fb1ac3.1.x86_64
kernel-tools-libs-4.18.0-513.5.1.el8_9.x86_64	
kernel-tools-libs-4.18.0-513.9.1.el8_9.x86_64	qemu-guest-agent-15:6.2.0-40.module+el8.9.0+20867+9a6a0901.2.x86_64
libX11-1.6.8-6.el8.x86_64	qt5-qtbase-5.15.3-5.el8.x86_64
libX11-common-1.6.8-6.el8.noarch	qt5-qtbase-common-5.15.3-5.el8.noarch
libX11-xcb-1.6.8-6.el8.x86_64	qt5-qtbase-gui-5.15.3-5.el8.x86_64
libfastjson-0.99.9-2.el8.x86_64	qt5-qtsvg-5.15.3-2.el8.x86_64
libnghttp2-1.33.0-5.el8_8.x86_64	rpm-4.14.3-28.el8_9.x86_64
libnsl-2.28-225.el8_8.6.x86_64	rpm-build-libs-4.14.3-28.el8_9.x86_64
libssh-0.9.6-13.el8_9.x86_64	rpm-libs-4.14.3-28.el8_9.x86_64
libssh-config-0.9.6-13.el8_9.noarch	rpm-plugin-selinux-4.14.3-28.el8_9.x86_64
libxml2-2.9.7-18.el8_9.x86_64	rpm-plugin-systemd-inhibit-4.14.3-28.el8_9.x86_64
linux-firmware-20230824-119.git0e048b06.el8_9.noarch	shadow-utils-2:4.6-19.el8.x86_64
	sqlite-3.26.0-19.el8_9.x86_64
nss-3.90.0-4.el8_9.x86_64	sqlite-libs-3.26.0-19.el8_9.x86_64
nss-softokn-3.90.0-4.el8_9.x86_64	tpm2-tss-2.3.2-5.el8.x86_64
nss-softokn-freebl-3.90.0-4.el8_9.x86_64	
nss-sysinit-3.90.0-4.el8_9.x86_64	

Security vulnerabilities resolved in ADS 4.0 OVA Security Service Pack #7:

Updated Package	RHSA Number	CVE	RHSA Severity
glibc-2.28-225.el8_8.6.x86_64 glibc-all-langpacks-2.28-225.el8_8.6.x86_64 glibc-common-2.28-225.el8_8.6.x86_64	RHSA-2023:5455	CVE-2023-4527 CVE-2023-4806 CVE-2023-4813	Important/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

glibc-langpack-en-2.28-225.el8_8.6.x86_64 libnsl-2.28-225.el8_8.6.x86_64		CVE-2023-4911	
bind-export-libs-32:9.11.36-8.el8_8.2.x86_64	RHSA-2023:5474	CVE-2023-3341	Important/Sec.
java-1.8.0-openjdk-1:1.8.0.392.b08-4.el8.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.392.b08-4.el8.x86_64	RHSA-2023:5731	CVE-2022-40433 CVE-2023-22067 CVE-2023-22081	Moderate/Sec.
libnghttp2-1.33.0-5.el8_8.x86_64	RHSA-2023:5837	CVE-2023-44487	Important/Sec.
platform-python-3.6.8-51.el8_8.2.x86_64 platform-python-devel-3.6.8-51.el8_8.2.x86_64 python3-libs-3.6.8-51.el8_8.2.x86_64	RHSA-2023:5997	CVE-2023-40217	Important/Sec.
qt5-qtsvg-5.15.3-2.el8.x86_64	RHSA-2023:6961	CVE-2023-32573	Low/Sec.
qt5-qtbase-5.15.3-5.el8.x86_64 qt5-qtbase-common-5.15.3-5.el8.noarch qt5-qtbase-gui-5.15.3-5.el8.x86_64	RHSA-2023:6967	CVE-2023-33285 CVE-2023-34410 CVE-2023-37369 CVE-2023-38197	Moderate/Sec.
libfastjson-0.99.9-2.el8.x86_64	RHSA-2023:6976	CVE-2020-12762	Moderate/Sec.
qemu-guest-agent-15:6.2.0-40.module+el8.9.0+20056+d9fb1ac3.1.x86_64	RHSA-2023:6980	CVE-2021-3750 CVE-2023-3301	Moderate/Sec.
libX11-1.6.8-6.el8.x86_64 libX11-common-1.6.8-6.el8.noarch libX11-xcb-1.6.8-6.el8.x86_64	RHSA-2023:7029	CVE-2023-3138	Moderate/Sec.
kernel-4.18.0-513.5.1.el8_9.x86_64 kernel-core-4.18.0-513.5.1.el8_9.x86_64 kernel-modules-4.18.0-513.5.1.el8_9.x86_64 kernel-tools-4.18.0-513.5.1.el8_9.x86_64 kernel-tools-libs-4.18.0-513.5.1.el8_9.x86_64 python3-perf-4.18.0-513.5.1.el8_9.x86_64	RHSA-2023:7077	CVE-2021-43975 CVE-2022-28388 CVE-2022-3594 CVE-2022-3640 CVE-2022-40982 CVE-2022-42895 CVE-2022-45887 CVE-2022-4744 CVE-2023-0458 CVE-2023-0590 CVE-2023-0597 CVE-2023-1073 CVE-2023-1074 CVE-2023-1075 CVE-2023-1079 CVE-2023-1118 CVE-2023-1206 CVE-2023-1252 CVE-2023-1382 CVE-2023-1855	Important/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

		CVE-2023-1989 CVE-2023-1998 CVE-2023-23455 CVE-2023-2513 CVE-2023-26545 CVE-2023-28328 CVE-2023-28772 CVE-2023-31084 CVE-2023-3141 CVE-2023-31436 CVE-2023-3161 CVE-2023-3212 CVE-2023-3268 CVE-2023-33203 CVE-2023-35823 CVE-2023-35824 CVE-2023-35825 CVE-2023-3772 CVE-2023-4132 CVE-2023-4732	
linux-firmware-20230824-119.git0e048b06.el8_9.noarch	RHSA-2023:7109	CVE-2023-20569	Moderate/Sec.
shadow-utils-2:4.6-19.el8.x86_64	RHSA-2023:7112	CVE-2023-4641	Low/Sec.
platform-python-3.6.8-56.el8_9.x86_64 platform-python-devel-3.6.8-56.el8_9.x86_64 python3-libs-3.6.8-56.el8_9.x86_64	RHSA-2023:7151	CVE-2007-4559	Moderate/Sec.
cups-libs-1:2.2.6-54.el8_9.x86_64	RHSA-2023:7165	CVE-2023-32324 CVE-2023-34241	Moderate/Sec.
tpm2-tss-2.3.2-5.el8.x86_64	RHSA-2023:7166	CVE-2023-22745	Low/Sec.
perl-HTTP-Tiny-0.074-2.el8.noarch	RHSA-2023:7174	CVE-2023-31486	Moderate/Sec.
platform-python-pip-9.0.3-23.el8.noarch python3-pip-9.0.3-23.el8.noarch python3-pip-wheel-9.0.3-23.el8.noarch	RHSA-2023:7176	CVE-2007-4559	Moderate/Sec.
bind-export-libs-32:9.11.36-11.el8_9.x86_64	RHSA-2023:7177	CVE-2022-3094	Moderate/Sec.
procps-ng-3.3.15-14.el8.x86_64	RHSA-2023:7187	CVE-2023-4016	Low/Sec.
fwupd-1.7.8-2.el8.x86_64	RHSA-2023:7189	CVE-2022-3287	Moderate/Sec.
avahi-libs-0.7-21.el8.x86_64	RHSA-	CVE-2023-1981	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

	2023:7190		
open-vm-tools-12.2.5-3.el8_9.1.x86_64	RHSA-2023:7265	CVE-2023-34058 CVE-2023-34059	Important/Sec.
kernel-4.18.0-513.9.1.el8_9.x86_64 kernel-core-4.18.0-513.9.1.el8_9.x86_64 kernel-modules-4.18.0-513.9.1.el8_9.x86_64 kernel-tools-4.18.0-513.9.1.el8_9.x86_64 kernel-tools-libs-4.18.0-513.9.1.el8_9.x86_64 python3-perf-4.18.0-513.9.1.el8_9.x86_64	RHSA-2023:7549	CVE-2022-45884 CVE-2022-45886 CVE-2022-45919 CVE-2023-1192 CVE-2023-2163 CVE-2023-3812 CVE-2023-5178	Important/Sec.
avahi-libs-0.7-21.el8_9.1.x86_64	RHSA-2023:7836	CVE-2021-3468 CVE-2023-38469 CVE-2023-38470 CVE-2023-38471 CVE-2023-38472 CVE-2023-38473	Moderate/Sec.
gstreamer1-plugins-bad-free-1.16.1-2.el8_9.x86_64	RHSA-2023:7841	CVE-2023-44446	Important/Sec.
openssl-1:1.1.1k-12.el8_9.x86_64 openssl-libs-1:1.1.1k-12.el8_9.x86_64 openssl-perl-1:1.1.1k-12.el8_9.x86_64	RHSA-2023:7877	CVE-2023-3446 CVE-2023-3817 CVE-2023-5678	Low/Sec.
nss-3.90.0-4.el8_9.x86_64 nss-softokn-3.90.0-4.el8_9.x86_64 nss-softokn-freebl-3.90.0-4.el8_9.x86_64 nss-sysinit-3.90.0-4.el8_9.x86_64 nss-util-3.90.0-4.el8_9.x86_64	RHSA-2024:0105	CVE-2023-5388	Moderate/Sec.
kernel-4.18.0-513.11.1.el8_9.x86_64 kernel-core-4.18.0-513.11.1.el8_9.x86_64 kernel-modules-4.18.0-513.11.1.el8_9.x86_64 kernel-tools-4.18.0-513.11.1.el8_9.x86_64 kernel-tools-libs-4.18.0-513.11.1.el8_9.x86_64 python3-perf-4.18.0-513.11.1.el8_9.x86_64	RHSA-2024:0113	CVE-2023-20569 CVE-2023-2162 CVE-2023-42753 CVE-2023-4622 CVE-2023-5633	Important/Sec.
platform-python-3.6.8-56.el8_9.2.x86_64 platform-python-devel-3.6.8-56.el8_9.2.x86_64 python3-libs-3.6.8-56.el8_9.2.x86_64	RHSA-2024:0114	CVE-2022-48560 CVE-2022-48564	Moderate/Sec.
libxml2-2.9.7-18.el8_9.x86_64 python3-libxml2-2.9.7-18.el8_9.x86_64	RHSA-2024:0119	CVE-2023-39615	Moderate/Sec.
pixman-0.38.4-3.el8_9.x86_64	RHSA-2024:0131	CVE-2022-44638	Moderate/Sec.
qemu-guest-agent-15:6.2.0-40.module+el8.9.0+20867+9a6a0901.2.x86_64	RHSA-2024:0135	CVE-2023-3019	Moderate/Sec.
gnutls-3.6.16-8.el8_9.x86_64	RHSA-2024:01	CVE-2023-5981	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

	55		
sqlite-3.26.0-19.el8_9.x86_64 sqlite-libs-3.26.0-19.el8_9.x86_64	RHSA-2024:0253	CVE-2023-7104	Moderate/Sec.
platform-python-3.6.8-56.el8_9.3.x86_64 platform-python-devel-3.6.8-56.el8_9.3.x86_64 python3-libs-3.6.8-56.el8_9.3.x86_64	RHSA-2024:0256	CVE-2023-27043	Moderate/Sec.
java-1.8.0-openjdk-1:1.8.0.402.b06-2.el8.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.402.b06-2.el8.x86_64	RHSA-2024:0265	CVE-2024-20918 CVE-2024-20919 CVE-2024-20921 CVE-2024-20926 CVE-2024-20945 CVE-2024-20952	Important/Sec.
openssh-8.0p1-19.el8_9.2.x86_64 openssh-clients-8.0p1-19.el8_9.2.x86_64 openssh-server-8.0p1-19.el8_9.2.x86_64	RHSA-2024:0606	CVE-2023-48795 CVE-2023-51385	Moderate/Sec.
gnutls-3.6.16-8.el8_9.1.x86_64	RHSA-2024:0627	CVE-2024-0553	Moderate/Sec.
libssh-0.9.6-13.el8_9.x86_64 libssh-config-0.9.6-13.el8_9.noarch	RHSA-2024:0628	CVE-2023-48795	Moderate/Sec.
python3-rpm-4.14.3-28.el8_9.x86_64 rpm-4.14.3-28.el8_9.x86_64 rpm-build-libs-4.14.3-28.el8_9.x86_64 rpm-libs-4.14.3-28.el8_9.x86_64 rpm-plugin-selinux-4.14.3-28.el8_9.x86_64 rpm-plugin-systemd-inhibit-4.14.3-28.el8_9.x86_64	RHSA-2024:0647	CVE-2021-35937 CVE-2021-35938 CVE-2021-35939	Moderate/Sec.

ADS-4.0 OVA Security Service Pack #6 includes the following rpm updates:

qemu-guest-agent-15:6.2.0-32.module+el8.8.0+18361+9f407f6e.x86_64	kernel-core-4.18.0-477.15.1.el8_8.x86_64
python3-unbound-1.16.2-5.el8.x86_64	kernel-modules-4.18.0-477.15.1.el8_8.x86_64
unbound-libs-1.16.2-5.el8.x86_64	kernel-tools-4.18.0-477.15.1.el8_8.x86_64
libwayland-client-1.21.0-1.el8.x86_64	kernel-tools-libs-4.18.0-477.15.1.el8_8.x86_64
libwayland-cursor-1.21.0-1.el8.x86_64	python3-perf-4.18.0-477.15.1.el8_8.x86_64
libwayland-egl-1.21.0-1.el8.x86_64	open-vm-tools-12.1.5-2.el8_8.x86_64
libwayland-server-1.21.0-1.el8.x86_64	bind-export-libs-32:9.11.36-8.el8_8.1.x86_64
libtiff-4.0.9-27.el8.x86_64	java-1.8.0-openjdk-1:1.8.0.382.b05-2.el8.x86_64
kpartx-0.8.4-37.el8.x86_64	java-1.8.0-openjdk-headless-1:1.8.0.382.b05-2.el8.x86_64
kernel-4.18.0-477.10.1.el8_8.x86_64	openssh-8.0p1-19.el8_8.x86_64
kernel-core-4.18.0-477.10.1.el8_8.x86_64	openssh-clients-8.0p1-19.el8_8.x86_64
kernel-modules-4.18.0-477.10.1.el8_8.x86_64	openssh-server-8.0p1-19.el8_8.x86_64
kernel-tools-4.18.0-477.10.1.el8_8.x86_64	dbus-1:1.12.8-24.el8_8.1.x86_64
kernel-tools-libs-4.18.0-477.10.1.el8_8.x86_64	dbus-common-1:1.12.8-24.el8_8.1.noarch
python3-perf-4.18.0-477.10.1.el8_8.x86_64	dbus-daemon-1:1.12.8-24.el8_8.1.x86_64
curl-7.61.1-30.el8.x86_64	dbus-libs-1:1.12.8-24.el8_8.1.x86_64
libcurl-7.61.1-30.el8.x86_64	dbus-tools-1:1.12.8-24.el8_8.1.x86_64
net-snmp-1:5.8-27.el8.x86_64	kernel-4.18.0-477.21.1.el8_8.x86_64
net-snmp-agent-libs-1:5.8-27.el8.x86_64	kernel-core-4.18.0-477.21.1.el8_8.x86_64
	kernel-modules-4.18.0-477.21.1.el8_8.x86_64

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

net-snmp-libs-1:5.8-27.el8.x86_64 dhcp-client-12:4.3.6-49.el8.x86_64 dhcp-common-12:4.3.6-49.el8.noarch dhcp-libs-12:4.3.6-49.el8.x86_64 bind-export-libs-32:9.11.36-8.el8.x86_64 libarchive-3.3.3-5.el8.x86_64 curl-7.61.1-30.el8_8.2.x86_64 libcurl-7.61.1-30.el8_8.2.x86_64 kernel-4.18.0-477.13.1.el8_8.x86_64 kernel-core-4.18.0-477.13.1.el8_8.x86_64 kernel-modules-4.18.0-477.13.1.el8_8.x86_64 kernel-tools-4.18.0-477.13.1.el8_8.x86_64 kernel-tools-libs-4.18.0-477.13.1.el8_8.x86_64 python3-perf-4.18.0-477.13.1.el8_8.x86_64 platform-python-3.6.8-51.el8_8.1.x86_64 platform-python-devel-3.6.8-51.el8_8.1.x86_64 python3-libs-3.6.8-51.el8_8.1.x86_64 qemu-guest-agent-15:6.2.0-32.module+el8.8.0+18361+9f407f6e.x86_64 libtiff-4.0.9-28.el8_8.x86_64 systemd-239-74.el8_8.2.x86_64 systemd-libs-239-74.el8_8.2.x86_64 systemd-pam-239-74.el8_8.2.x86_64 systemd-udev-239-74.el8_8.2.x86_64 libssh-0.9.6-10.el8_8.x86_64 libssh-config-0.9.6-10.el8_8.noarch sqlite-3.26.0-18.el8_8.x86_64 sqlite-libs-3.26.0-18.el8_8.x86_64 kernel-4.18.0-477.15.1.el8_8.x86_64	kernel-tools-4.18.0-477.21.1.el8_8.x86_64 kernel-tools-libs-4.18.0-477.21.1.el8_8.x86_64 python3-perf-4.18.0-477.21.1.el8_8.x86_64 curl-7.61.1-30.el8_8.3.x86_64 libcurl-7.61.1-30.el8_8.3.x86_64 libcap-2.48-5.el8_8.x86_64 libxml2-2.9.7-16.el8_8.1.x86_64 python3-libxml2-2.9.7-16.el8_8.1.x86_64 python3-syspurpose-1.28.36-3.el8_8.x86_64 cups-libs-1:2.2.6-51.el8_8.1.x86_64 flac-libs-1.3.2-9.el8_8.1.x86_64 kernel-4.18.0-477.27.1.el8_8.x86_64 kernel-core-4.18.0-477.27.1.el8_8.x86_64 kernel-modules-4.18.0-477.27.1.el8_8.x86_64 kernel-tools-4.18.0-477.27.1.el8_8.x86_64 kernel-tools-libs-4.18.0-477.27.1.el8_8.x86_64 python3-perf-4.18.0-477.27.1.el8_8.x86_64 linux-firmware-20230404-117.git2e92a49f.el8_8.noarch ncurses-6.1-9.20180224.el8_8.1.x86_64 ncurses-base-6.1-9.20180224.el8_8.1.noarch ncurses-libs-6.1-9.20180224.el8_8.1.x86_64 dmidecode-1:3.3-4.el8_8.1.x86_64 qemu-guest-agent-15:6.2.0-33.module+el8.8.0+19768+98f68f21.x86_64 libwebp-1.0.0-8.el8_8.1.x86_64 open-vm-tools-12.1.5-2.el8_8.3.x86_64 libtiff-4.0.9-29.el8_8.x86_64

Security vulnerabilities resolved in ADS 4.0 OVA Security Service Pack #6:

Updated Package	RHSA Number	CVE	RHSA Severity
qemu-guest-agent-15:6.2.0-32.module+el8.8.0+18361+9f407f6e.x86_64	RHSA-2023:2757	CVE-2021-46790 CVE-2022-30784 CVE-2022-30786 CVE-2022-30788 CVE-2022-30789 CVE-2022-3165 CVE-2023-1018	Moderate/Sec.
python3-unbound-1.16.2-5.el8.x86_64 unbound-libs-1.16.2-5.el8.x86_64	RHSA-2023:2771	CVE-2022-3204	Moderate/Sec.
libwayland-client-1.21.0-1.el8.x86_64 libwayland-cursor-1.21.0-1.el8.x86_64 libwayland-egl-1.21.0-1.el8.x86_64 libwayland-server-1.21.0-1.el8.x86_64	RHSA-2023:2786	CVE-2021-3782	Moderate/Sec.
libtiff-4.0.9-27.el8.x86_64	RHSA-2023:2883	CVE-2022-3627	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

		CVE-2022-3970	
kpartx-0.8.4-37.el8.x86_64	RHSA-2023:2948	CVE-2022-41973	Moderate/Sec.
kernel-4.18.0-477.10.1.el8_8.x86_64 kernel-core-4.18.0-477.10.1.el8_8.x86_64 kernel-modules-4.18.0-477.10.1.el8_8.x86_64 kernel-tools-4.18.0-477.10.1.el8_8.x86_64 kernel-tools-libs-4.18.0-477.10.1.el8_8.x86_64 python3-perf-4.18.0-477.10.1.el8_8.x86_64	RHSA-2023:2951	CVE-2021-26341 CVE-2021-33655 CVE-2021-33656 CVE-2022-1462 CVE-2022-1679 CVE-2022-1789 CVE-2022-20141 CVE-2022-2196 CVE-2022-25265 CVE-2022-2663 CVE-2022-3028 CVE-2022-30594 CVE-2022-3239 CVE-2022-3522 CVE-2022-3524 CVE-2022-3564 CVE-2022-3566 CVE-2022-3567 CVE-2022-3619 CVE-2022-3623 CVE-2022-3625 CVE-2022-3628 CVE-2022-3707 CVE-2022-39188 CVE-2022-39189 CVE-2022-41218 CVE-2022-4129 CVE-2022-41674 CVE-2022-42703 CVE-2022-42720 CVE-2022-42721 CVE-2022-42722 CVE-2022-43750 CVE-2022-47929 CVE-2023-0394 CVE-2023-0461 CVE-2023-1195 CVE-2023-1582 CVE-2023-23454	Important/Sec.
curl-7.61.1-30.el8.x86_64 libcurl-7.61.1-30.el8.x86_64	RHSA-2023:2963	CVE-2022-35252 CVE-2022-43552	Low/Sec.
net-snmp-1:5.8-27.el8.x86_64 net-snmp-agent-libs-1:5.8-27.el8.x86_64 net-snmp-libs-1:5.8-27.el8.x86_64	RHSA-2023:2969	CVE-2022-44792 CVE-2022-44793	Moderate/Sec.
dhcp-client-12:4.3.6-49.el8.x86_64 dhcp-common-12:4.3.6-49.el8.noarch dhcp-libs-12:4.3.6-49.el8.x86_64	RHSA-2023:3000	CVE-2022-2928 CVE-2022-2929	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

bind-export-libs-32:9.11.36-8.el8.x86_64	RHSA-2023:3002	CVE-2022-2795	Moderate/Sec.
libarchive-3.3.3-5.el8.x86_64	RHSA-2023:3018	CVE-2022-36227	Low/Sec.
curl-7.61.1-30.el8_8.2.x86_64 libcurl-7.61.1-30.el8_8.2.x86_64	RHSA-2023:3106	CVE-2023-27535	Moderate/Sec.
kernel-4.18.0-477.13.1.el8_8.x86_64 kernel-core-4.18.0-477.13.1.el8_8.x86_64 kernel-modules-4.18.0-477.13.1.el8_8.x86_64 kernel-tools-4.18.0-477.13.1.el8_8.x86_64 kernel-tools-libs-4.18.0-477.13.1.el8_8.x86_64 python3-perf-4.18.0-477.13.1.el8_8.x86_64	RHSA-2023:3349	CVE-2023-32233	Important/Sec.
platform-python-3.6.8-51.el8_8.1.x86_64 platform-python-devel-3.6.8-51.el8_8.1.x86_64 python3-libs-3.6.8-51.el8_8.1.x86_64	RHSA-2023:3591	CVE-2023-24329	Important/Sec.
qemu-guest-agent-15:6.2.0-32.module+el8.8.0+18361+9f407f6e.x86_64	RHSA-2023:3822	CVE-2023-2700	Moderate/Sec.
libtiff-4.0.9-28.el8_8.x86_64 systemd-239-74.el8_8.2.x86_64 systemd-libs-239-74.el8_8.2.x86_64 systemd-pam-239-74.el8_8.2.x86_64 systemd-udev-239-74.el8_8.2.x86_64	RHSA-2023:3827	CVE-2022-48281	Moderate/Sec.
libssh-0.9.6-10.el8_8.x86_64 libssh-config-0.9.6-10.el8_8.noarch	RHSA-2023:3839	CVE-2023-1667 CVE-2023-2283	Moderate/Sec.
sqlite-3.26.0-18.el8_8.x86_64 sqlite-libs-3.26.0-18.el8_8.x86_64	RHSA-2023:3840	CVE-2020-24736	Moderate/Sec.
kernel-4.18.0-477.15.1.el8_8.x86_64 kernel-core-4.18.0-477.15.1.el8_8.x86_64 kernel-modules-4.18.0-477.15.1.el8_8.x86_64 kernel-tools-4.18.0-477.15.1.el8_8.x86_64 kernel-tools-libs-4.18.0-477.15.1.el8_8.x86_64 python3-perf-4.18.0-477.15.1.el8_8.x86_64	RHSA-2023:3847	CVE-2023-28466	Moderate/Sec.
open-vm-tools-12.1.5-2.el8_8.x86_64	RHSA-2023:3949	CVE-2023-20867	Low/Sec.
bind-export-libs-32:9.11.36-8.el8_8.1.x86_64	RHSA-2023:4102	CVE-2023-2828	Important/Sec.
java-1.8.0-openjdk-1:1.8.0.382.b05-2.el8.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.382.b05-2.el8.x86_64	RHSA-2023:4176	CVE-2023-22045 CVE-2023-22049	Moderate/Sec.
openssh-8.0p1-19.el8_8.x86_64 openssh-clients-8.0p1-19.el8_8.x86_64 openssh-server-8.0p1-19.el8_8.x86_64	RHSA-2023:4419	CVE-2023-38408	Important/Sec.
dbus-1:1.12.8-24.el8_8.1.x86_64 dbus-common-1:1.12.8-24.el8_8.1.noarch	RHSA-2023:4498	CVE-2023-34969	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

dbus-daemon-1:1.12.8-24.el8_8.1.x86_64 dbus-libs-1:1.12.8-24.el8_8.1.x86_64 dbus-tools-1:1.12.8-24.el8_8.1.x86_64			
kernel-4.18.0-477.21.1.el8_8.x86_64 kernel-core-4.18.0-477.21.1.el8_8.x86_64 kernel-modules-4.18.0-477.21.1.el8_8.x86_64 kernel-tools-4.18.0-477.21.1.el8_8.x86_64 kernel-tools-libs-4.18.0-477.21.1.el8_8.x86_64 python3-perf-4.18.0-477.21.1.el8_8.x86_64	RHSA-2023:4517	CVE-2022-42896 CVE-2023-1281 CVE-2023-1829 CVE-2023-2124 CVE-2023-2194 CVE-2023-2235	Important/Sec.
curl-7.61.1-30.el8_8.3.x86_64 libcurl-7.61.1-30.el8_8.3.x86_64	RHSA-2023:4523	CVE-2023-27536 CVE-2023-28321	Moderate/Sec.
libcap-2.48-5.el8_8.x86_64	RHSA-2023:4524	CVE-2023-2602 CVE-2023-2603	Moderate/Sec.
libxml2-2.9.7-16.el8_8.1.x86_64 python3-libxml2-2.9.7-16.el8_8.1.x86_64	RHSA-2023:4529	CVE-2023-28484 CVE-2023-29469	Moderate/Sec.
python3-syspurpose-1.28.36-3.el8_8.x86_64	RHSA-2023:4706	CVE-2023-3899	Important/Sec.
cups-libs-1:2.2.6-51.el8_8.1.x86_64	RHSA-2023:4864	CVE-2023-32360	Important/Sec.
flac-libs-1.3.2-9.el8_8.1.x86_64	RHSA-2023:5046	CVE-2020-22219	Important/Sec.
kernel-4.18.0-477.27.1.el8_8.x86_64 kernel-core-4.18.0-477.27.1.el8_8.x86_64 kernel-modules-4.18.0-477.27.1.el8_8.x86_64 kernel-tools-4.18.0-477.27.1.el8_8.x86_64 kernel-tools-libs-4.18.0-477.27.1.el8_8.x86_64 python3-perf-4.18.0-477.27.1.el8_8.x86_64	RHSA-2023:5244	CVE-2023-2002 CVE-2023-20593 CVE-2023-3090 CVE-2023-3390 CVE-2023-35001 CVE-2023-35788 CVE-2023-3776 CVE-2023-4004	Important/Sec.
linux-firmware-20230404-117.git2e92a49f.el8_8.noarch	RHSA-2023:5245	CVE-2023-20593	Moderate/Sec.
ncurses-6.1-9.20180224.el8_8.1.x86_64 ncurses-base-6.1-9.20180224.el8_8.1.noarch ncurses-libs-6.1-9.20180224.el8_8.1.x86_64	RHSA-2023:5249	CVE-2023-29491	Moderate/Sec.
dmidecode-1:3.3-4.el8_8.1.x86_64	RHSA-2023:5252	CVE-2023-30630	Moderate/Sec.
qemu-guest-agent-15:6.2.0-33.module+el8.8.0+19768+98f68f21.x86_64	RHSA-2023:5264	CVE-2022-40284 CVE-2023-3354	Important/Sec.
libwebp-1.0.0-8.el8_8.1.x86_64	RHSA-2023:5309	CVE-2023-4863	Important/Sec.
open-vm-tools-12.1.5-2.el8_8.3.x86_64	RHSA-2023:5312	CVE-2023-20900	Important/Sec.
libtiff-4.0.9-29.el8_8.x86_64	RHSA-2023:5353	CVE-2023-0800 CVE-2023-0801 CVE-2023-0802 CVE-2023-0803	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

		CVE-2023-0804	

ADS-4.0 OVA Security Service Pack #5 includes the following rpm updates:

grub2-common-1:2.02-142.el8_7.1.noarch	kernel-tools-4.18.0-425.13.1.el8_7.x86_64
grub2-efi-x64-1:2.02-142.el8_7.1.x86_64	kernel-tools-libs-4.18.0-425.13.1.el8_7.x86_64
grub2-tools-1:2.02-142.el8_7.1.x86_64	python3-perf-4.18.0-425.13.1.el8_7.x86_64
grub2-tools-extra-1:2.02-142.el8_7.1.x86_64	platform-python-3.6.8-48.el8_7.1.x86_64
grub2-tools-minimal-1:2.02-142.el8_7.1.x86_64	platform-python-devel-3.6.8-48.el8_7.1.x86_64
libtiff-4.0.9-26.el8_7.x86_64	python3-libs-3.6.8-48.el8_7.1.x86_64
dbus-1:1.12.8-23.el8_7.1.x86_64	platform-python-setuptools-39.2.0-6.el8_7.1.noarch
dbus-common-1:1.12.8-23.el8_7.1.noarch	python3-setuptools-39.2.0-6.el8_7.1.noarch
dbus-daemon-1:1.12.8-23.el8_7.1.x86_64	python3-setuptools-wheel-39.2.0-6.el8_7.1.noarch
dbus-libs-1:1.12.8-23.el8_7.1.x86_64	systemd-239-68.el8_7.4.x86_64
dbus-tools-1:1.12.8-23.el8_7.1.x86_64	systemd-libs-239-68.el8_7.4.x86_64
qemu-guest-agent-15:6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64	systemd-pam-239-68.el8_7.4.x86_64
systemd-239-68.el8_7.1.x86_64	systemd-udev-239-68.el8_7.4.x86_64
systemd-libs-239-68.el8_7.1.x86_64	tar-2:1.30-6.el8_7.1.x86_64
systemd-pam-239-68.el8_7.1.x86_64	curl-7.61.1-25.el8_7.3.x86_64
systemd-udev-239-68.el8_7.1.x86_64	libcurl-7.61.1-25.el8_7.3.x86_64
kernel-4.18.0-425.10.1.el8_7.x86_64	nss-3.79.0-11.el8_7.x86_64
kernel-core-4.18.0-425.10.1.el8_7.x86_64	nss-softokn-3.79.0-11.el8_7.x86_64
kernel-modules-4.18.0-425.10.1.el8_7.x86_64	nss-softokn-freebl-3.79.0-11.el8_7.x86_64
kernel-tools-4.18.0-425.10.1.el8_7.x86_64	nss-sysinit-3.79.0-11.el8_7.x86_64
kernel-tools-libs-4.18.0-425.10.1.el8_7.x86_64	nss-util-3.79.0-11.el8_7.x86_64
python3-perf-4.18.0-425.10.1.el8_7.x86_64	openssl-1:1.1.1k-9.el8_7.x86_64
expat-2.2.5-10.el8_7.1.x86_64	openssl-libs-1:1.1.1k-9.el8_7.x86_64
sqlite-3.26.0-17.el8_7.x86_64	openssl-perl-1:1.1.1k-9.el8_7.x86_64
sqlite-libs-3.26.0-17.el8_7.x86_64	kernel-4.18.0-425.19.2.el8_7.x86_64
libtasn1-4.13-4.el8_7.x86_64	kernel-core-4.18.0-425.19.2.el8_7.x86_64
libxml2-2.9.7-15.el8_7.1.x86_64	kernel-modules-4.18.0-425.19.2.el8_7.x86_64
python3-libxml2-2.9.7-15.el8_7.1.x86_64	kernel-tools-4.18.0-425.19.2.el8_7.x86_64
java-1.8.0-openjdk-1:1.8.0.362.b09-2.el8_7.x86_64	kernel-tools-libs-4.18.0-425.19.2.el8_7.x86_64
java-1.8.0-openjdk-headless-1:1.8.0.362.b09-2.el8_7.x86_64	python3-perf-4.18.0-425.19.2.el8_7.x86_64
sudo-1.8.29-8.el8_7.1.x86_64	gnutls-3.6.16-6.el8_7.x86_64
libksba-1.3.5-9.el8_7.x86_64	java-1.8.0-openjdk-1:1.8.0.372.b07-1.el8_7.x86_64
kernel-4.18.0-425.13.1.el8_7.x86_64	java-1.8.0-openjdk-headless-1:1.8.0.372.b07-1.el8_7.x86_64
kernel-core-4.18.0-425.13.1.el8_7.x86_64	libwebp-1.0.0-8.el8_7.x86_64
kernel-modules-4.18.0-425.13.1.el8_7.x86_64	

Security vulnerabilities resolved in ADS 4.0 OVA Security Service Pack #5:

Updated Package	RHSA Number	CVE	RHSA Severity
grub2-common-1:2.02-142.el8_7.1.noarch grub2-efi-x64-1:2.02-142.el8_7.1.x86_64 grub2-tools-1:2.02-142.el8_7.1.x86_64	RHSA-2023:0049	CVE-2022-2601 CVE-2022-3775	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

grub2-tools-extra-1:2.02-142.el8_7.1.x86_64 grub2-tools-minimal-1:2.02-142.el8_7.1.x86_64			
libtiff-4.0.9-26.el8_7.x86_64	RHSA-2023:0095	CVE-2022-2519 CVE-2022-2520 CVE-2022-2521 CVE-2022-2867 CVE-2022-2868 CVE-2022-2869 CVE-2022-2953	Moderate/Sec.
dbus-1:1.12.8-23.el8_7.1.x86_64 dbus-common-1:1.12.8-23.el8_7.1.noarch dbus-daemon-1:1.12.8-23.el8_7.1.x86_64 dbus-libs-1:1.12.8-23.el8_7.1.x86_64 dbus-tools-1:1.12.8-23.el8_7.1.x86_64	RHSA-2023:0096	CVE-2022-42010 CVE-2022-42011 CVE-2022-42012	Moderate/Sec.
qemu-guest-agent-15:6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64	RHSA-2023:0099	CVE-2022-4144	Moderate/Sec.
systemd-239-68.el8_7.1.x86_64 systemd-libs-239-68.el8_7.1.x86_64 systemd-pam-239-68.el8_7.1.x86_64 systemd-udev-239-68.el8_7.1.x86_64	RHSA-2023:0100	CVE-2022-3821	Moderate/Sec.
kernel-4.18.0-425.10.1.el8_7.x86_64 kernel-core-4.18.0-425.10.1.el8_7.x86_64 kernel-modules-4.18.0-425.10.1.el8_7.x86_64 kernel-tools-4.18.0-425.10.1.el8_7.x86_64 kernel-tools-libs-4.18.0-425.10.1.el8_7.x86_64 python3-perf-4.18.0-425.10.1.el8_7.x86_64	RHSA-2023:0101	CVE-2022-2964 CVE-2022-4139	Important/Sec.
expat-2.2.5-10.el8_7.1.x86_64	RHSA-2023:0103	CVE-2022-43680	Moderate/Sec.
sqlite-3.26.0-17.el8_7.x86_64 sqlite-libs-3.26.0-17.el8_7.x86_64	RHSA-2023:0110	CVE-2022-35737	Moderate/Sec.
libtasn1-4.13-4.el8_7.x86_64	RHSA-2023:0116	CVE-2021-46848	Moderate/Sec.
libxml2-2.9.7-15.el8_7.1.x86_64 python3-libxml2-2.9.7-15.el8_7.1.x86_64	RHSA-2023:0173	CVE-2022-40303 CVE-2022-40304	Moderate/Sec.
java-1.8.0-openjdk-1:1.8.0.362.b09-2.el8_7.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.362.b09-2.el8_7.x86_64	RHSA-2023:0208	CVE-2023-21830 CVE-2023-21843	Moderate/Sec.
sudo-1.8.29-8.el8_7.1.x86_64	RHSA-2023:0284	CVE-2023-22809	Important/Sec.
libksba-1.3.5-9.el8_7.x86_64	RHSA-2023:0625	CVE-2022-47629	Important/Sec.
kernel-4.18.0-425.13.1.el8_7.x86_64 kernel-core-4.18.0-425.13.1.el8_7.x86_64 kernel-modules-4.18.0-425.13.1.el8_7.x86_64 kernel-tools-4.18.0-425.13.1.el8_7.x86_64 kernel-tools-libs-4.18.0-425.13.1.el8_7.x86_64 python3-perf-4.18.0-425.13.1.el8_7.x86_64	RHSA-2023:0832	CVE-2022-2873 CVE-2022-41222 CVE-2022-43945	Important/Sec.
platform-python-3.6.8-48.el8_7.1.x86_64	RHSA-2023:0833	CVE-2020-10735	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

platform-python-devel-3.6.8-48.el8_7.1.x86_64 python3-libs-3.6.8-48.el8_7.1.x86_64		CVE-2021-28861 CVE-2022-45061	
platform-python-setuptools-39.2.0-6.el8_7.1.noarch python3-setuptools-39.2.0-6.el8_7.1.noarch python3-setuptools-wheel-39.2.0-6.el8_7.1.noarch	RHSA-2023:0835	CVE-2022-40897	Moderate/Sec.
systemd-239-68.el8_7.4.x86_64 systemd-libs-239-68.el8_7.4.x86_64 systemd-pam-239-68.el8_7.4.x86_64 systemd-udev-239-68.el8_7.4.x86_64	RHSA-2023:0837	CVE-2022-4415	Moderate/Sec.
tar-2:1.30-6.el8_7.1.x86_64	RHSA-2023:0842	CVE-2022-48303	Moderate/Sec.
curl-7.61.1-25.el8_7.3.x86_64 libcurl-7.61.1-25.el8_7.3.x86_64	RHSA-2023:1140	CVE-2023-23916	Moderate/Sec.
nss-3.79.0-11.el8_7.x86_64 nss-softokn-3.79.0-11.el8_7.x86_64 nss-softokn-freebl-3.79.0-11.el8_7.x86_64 nss-sysinit-3.79.0-11.el8_7.x86_64 nss-util-3.79.0-11.el8_7.x86_64	RHSA-2023:1252	CVE-2023-0767	Important/Sec.
openssl-1:1.1.1k-9.el8_7.x86_64 openssl-libs-1:1.1.1k-9.el8_7.x86_64 openssl-perl-1:1.1.1k-9.el8_7.x86_64	RHSA-2023:1405	CVE-2022-4304 CVE-2022-4450 CVE-2023-0215 CVE-2023-0286	Important/Sec.
kernel-4.18.0-425.19.2.el8_7.x86_64 kernel-core-4.18.0-425.19.2.el8_7.x86_64 kernel-modules-4.18.0-425.19.2.el8_7.x86_64 kernel-tools-4.18.0-425.19.2.el8_7.x86_64 kernel-tools-libs-4.18.0-425.19.2.el8_7.x86_64 python3-perf-4.18.0-425.19.2.el8_7.x86_64	RHSA-2023:1566	CVE-2022-4269 CVE-2022-4378 CVE-2023-0266 CVE-2023-0386	Important/Sec.
gnutls-3.6.16-6.el8_7.x86_64	RHSA-2023:1569	CVE-2023-0361	Moderate/Sec.
java-1.8.0-openjdk-1:1.8.0.372.b07-1.el8_7.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.372.b07-1.el8_7.x86_64	RHSA-2023:1908	CVE-2023-21930 CVE-2023-21937 CVE-2023-21938 CVE-2023-21939 CVE-2023-21954 CVE-2023-21967 CVE-2023-21968	Important/Sec.
libwebp-1.0.0-8.el8_7.x86_64	RHSA-2023:2076	CVE-2023-1999	Important/Sec.

ADS-4.0 OVA Security Service Pack #4 includes the following rpm updates:

bind-export-libs-32:9.11.36-3.el8_6.1.x86_64	openblas-0.3.15-4.el8.x86_64
expat-2.2.5-8.el8_6.3.x86_64	openblas-threads-0.3.15-4.el8.x86_64
java-1.8.0-openjdk-1:1.8.0.352.b08-2.el8_6.x86_64	kernel-4.18.0-425.3.1.el8.x86_64
java-1.8.0-openjdk-headless-1:1.8.0.352.b08-2.el8_6.x86_64	kernel-core-4.18.0-425.3.1.el8.x86_64
libksba-1.3.5-8.el8_6.x86_64	kernel-modules-4.18.0-425.3.1.el8.x86_64
gnutls-3.6.16-5.el8_6.x86_64	kernel-tools-4.18.0-425.3.1.el8.x86_64
	kernel-tools-libs-4.18.0-425.3.1.el8.x86_64

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

zlib-1.2.11-19.el8_6.x86_64 sqlite-3.26.0-16.el8_6.x86_64 sqlite-libs-3.26.0-16.el8_6.x86_64 kernel-4.18.0-372.32.1.el8_6.x86_64 kernel-core-4.18.0-372.32.1.el8_6.x86_64 kernel-modules-4.18.0-372.32.1.el8_6.x86_64 kernel-tools-4.18.0-372.32.1.el8_6.x86_64 kernel-tools-libs-4.18.0-372.32.1.el8_6.x86_64 python3-perf-4.18.0-372.32.1.el8_6.x86_64 kpartx-0.8.4-22.el8_6.2.x86_64 qemu-guest-agent-15:6.2.0-20.module+el8.7.0+16689+53d59bc2.1.x86_64 fribidi-1.0.4-9.el8.x86_64 libtiff-4.0.9-23.el8.x86_64 python3-unbound-1.16.2-2.el8.x86_64 unbound-libs-1.16.2-2.el8.x86_64	python3-perf-4.18.0-425.3.1.el8.x86_64 gdisk-1.0.3-11.el8.x86_64 glib2-2.56.4-159.el8.x86_64 libxml2-2.9.7-15.el8.x86_64 python3-libxml2-2.9.7-15.el8.x86_64 e2fsprogs-1.45.6-5.el8.x86_64 e2fsprogs-libs-1.45.6-5.el8.x86_64 libcom_err-1.45.6-5.el8.x86_64 libss-1.45.6-5.el8.x86_64 freetype-2.9.1-9.el8.x86_64 bind-export-libs-32:9.11.36-5.el8.x86_64 kpartx-0.8.4-28.el8_7.1.x86_64 krb5-libs-1.18.2-22.el8_7.x86_64

Security vulnerabilities resolved in ADS 4.0 OVA Security Service Pack #4:

Updated Package	RHSA Number	CVE	RHSA Severity
bind-export-libs-32:9.11.36-3.el8_6.1.x86_64	RHSA-2022:6778	CVE-2022-38177 CVE-2022-38178	Important/Sec.
expat-2.2.5-8.el8_6.3.x86_64	RHSA-2022:6878	CVE-2022-40674	Important/Sec.
java-1.8.0-openjdk-1:1.8.0.352.b08-2.el8_6.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.352.b08-2.el8_6.x86_64	RHSA-2022:7006	CVE-2022-21619 CVE-2022-21624 CVE-2022-21626 CVE-2022-21628	Moderate/Sec.
libksba-1.3.5-8.el8_6.x86_64	RHSA-2022:7089	CVE-2022-3515	Important/Sec.
gnutls-3.6.16-5.el8_6.x86_64	RHSA-2022:7105	CVE-2022-2509	Moderate/Sec.
zlib-1.2.11-19.el8_6.x86_64	RHSA-2022:7106	CVE-2022-37434	Moderate/Sec.
sqlite-3.26.0-16.el8_6.x86_64 sqlite-libs-3.26.0-16.el8_6.x86_64	RHSA-2022:7108	CVE-2020-35525 CVE-2020-35527	Moderate/Sec.
kernel-4.18.0-372.32.1.el8_6.x86_64 kernel-core-4.18.0-372.32.1.el8_6.x86_64 kernel-modules-4.18.0-372.32.1.el8_6.x86_64 kernel-tools-4.18.0-372.32.1.el8_6.x86_64 kernel-tools-libs-4.18.0-372.32.1.el8_6.x86_64 python3-perf-4.18.0-372.32.1.el8_6.x86_64	RHSA-2022:7110	CVE-2022-0494 CVE-2022-1353 CVE-2022-23825 CVE-2022-2588 CVE-2022-29901	Important/Sec.
kpartx-0.8.4-22.el8_6.2.x86_64	RHSA-2022:7192	CVE-2022-41974	Important/Sec.
qemu-guest-agent-15:6.2.0-	RHSA-2022:7472	CVE-2021-3507	Low/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

20.module+el8.7.0+16689+53d59bc2.1.x86_64		CVE-2022-0897 CVE-2022-2211 CVE-2022-23645	
fribidi-1.0.4-9.el8.x86_64	RHSA-2022:7514	CVE-2022-25308 CVE-2022-25309 CVE-2022-25310	Moderate/Sec.
libtiff-4.0.9-23.el8.x86_64	RHSA-2022:7585	CVE-2022-0561 CVE-2022-0562 CVE-2022-0865 CVE-2022-0891 CVE-2022-0908 CVE-2022-0909 CVE-2022-0924 CVE-2022-1355 CVE-2022-22844	Moderate/Sec.
python3-unbound-1.16.2-2.el8.x86_64 unbound-libs-1.16.2-2.el8.x86_64	RHSA-2022:7622	CVE-2022-30698 CVE-2022-30699	Moderate/Sec.
openblas-0.3.15-4.el8.x86_64 openblas-threads-0.3.15-4.el8.x86_64	RHSA-2022:7639	CVE-2021-4048	Moderate/Sec.
kernel-4.18.0-425.3.1.el8.x86_64 kernel-core-4.18.0-425.3.1.el8.x86_64 kernel-modules-4.18.0-425.3.1.el8.x86_64 kernel-tools-4.18.0-425.3.1.el8.x86_64 kernel-tools-libs-4.18.0-425.3.1.el8.x86_64 python3-perf-4.18.0-425.3.1.el8.x86_64	RHSA-2022:7683	CVE-2020-36516 CVE-2020-36558 CVE-2021-30002 CVE-2021-3640 CVE-2022-0168 CVE-2022-0617 CVE-2022-0854 CVE-2022-1016 CVE-2022-1048 CVE-2022-1055 CVE-2022-1184 CVE-2022-1852 CVE-2022-20368 CVE-2022-2078 CVE-2022-21499 CVE-2022-23960 CVE-2022-24448 CVE-2022-2586 CVE-2022-26373 CVE-2022-2639 CVE-2022-27950 CVE-2022-28390 CVE-2022-28893 CVE-2022-2938 CVE-2022-29581 CVE-2022-36946	Moderate/Sec.
gdisk-1.0.3-11.el8.x86_64	RHSA-2022:7700	CVE-2020-0256 CVE-2021-0308	Moderate/Sec.
glib2-2.56.4-159.el8.x86_64	RHSA-2022:7704	CVE-2022-22624 CVE-2022-22628 CVE-2022-22629 CVE-2022-22662	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

		CVE-2022-26700 CVE-2022-26709 CVE-2022-26710 CVE-2022-26716 CVE-2022-26717 CVE-2022-26719 CVE-2022-30293	
libxml2-2.9.7-15.el8.x86_64 python3-libxml2-2.9.7-15.el8.x86_64	RHSA-2022:7715	CVE-2016-3709	Moderate/Sec.
e2fsprogs-1.45.6-5.el8.x86_64 e2fsprogs-libs-1.45.6-5.el8.x86_64 libcom_err-1.45.6-5.el8.x86_64 libss-1.45.6-5.el8.x86_64	RHSA-2022:7720	CVE-2022-1304	Moderate/Sec.
freetype-2.9.1-9.el8.x86_64	RHSA-2022:7745	CVE-2022-27404 CVE-2022-27405 CVE-2022-27406	Moderate/Sec.
bind-export-libs-32:9.11.36-5.el8.x86_64	RHSA-2022:7790	CVE-2021-25220	Moderate/Sec.
kpartx-0.8.4-28.el8_7.1.x86_64	RHSA-2022:7928	CVE-2022-3787	Important/Sec.
krb5-libs-1.18.2-22.el8_7.x86_64	RHSA-2022:8638	CVE-2022-42898	Important/Sec.

ADS-4.0 OVA Security Service Pack #3 includes the following rpm updates:

libgcrypt-1.8.5-7.el8_6.x86_64	openssl-libs-1:1.1.1k-7.el8_6.x86_64
curl-7.61.1-22.el8_6.3.x86_64	openssl-perl-1:1.1.1k-7.el8_6.x86_64
libcurl-7.61.1-22.el8_6.3.x86_64	kernel-4.18.0-372.19.1.el8_6.x86_64
expat-2.2.5-8.el8_6.2.x86_64	kernel-core-4.18.0-372.19.1.el8_6.x86_64
kernel-4.18.0-372.13.1.el8_6.x86_64	kernel-modules-4.18.0-372.19.1.el8_6.x86_64
kernel-core-4.18.0-372.13.1.el8_6.x86_64	kernel-tools-4.18.0-372.19.1.el8_6.x86_64
kernel-modules-4.18.0-372.13.1.el8_6.x86_64	kernel-tools-libs-4.18.0-372.19.1.el8_6.x86_64
kernel-tools-4.18.0-372.13.1.el8_6.x86_64	python3-perf-4.18.0-372.19.1.el8_6.x86_64
kernel-tools-libs-4.18.0-372.13.1.el8_6.x86_64	qemu-guest-agent-15:6.2.0-
python3-perf-4.18.0-372.13.1.el8_6.x86_64	11.module+el8.6.0+15668+464a1f31.2.x86_64
libxml2-2.9.7-13.el8_6.1.x86_64	curl-7.61.1-22.el8_6.4.x86_64
python3-libxml2-2.9.7-13.el8_6.1.x86_64	libcurl-7.61.1-22.el8_6.4.x86_64
vim-minimal-2:8.0.1763-19.el8_6.2.x86_64	systemd-239-58.el8_6.4.x86_64
compat-openssl10-1:1.0.2o-4.el8_6.x86_64	systemd-libs-239-58.el8_6.4.x86_64
libinput-1.16.3-3.el8_6.x86_64	systemd-pam-239-58.el8_6.4.x86_64
kernel-4.18.0-372.16.1.el8_6.x86_64	systemd-udev-239-58.el8_6.4.x86_64
kernel-core-4.18.0-372.16.1.el8_6.x86_64	open-vm-tools-11.3.5-1.el8_6.1.x86_64
kernel-modules-4.18.0-372.16.1.el8_6.x86_64	platform-python-3.6.8-47.el8_6.x86_64
kernel-tools-4.18.0-372.16.1.el8_6.x86_64	platform-python-devel-3.6.8-47.el8_6.x86_64
kernel-tools-libs-4.18.0-372.16.1.el8_6.x86_64	python3-libs-3.6.8-47.el8_6.x86_64
python3-perf-4.18.0-372.16.1.el8_6.x86_64	kernel-4.18.0-372.26.1.el8_6.x86_64
java-1.8.0-openjdk-1:1.8.0.342.b07-2.el8_6.x86_64	kernel-core-4.18.0-372.26.1.el8_6.x86_64
java-1.8.0-openjdk-headless-1:1.8.0.342.b07-	kernel-modules-4.18.0-372.26.1.el8_6.x86_64

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

2.el8_6.x86_64 pcre2-10.32-3.el8_6.x86_64 pcre2-utf16-10.32-3.el8_6.x86_64 vim-minimal-2:8.0.1763-19.el8_6.4.x86_64 openssl-1:1.1.1k-7.el8_6.x86_64	kernel-tools-4.18.0-372.26.1.el8_6.x86_64 kernel-tools-libs-4.18.0-372.26.1.el8_6.x86_64 python3-perf-4.18.0-372.26.1.el8_6.x86_64 gnupg2-2.2.20-3.el8_6.x86_64 gnupg2-smime-2.2.20-3.el8_6.x86_64

Security vulnerabilities resolved in ADS 4.0 OVA Security Service Pack #3:

Updated Package	RHSA Number	CVE	RHSA Severity
libgcrypt-1.8.5-7.el8_6.x86_64	RHSA-2022:5311	CVE-2021-40528	Moderate/Sec.
curl-7.61.1-22.el8_6.3.x86_64 libcurl-7.61.1-22.el8_6.3.x86_64	RHSA-2022:5313	CVE-2022-22576 CVE-2022-27774 CVE-2022-27776 CVE-2022-27782	Moderate/Sec.
expat-2.2.5-8.el8_6.2.x86_64	RHSA-2022:5314	CVE-2022-25313 CVE-2022-25314	Moderate/Sec.
kernel-4.18.0-372.13.1.el8_6.x86_64 kernel-core-4.18.0-372.13.1.el8_6.x86_64 kernel-modules-4.18.0-372.13.1.el8_6.x86_64 kernel-tools-4.18.0-372.13.1.el8_6.x86_64 kernel-tools-libs-4.18.0-372.13.1.el8_6.x86_64 python3-perf-4.18.0-372.13.1.el8_6.x86_64	RHSA-2022:5316	CVE-2020-28915 CVE-2022-27666	Important/Sec.
libxml2-2.9.7-13.el8_6.1.x86_64 python3-libxml2-2.9.7-13.el8_6.1.x86_64	RHSA-2022:5317	CVE-2022-29824	Moderate/Sec.
vim-minimal-2:8.0.1763-19.el8_6.2.x86_64	RHSA-2022:5319	CVE-2022-1621 CVE-2022-1629	Moderate/Sec.
compat-openssl10-1:1.0.2o-4.el8_6.x86_64	RHSA-2022:5326	CVE-2022-0778	Low/Sec.
libinput-1.16.3-3.el8_6.x86_64	RHSA-2022:5331	CVE-2022-1215	Moderate/Sec.
kernel-4.18.0-372.16.1.el8_6.x86_64 kernel-core-4.18.0-372.16.1.el8_6.x86_64 kernel-modules-4.18.0-372.16.1.el8_6.x86_64 kernel-tools-4.18.0-372.16.1.el8_6.x86_64 kernel-tools-libs-4.18.0-372.16.1.el8_6.x86_64 python3-perf-4.18.0-372.16.1.el8_6.x86_64	RHSA-2022:5564	CVE-2022-1729	Important/Sec.
java-1.8.0-openjdk-1:1.8.0.342.b07-2.el8_6.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.342.b07-2.el8_6.x86_64	RHSA-2022:5696	CVE-2022-21540 CVE-2022-21541 CVE-2022-34169	Important/Sec.
pcre2-10.32-3.el8_6.x86_64 pcre2-utf16-10.32-3.el8_6.x86_64	RHSA-2022:5809	CVE-2022-1586	Moderate/Sec.
vim-minimal-2:8.0.1763-19.el8_6.4.x86_64	RHSA-2022:5813	CVE-2022-1785 CVE-2022-1897 CVE-2022-1927	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

openssl-1:1.1.1k-7.el8_6.x86_64 openssl-libs-1:1.1.1k-7.el8_6.x86_64 openssl-perl-1:1.1.1k-7.el8_6.x86_64	RHSA-2022:5818	CVE-2022-1292 CVE-2022-2068 CVE-2022-2097	Moderate/Sec.
kernel-4.18.0-372.19.1.el8_6.x86_64 kernel-core-4.18.0-372.19.1.el8_6.x86_64 kernel-modules-4.18.0-372.19.1.el8_6.x86_64 kernel-tools-4.18.0-372.19.1.el8_6.x86_64 kernel-tools-libs-4.18.0-372.19.1.el8_6.x86_64 python3-perf-4.18.0-372.19.1.el8_6.x86_64	RHSA-2022:5819	CVE-2022-1012 CVE-2022-32250	Important/Sec.
qemu-guest-agent-15:6.2.0-11.module+el8.6.0+15668+464a1f31.2.x86_64	RHSA-2022:5821	CVE-2021-4206 CVE-2021-4207 CVE-2022-26353 CVE-2022-26354	Moderate/Sec.
curl-7.61.1-22.el8_6.4.x86_64 libcurl-7.61.1-22.el8_6.4.x86_64	RHSA-2022:6159	CVE-2022-32206 CVE-2022-32208	Moderate/Sec.
systemd-239-58.el8_6.4.x86_64 systemd-libs-239-58.el8_6.4.x86_64 systemd-pam-239-58.el8_6.4.x86_64 systemd-udev-239-58.el8_6.4.x86_64	RHSA-2022:6206	CVE-2022-2526	Important/Sec.
open-vm-tools-11.3.5-1.el8_6.1.x86_64	RHSA-2022:6357	CVE-2022-31676	Important/Sec.
platform-python-3.6.8-47.el8_6.x86_64 platform-python-devel-3.6.8-47.el8_6.x86_64 python3-libs-3.6.8-47.el8_6.x86_64	RHSA-2022:6457	CVE-2015-20107 CVE-2022-0391	Moderate/Sec.
kernel-4.18.0-372.26.1.el8_6.x86_64 kernel-core-4.18.0-372.26.1.el8_6.x86_64 kernel-modules-4.18.0-372.26.1.el8_6.x86_64 kernel-tools-4.18.0-372.26.1.el8_6.x86_64 kernel-tools-libs-4.18.0-372.26.1.el8_6.x86_64 python3-perf-4.18.0-372.26.1.el8_6.x86_64	RHSA-2022:6460	CVE-2022-21123 CVE-2022-21125 CVE-2022-21166	Moderate/Sec.
gnupg2-2.2.20-3.el8_6.x86_64 gnupg2-smime-2.2.20-3.el8_6.x86_64	RHSA-2022:6463	CVE-2022-34903	Moderate/Sec.

ADS-4.0 OVA Security Service Pack #2 includes the following rpm updates:

bind-export-libs-32:9.11.36-3.el8.x86_64	libssh-0.9.6-3.el8.x86_64
bluez-libs-5.56-3.el8.x86_64	libssh-config-0.9.6-3.el8.noarch
cairo-1.15.12-6.el8.x86_64	libtiff-4.0.9-21.el8.x86_64
cpio-2.12-11.el8.x86_64	libudisks2-2.9.0-9.el8.x86_64
cups-libs-1:2.2.6-45.el8_6.2.x86_64	libxml2-2.9.7-12.el8_5.x86_64
expat-2.2.5-4.el8_5.3.x86_64	mokutil-1:0.3.0-11.el8_6.1.x86_64
glibc-2.28-164.el8_5.3.x86_64	openssh-8.0p1-13.el8.x86_64
glibc-all-langpacks-2.28-164.el8_5.3.x86_64	openssh-clients-8.0p1-13.el8.x86_64
glibc-common-2.28-164.el8_5.3.x86_64	openssh-server-8.0p1-13.el8.x86_64
glibc-langpack-en-2.28-164.el8_5.3.x86_64	openssl-1:1.1.1k-6.el8_5.x86_64
grub2-common-1:2.02-123.el8.noarch	openssl-libs-1:1.1.1k-6.el8_5.x86_64
grub2-common-1:2.02-123.el8_6.8.noarch	openssl-perl-1:1.1.1k-6.el8_5.x86_64
grub2-efi-x64-1:2.02-123.el8.x86_64	pixman-0.38.4-2.el8.x86_64
grub2-efi-x64-1:2.02-123.el8_6.8.x86_64	platform-python-3.6.8-45.el8.x86_64
grub2-tools-1:2.02-123.el8.x86_64	platform-python-devel-3.6.8-45.el8.x86_64

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

grub2-tools-1:2.02-123.el8_6.8.x86_64 grub2-tools-extra-1:2.02-123.el8.x86_64 grub2-tools-extra-1:2.02-123.el8_6.8.x86_64 grub2-tools-minimal-1:2.02-123.el8.x86_64 grub2-tools-minimal-1:2.02-123.el8_6.8.x86_64 gzip-1.9-13.el8_5.x86_64 java-1.8.0-openjdk-1:1.8.0.332.b09-1.el8_5.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.332.b09-1.el8_5.x86_64 kernel-4.18.0-348.23.1.el8_5.x86_64 kernel-4.18.0-372.9.1.el8.x86_64 kernel-core-4.18.0-348.23.1.el8_5.x86_64 kernel-core-4.18.0-372.9.1.el8.x86_64 kernel-modules-4.18.0-348.23.1.el8_5.x86_64 kernel-modules-4.18.0-372.9.1.el8.x86_64 kernel-tools-4.18.0-348.23.1.el8_5.x86_64 kernel-tools-4.18.0-372.9.1.el8.x86_64 kernel-tools-libs-4.18.0-348.23.1.el8_5.x86_64 kernel-tools-libs-4.18.0-372.9.1.el8.x86_64 libarchive-3.3.3-3.el8_5.x86_64 libnsl-2.28-164.el8_5.3.x86_64 libsndfile-1.0.28-12.el8.x86_64	polkit-0.115-13.el8_5.2.x86_64 polkit-libs-0.115-13.el8_5.2.x86_64 python3-libs-3.6.8-45.el8.x86_64 python3-libxml2-2.9.7-12.el8_5.x86_64 python3-perf-4.18.0-348.23.1.el8_5.x86_64 python3-perf-4.18.0-372.9.1.el8.x86_64 qemu-guest-agent-15:4.2.0-59.module+el8.5.0+14169+68d2f392.2.x86_64 qemu-guest-agent-15:6.2.0-11.module+el8.6.0+14707+5aa4b42d.x86_64 qt5-qtbase-5.15.2-4.el8.x86_64 qt5-qtbase-common-5.15.2-4.el8.noarch qt5-qtbase-gui-5.15.2-4.el8.x86_64 qt5-qtsvg-5.15.2-4.el8.x86_64 rsyslog-8.2102.0-7.el8_6.1.x86_64 rsyslog-gnutls-8.2102.0-7.el8_6.1.x86_64 shim-x64-15.6-1.el8.x86_64 udisks2-2.9.0-9.el8.x86_64 vim-minimal-2:8.0.1763-16.el8_5.12.x86_64 vim-minimal-2:8.0.1763-16.el8_5.13.x86_64 xz-5.2.4-4.el8_6.x86_64 xz-libs-5.2.4-4.el8_6.x86_64 zlib-1.2.11-18.el8_5.x86_64

Security vulnerabilities resolved in ADS 4.0 OVA Security Service Pack #2:

Updated Package	RHSA Number	CVE	RHSA Severity
qemu-guest-agent-15:4.2.0-59.module+el8.5.0+14169+68d2f392.2.x86_64	RHSA-2022:0886	CVE-2022-0358	Moderate/Sec.
libarchive-3.3.3-3.el8_5.x86_64	RHSA-2022:0892	CVE-2021-23177 CVE-2021-31566	Moderate/Sec.
vim-minimal-2:8.0.1763-16.el8_5.12.x86_64	RHSA-2022:0894	CVE-2022-0261 CVE-2022-0318 CVE-2022-0359 CVE-2022-0361 CVE-2022-0392 CVE-2022-0413	Moderate/Sec.
glibc-2.28-164.el8_5.3.x86_64 glibc-all-langpacks-2.28-164.el8_5.3.x86_64 glibc-common-2.28-164.el8_5.3.x86_64 glibc-langpack-en-2.28-164.el8_5.3.x86_64 libnsl-2.28-164.el8_5.3.x86_64	RHSA-2022:0896	CVE-2021-3999 CVE-2022-23218 CVE-2022-23219	Moderate/Sec.
libxml2-2.9.7-12.el8_5.x86_64 python3-libxml2-2.9.7-12.el8_5.x86_64	RHSA-2022:0899	CVE-2022-23308	Moderate/Sec.
expat-2.2.5-4.el8_5.3.x86_64	RHSA-2022:0951	CVE-2021-45960 CVE-2021-46143	Important/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

		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	
openssl-1:1.1.1k-6.el8_5.x86_64 openssl-libs-1:1.1.1k-6.el8_5.x86_64 openssl-perl-1:1.1.1k-6.el8_5.x86_64	RHSA-2022:1065	CVE-2022-0778	Important/Sec.
java-1.8.0-openjdk-1:1.8.0.332.b09-1.el8_5.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.332.b09-1.el8_5.x86_64	RHSA-2022:1491	CVE-2022-21426 CVE-2022-21434 CVE-2022-21443 CVE-2022-21476 CVE-2022-21496	Important/Sec.
gzip-1.9-13.el8_5.x86_64	RHSA-2022:1537	CVE-2022-1271	Important/Sec.
polkit-0.115-13.el8_5.2.x86_64 polkit-libs-0.115-13.el8_5.2.x86_64	RHSA-2022:1546	CVE-2021-4115	Moderate/Sec.
kernel-4.18.0-348.23.1.el8_5.x86_64 kernel-core-4.18.0-348.23.1.el8_5.x86_64 kernel-modules-4.18.0-348.23.1.el8_5.x86_64 kernel-tools-4.18.0-348.23.1.el8_5.x86_64 kernel-tools-libs-4.18.0-348.23.1.el8_5.x86_64 python3-perf-4.18.0-348.23.1.el8_5.x86_64	RHSA-2022:1550	CVE-2021-4028 CVE-2022-25636	Important/Sec.
vim-minimal-2:8.0.1763-16.el8_5.13.x86_64	RHSA-2022:1552	CVE-2022-1154	Moderate/Sec.
zlib-1.2.11-18.el8_5.x86_64	RHSA-2022:1642	CVE-2018-25032	Important/Sec.
qemu-guest-agent-15:6.2.0-11.module+el8.6.0+14707+5aa4b42d.x86_64	RHSA-2022:1759	CVE-2021-20196 CVE-2021-33285 CVE-2021-33286 CVE-2021-33287 CVE-2021-33289 CVE-2021-35266 CVE-2021-35267 CVE-2021-35268 CVE-2021-35269 CVE-2021-3622 CVE-2021-3716 CVE-2021-3748 CVE-2021-39251 CVE-2021-39252 CVE-2021-39253 CVE-2021-39254 CVE-2021-39255	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

		CVE-2021-39256 CVE-2021-39257 CVE-2021-39258 CVE-2021-39259 CVE-2021-39260 CVE-2021-39261 CVE-2021-39262 CVE-2021-39263 CVE-2021-3975 CVE-2021-4145 CVE-2021-4158 CVE-2022-0485	
qt5-qtbase-5.15.2-4.el8.x86_64 qt5-qtbase-common-5.15.2-4.el8.noarch qt5-qtbase-gui-5.15.2-4.el8.x86_64	RHSA-2022:1796	CVE-2021-38593	Moderate/Sec.
libtiff-4.0.9-21.el8.x86_64	RHSA-2022:1810	CVE-2020-19131	Moderate/Sec.
libudisks2-2.9.0-9.el8.x86_64 udisks2-2.9.0-9.el8.x86_64	RHSA-2022:1820	CVE-2021-3802	Low/Sec.
qt5-qtsvg-5.15.2-4.el8.x86_64	RHSA-2022:1920	CVE-2021-45930	Moderate/Sec.
cairo-1.15.12-6.el8.x86_64 pixman-0.38.4-2.el8.x86_64	RHSA-2022:1961	CVE-2020-35492	Moderate/Sec.
libsndfile-1.0.28-12.el8.x86_64	RHSA-2022:1968	CVE-2021-4156	Moderate/Sec.
platform-python-3.6.8-45.el8.x86_64 platform-python-devel-3.6.8-45.el8.x86_64 python3-libs-3.6.8-45.el8.x86_64	RHSA-2022:1986	CVE-2021-3737 CVE-2021-4189	Moderate/Sec.
kernel-4.18.0-372.9.1.el8.x86_64 kernel-core-4.18.0-372.9.1.el8.x86_64 kernel-modules-4.18.0-372.9.1.el8.x86_64 kernel-tools-4.18.0-372.9.1.el8.x86_64 kernel-tools-libs-4.18.0-372.9.1.el8.x86_64 python3-perf-4.18.0-372.9.1.el8.x86_64	RHSA-2022:1988	CVE-2020-0404 CVE-2020-13974 CVE-2020-27820 CVE-2020-4788 CVE-2021-0941 CVE-2021-20322 CVE-2021-21781 CVE-2021-26401 CVE-2021-29154 CVE-2021-3612 CVE-2021-3669 CVE-2021-37159 CVE-2021-3743 CVE-2021-3744 CVE-2021-3752 CVE-2021-3759 CVE-2021-3764 CVE-2021-3772 CVE-2021-3773 CVE-2021-4002 CVE-2021-4037 CVE-2021-4083	Important/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

		CVE-2021-4157 CVE-2021-41864 CVE-2021-4197 CVE-2021-4203 CVE-2021-42739 CVE-2021-43056 CVE-2021-43389 CVE-2021-43976 CVE-2021-44733 CVE-2021-45485 CVE-2021-45486 CVE-2022-0001 CVE-2022-0002 CVE-2022-0286 CVE-2022-0322 CVE-2022-1011	
cpio-2.12-11.el8.x86_64	RHSA-2022:1991	CVE-2021-38185	Moderate/Sec.
openssh-8.0p1-13.el8.x86_64 openssh-clients-8.0p1-13.el8.x86_64 openssh-server-8.0p1-13.el8.x86_64	RHSA-2022:2013	CVE-2021-41617	Moderate/Sec.
libssh-0.9.6-3.el8.x86_64 libssh-config-0.9.6-3.el8.noarch	RHSA-2022:2031	CVE-2021-3634	Low/Sec.
bluez-libs-5.56-3.el8.x86_64	RHSA-2022:2081	CVE-2021-41229	Low/Sec.
bind-export-libs-32:9.11.36-3.el8.x86_64	RHSA-2022:2092	CVE-2021-25219	Moderate/Sec.
grub2-common-1:2.02-123.el8.noarch grub2-efi-x64-1:2.02-123.el8.x86_64 grub2-tools-1:2.02-123.el8.x86_64 grub2-tools-extra-1:2.02-123.el8.x86_64 grub2-tools-minimal-1:2.02-123.el8.x86_64	RHSA-2022:2110	CVE-2021-3981	Low/Sec.
rsyslog-8.2102.0-7.el8_6.1.x86_64 rsyslog-gnutls-8.2102.0-7.el8_6.1.x86_64	RHSA-2022:4799	CVE-2022-24903	Important/Sec.
xz-5.2.4-4.el8_6.x86_64 xz-libs-5.2.4-4.el8_6.x86_64	RHSA-2022:4991	CVE-2022-1271	Important/Sec.
cups-libs-1:2.2.6-45.el8_6.2.x86_64	RHSA-2022:5056	CVE-2022-26691	Important/Sec.
grub2-common-1:2.02-123.el8_6.8.noarch grub2-efi-x64-1:2.02-123.el8_6.8.x86_64 grub2-tools-1:2.02-123.el8_6.8.x86_64 grub2-tools-extra-1:2.02-123.el8_6.8.x86_64 grub2-tools-minimal-1:2.02-123.el8_6.8.x86_64 mokutil-1:0.3.0-11.el8_6.1.x86_64 shim-x64-15.6-1.el8.x86_64	RHSA-2022:5095	CVE-2021-3695 CVE-2021-3696 CVE-2021-3697 CVE-2022-28733 CVE-2022-28734 CVE-2022-28735 CVE-2022-28736 CVE-2022-28737	Important/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

ADS-4.0 OVA Security Service Pack #1 includes the following rpm updates:

bind-export-libs-32:9.11.26-6.el8.x86_64	ncurses-6.1-9.20180224.el8.x86_64
bluez-libs-5.56-1.el8.x86_64	ncurses-base-6.1-9.20180224.el8.noarch
cryptsetup-libs-2.3.3-4.el8_5.1.x86_64	ncurses-libs-6.1-9.20180224.el8.x86_64
cups-libs-1:2.2.6-40.el8.x86_64	nettle-3.4.1-7.el8.x86_64
curl-7.61.1-18.el8_4.2.x86_64	nss-3.67.0-7.el8_5.x86_64
curl-7.61.1-22.el8.x86_64	nss-softokn-3.67.0-7.el8_5.x86_64
cyrus-sasl-2.1.27-6.el8_5.x86_64	nss-softokn-freebl-3.67.0-7.el8_5.x86_64
cyrus-sasl-lib-2.1.27-6.el8_5.x86_64	nss-sysinit-3.67.0-7.el8_5.x86_64
dnf-4.7.0-4.el8.noarch	nss-util-3.67.0-7.el8_5.x86_64
dnf-data-4.7.0-4.el8.noarch	openssh-8.0p1-10.el8.x86_64
file-5.33-20.el8.x86_64	openssh-clients-8.0p1-10.el8.x86_64
file-libs-5.33-20.el8.x86_64	openssh-server-8.0p1-10.el8.x86_64
glib2-2.56.4-156.el8.x86_64	openssl-1:1.1.1k-4.el8.x86_64
glibc-2.28-164.el8.x86_64	openssl-1:1.1.1k-5.el8_5.x86_64
glibc-all-langpacks-2.28-164.el8.x86_64	openssl-libs-1:1.1.1k-4.el8.x86_64
glibc-common-2.28-164.el8.x86_64	openssl-libs-1:1.1.1k-5.el8_5.x86_64
glibc-langpack-en-2.28-164.el8.x86_64	openssl-perl-1:1.1.1k-4.el8.x86_64
gnutls-3.6.16-4.el8.x86_64	openssl-perl-1:1.1.1k-5.el8_5.x86_64
gtk-update-icon-cache-3.22.30-8.el8.x86_64	pcre-8.42-6.el8.x86_64
jasper-libs-2.0.14-5.el8.x86_64	platform-python-3.6.8-39.el8_4.x86_64
java-1.8.0-openjdk-1:1.8.0.322.b06-2.el8_5.x86_64	platform-python-3.6.8-41.el8.x86_64
java-1.8.0-openjdk-headless-1:1.8.0.322.b06-2.el8_5.x86_64	platform-python-devel-3.6.8-39.el8_4.x86_64
	platform-python-devel-3.6.8-41.el8.x86_64
json-c-0.13.1-2.el8.x86_64	platform-python-pip-9.0.3-20.el8.noarch
kernel-4.18.0-305.25.1.el8_4.x86_64	polkit-0.115-13.el8_5.1.x86_64
kernel-4.18.0-348.12.2.el8_5.x86_64	polkit-libs-0.115-13.el8_5.1.x86_64
kernel-4.18.0-348.2.1.el8_5.x86_64	python-qt5-rpm-macros-5.15.0-2.el8.noarch
kernel-4.18.0-348.20.1.el8_5.x86_64	python3-dnf-4.7.0-4.el8.noarch
kernel-4.18.0-348.7.1.el8_5.x86_64	python3-hawkey-0.63.0-3.el8.x86_64
kernel-4.18.0-348.el8.x86_64	python3-libdnf-0.63.0-3.el8.x86_64
kernel-core-4.18.0-305.25.1.el8_4.x86_64	python3-libs-3.6.8-39.el8_4.x86_64
kernel-core-4.18.0-348.12.2.el8_5.x86_64	python3-libs-3.6.8-41.el8.x86_64
kernel-core-4.18.0-348.2.1.el8_5.x86_64	python3-perf-4.18.0-305.25.1.el8_4.x86_64
kernel-core-4.18.0-348.20.1.el8_5.x86_64	python3-perf-4.18.0-348.12.2.el8_5.x86_64
kernel-core-4.18.0-348.7.1.el8_5.x86_64	python3-perf-4.18.0-348.2.1.el8_5.x86_64
kernel-core-4.18.0-348.el8.x86_64	python3-perf-4.18.0-348.20.1.el8_5.x86_64
kernel-modules-4.18.0-305.25.1.el8_4.x86_64	python3-perf-4.18.0-348.7.1.el8_5.x86_64
kernel-modules-4.18.0-348.12.2.el8_5.x86_64	python3-perf-4.18.0-348.el8.x86_64
kernel-modules-4.18.0-348.2.1.el8_5.x86_64	python3-pip-9.0.3-20.el8.noarch
kernel-modules-4.18.0-348.20.1.el8_5.x86_64	python3-pip-wheel-9.0.3-20.el8.noarch
kernel-modules-4.18.0-348.7.1.el8_5.x86_64	python3-pyqt5-sip-4.19.24-2.el8.x86_64
kernel-modules-4.18.0-348.el8.x86_64	python3-qt5-5.15.0-2.el8.x86_64
kernel-tools-4.18.0-305.25.1.el8_4.x86_64	python3-qt5-base-5.15.0-2.el8.x86_64
kernel-tools-4.18.0-348.12.2.el8_5.x86_64	python3-rpm-4.14.3-19.el8.x86_64
kernel-tools-4.18.0-348.2.1.el8_5.x86_64	python3-rpm-4.14.3-19.el8_5.2.x86_64
kernel-tools-4.18.0-348.20.1.el8_5.x86_64	python3-scipy-1.0.0-21.module+el8.5.0+10916+41bd434d.x86_64
kernel-tools-4.18.0-348.7.1.el8_5.x86_64	
kernel-tools-4.18.0-348.el8.x86_64	python36-3.6.8-38.module+el8.5.0+12207+5c5719bc.x86_64
kernel-tools-libs-4.18.0-305.25.1.el8_4.x86_64	qemu-guest-agent-15:4.2.0-59.module+el8.5.0+12817+cb650d43.x86_64
kernel-tools-libs-4.18.0-348.12.2.el8_5.x86_64	
kernel-tools-libs-4.18.0-348.2.1.el8_5.x86_64	qemu-guest-agent-15:4.2.0-

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

kernel-tools-libs-4.18.0-348.20.1.el8_5.x86_64	59.module+el8.5.0+13495+8166cdf8.1.x86_64
kernel-tools-libs-4.18.0-348.7.1.el8_5.x86_64	qt5-qtbase-5.15.2-3.el8.x86_64
kernel-tools-libs-4.18.0-348.el8.x86_64	qt5-qtbase-common-5.15.2-3.el8.noarch
kexec-tools-2.0.20-57.el8.x86_64	qt5-qtbase-gui-5.15.2-3.el8.x86_64
libX11-1.6.8-5.el8.x86_64	qt5-qtconnectivity-5.15.2-2.el8.x86_64
libX11-common-1.6.8-5.el8.noarch	qt5-qtdeclarative-5.15.2-2.el8.x86_64
libX11-xcb-1.6.8-5.el8.x86_64	qt5-qtlocation-5.15.2-2.el8.x86_64
libcurl-7.61.1-18.el8_4.2.x86_64	qt5-qtmultimedia-5.15.2-2.el8.x86_64
libcurl-7.61.1-22.el8.x86_64	qt5-qtsensors-5.15.2-2.el8.x86_64
libdnf-0.63.0-3.el8.x86_64	qt5-qtserialport-5.15.2-2.el8.x86_64
libgcc-8.5.0-3.el8.x86_64	qt5-qtsvg-5.15.2-3.el8.x86_64
libgcc-8.5.0-4.el8_5.x86_64	qt5-qttools-common-5.15.2-3.el8.noarch
libgcrypt-1.8.5-6.el8.x86_64	qt5-qttools-libs-designer-5.15.2-3.el8.x86_64
libgfortran-8.5.0-3.el8.x86_64	qt5-qttools-libs-help-5.15.2-3.el8.x86_64
libgfortran-8.5.0-4.el8_5.x86_64	qt5-qtwebchannel-5.15.2-2.el8.x86_64
libgomp-8.5.0-3.el8.x86_64	qt5-qtwebsockets-5.15.2-2.el8.x86_64
libgomp-8.5.0-4.el8_5.x86_64	qt5-qtx11extras-5.15.2-2.el8.x86_64
libjpeg-turbo-1.5.3-12.el8.x86_64	qt5-qtxmlpatterns-5.15.2-2.el8.x86_64
libnsl-2.28-164.el8.x86_64	rpm-4.14.3-19.el8.x86_64
libquadmath-8.5.0-3.el8.x86_64	rpm-4.14.3-19.el8_5.2.x86_64
libquadmath-8.5.0-4.el8_5.x86_64	rpm-build-libs-4.14.3-19.el8.x86_64
libsepol-2.9-3.el8.x86_64	rpm-build-libs-4.14.3-19.el8_5.2.x86_64
libsolv-0.7.16-3.el8_4.x86_64	rpm-libs-4.14.3-19.el8.x86_64
libsolv-0.7.19-1.el8.x86_64	rpm-libs-4.14.3-19.el8_5.2.x86_64
libssh-0.9.4-3.el8.x86_64	rpm-plugin-selinux-4.14.3-19.el8.x86_64
libssh-config-0.9.4-3.el8.noarch	rpm-plugin-selinux-4.14.3-19.el8_5.2.x86_64
libstdc++-8.5.0-3.el8.x86_64	rpm-plugin-systemd-inhibit-4.14.3-19.el8.x86_64
libstdc++-8.5.0-4.el8_5.x86_64	rpm-plugin-systemd-inhibit-4.14.3-19.el8_5.2.x86_64
libtiff-4.0.9-20.el8.x86_64	sqlite-3.26.0-15.el8.x86_64
libwebp-1.0.0-5.el8.x86_64	sqlite-libs-3.26.0-15.el8.x86_64
lua-5.3.4-12.el8.x86_64	tcpdump-14:4.9.3-2.el8.x86_64
lua-libs-5.3.4-12.el8.x86_64	vim-minimal-2:8.0.1763-16.el8.x86_64
	vim-minimal-2:8.0.1763-16.el8_5.4.x86_64
	yum-4.7.0-4.el8.noarch

Security vulnerabilities resolved in ADS 4.0 OVA Security Service Pack #1:

Updated Package	RHSA Number	CVE	RHSA Severity
kernel-4.18.0-305.25.1.el8_4.x86_64 kernel-core-4.18.0-305.25.1.el8_4.x86_64 kernel-modules-4.18.0-305.25.1.el8_4.x86_64 kernel-tools-4.18.0-305.25.1.el8_4.x86_64 kernel-tools-libs-4.18.0-305.25.1.el8_4.x86_64 python3-perf-4.18.0-305.25.1.el8_4.x86_64	RHSA-2021:4056	CVE-2020-36385 CVE-2021-0512 CVE-2021-3656	Important/Sec. Moderate/Sec. Important/Sec. Moderate/Sec. Important/Sec. Important/Sec.
platform-python-3.6.8-39.el8_4.x86_64 platform-python-devel-3.6.8-39.el8_4.x86_64 python3-libs-3.6.8-39.el8_4.x86_64	RHSA-2021:4057	CVE-2021-3733	Moderate/Sec.
curl-7.61.1-18.el8_4.2.x86_64	RHSA-2021:4059	CVE-2021-22946	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

libcurl-7.61.1-18.el8_4.2.x86_64		CVE-2021-22947	
libsolv-0.7.16-3.el8_4.x86_64	RHSA-2021:4060	CVE-2021-33928 CVE-2021-33929 CVE-2021-33930 CVE-2021-33938	Moderate/Sec.
python3-scipy-1.0.0-21.module+el8.5.0+10916+41bd434d.x python36-3.6.8-38.module+el8.5.0+12207+5c5719bc.x86_64	RHSA-2021:4150	CVE-2021-20270 CVE-2021-27291	Moderate/Sec.
python-qt5-rpm-macros-5.15.0-2.el8.noarch python3-pyqt5-sip-4.19.24-2.el8.x86_64 python3-qt5-5.15.0-2.el8.x86_64 python3-qt5-base-5.15.0-2.el8.x86_64 qt5-qtbase-5.15.2-3.el8.x86_64 qt5-qtbase-common-5.15.2-3.el8.noarch qt5-qtbase-gui-5.15.2-3.el8.x86_64 qt5-qtconnectivity-5.15.2-2.el8.x86_64 qt5-qtdeclarative-5.15.2-2.el8.x86_64 qt5-qtlocation-5.15.2-2.el8.x86_64 qt5-qtmultimedia-5.15.2-2.el8.x86_64 qt5-qtsensors-5.15.2-2.el8.x86_64 qt5-qtserialport-5.15.2-2.el8.x86_64 qt5-qtsvg-5.15.2-3.el8.x86_64 qt5-qttools-common-5.15.2-3.el8.noarch qt5-qttools-libs-designer-5.15.2-3.el8.x86_64 qt5-qttools-libs-help-5.15.2-3.el8.x86_64 qt5-qtwebchannel-5.15.2-2.el8.x86_64 qt5-qtwebsockets-5.15.2-2.el8.x86_64 qt5-qtx11extras-5.15.2-2.el8.x86_64 qt5-qtxmlpatterns-5.15.2-2.el8.x86_64	RHSA-2021:4172	CVE-2021-3481	Moderate/Sec.
qemu-guest-agent-15:4.2.0-59.module+el8.5.0+12817+cb650d43.x86_64	RHSA-2021:4191	CVE-2020-15859 CVE-2021-3592 CVE-2021-3593 CVE-2021-3594 CVE-2021-3595 CVE-2021-3631 CVE-2021-3667	Moderate/Sec.
libwebp-1.0.0-5.el8.x86_64	RHSA-2021:4231	CVE-2018-25009 CVE-2018-25010 CVE-2018-25012 CVE-2018-25013 CVE-2018-25014 CVE-2020-36330 CVE-2020-36331 CVE-2020-36332	Moderate/Sec.
jasper-libs-2.0.14-5.el8.x86_64	RHSA-2021:4235	CVE-2020-27828 CVE-2021-26926 CVE-2021-26927 CVE-2021-3272	Moderate/Sec.
tcpdump-14:4.9.3-2.el8.x86_64	RHSA-2021:4236	CVE-2020-8037	Low/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

libtiff-4.0.9-20.el8.x86_64	RHSA-2021:4241	CVE-2020-35521 CVE-2020-35522 CVE-2020-35523 CVE-2020-35524	Moderate/Sec.
libjpeg-turbo-1.5.3-12.el8.x86_64	RHSA-2021:4288	CVE-2020-17541	Moderate/Sec.
libX11-1.6.8-5.el8.x86_64 libX11-common-1.6.8-5.el8.noarch libX11-xcb-1.6.8-5.el8.x86_64	RHSA-2021:4326	CVE-2021-31535	Moderate/Sec.
kernel-4.18.0-348.el8.x86_64 kernel-core-4.18.0-348.el8.x86_64 kernel-modules-4.18.0-348.el8.x86_64 kernel-tools-4.18.0-348.el8.x86_64 kernel-tools-libs-4.18.0-348.el8.x86_64 python3-perf-4.18.0-348.el8.x86_64	RHSA-2021:4356	CVE-2020-0427 CVE-2020-24502 CVE-2020-24503 CVE-2020-24504 CVE-2020-24586 CVE-2020-24587 CVE-2020-24588 CVE-2020-26139 CVE-2020-26140 CVE-2020-26141 CVE-2020-26143 CVE-2020-26144 CVE-2020-26145 CVE-2020-26146 CVE-2020-26147 CVE-2020-27777 CVE-2020-29368 CVE-2020-29660 CVE-2020-36158 CVE-2020-36386 CVE-2021-0129 CVE-2021-20194 CVE-2021-20239 CVE-2021-23133 CVE-2021-28950 CVE-2021-28971 CVE-2021-29155 CVE-2021-29646 CVE-2021-29650 CVE-2021-31440 CVE-2021-31829 CVE-2021-31916 CVE-2021-33200 CVE-2021-3348 CVE-2021-3489 CVE-2021-3564 CVE-2021-3573 CVE-2021-3600 CVE-2021-3635 CVE-2021-3659 CVE-2021-3679 CVE-2021-3732	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

glibc-2.28-164.el8.x86_64 glibc-all-langpacks-2.28-164.el8.x86_64 glibc-common-2.28-164.el8.x86_64 glibc-langpack-en-2.28-164.el8.x86_64 libnsl-2.28-164.el8.x86_64	RHSA-2021:4358	CVE-2021-27645 CVE-2021-33574 CVE-2021-35942	Moderate/Sec.
openssh-8.0p1-10.el8.x86_64 openssh-clients-8.0p1-10.el8.x86_64 openssh-server-8.0p1-10.el8.x86_64	RHSA-2021:4368	CVE-2020-14145	Moderate/Sec.
pcre-8.42-6.el8.x86_64	RHSA-2021:4373	CVE-2019-20838 CVE-2020-14155	Low/Sec.
file-5.33-20.el8.x86_64 file-libs-5.33-20.el8.x86_64	RHSA-2021:4374	CVE-2019-18218	Moderate/Sec.
gtk-update-icon-cache-3.22.30-8.el8.x86_64	RHSA-2021:4381	CVE-2020-13558 CVE-2020-24870 CVE-2020-27918 CVE-2020-29623 CVE-2020-36241 CVE-2021-1765 CVE-2021-1788 CVE-2021-1789 CVE-2021-1799 CVE-2021-1801 CVE-2021-1844 CVE-2021-1870 CVE-2021-1871 CVE-2021-21775 CVE-2021-21779 CVE-2021-21806 CVE-2021-28650 CVE-2021-30663 CVE-2021-30665 CVE-2021-30682 CVE-2021-30689 CVE-2021-30720 CVE-2021-30734 CVE-2021-30744 CVE-2021-30749 CVE-2021-30758 CVE-2021-30795 CVE-2021-30797 CVE-2021-30799	Moderate/Sec.
json-c-0.13.1-2.el8.x86_64	RHSA-2021:4382	CVE-2020-12762	Moderate/Sec.
bind-export-libs-32:9.11.26-6.el8.x86_64	RHSA-2021:4384	CVE-2021-25214	Moderate/Sec.
glib2-2.56.4-156.el8.x86_64	RHSA-2021:4385	CVE-2021-28153 CVE-2021-3800	Moderate/Sec.
libgcc-8.5.0-3.el8.x86_64 libgfortran-8.5.0-3.el8.x86_64 libgomp-8.5.0-3.el8.x86_64	RHSA-2021:4386	CVE-2018-20673	Low/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

libquadmath-8.5.0-3.el8.x86_64 libstdc++-8.5.0-3.el8.x86_64			
libssh-0.9.4-3.el8.x86_64 libssh-config-0.9.4-3.el8.noarch	RHSA-2021:4387	CVE-2020-16135	Low/Sec.
cups-libs-1:2.2.6-40.el8.x86_64	RHSA-2021:4393	CVE-2020-10001	Moderate/Sec.
sqlite-3.26.0-15.el8.x86_64 sqlite-libs-3.26.0-15.el8.x86_64	RHSA-2021:4396	CVE-2019-13750 CVE-2019-13751 CVE-2019-19603 CVE-2019-5827 CVE-2020-13435	Moderate/Sec.
platform-python-3.6.8-41.el8.x86_64 platform-python-devel-3.6.8-41.el8.x86_64 python3-libs-3.6.8-41.el8.x86_64	RHSA-2021:4399	CVE-2021-3426	Moderate/Sec.
kexec-tools-2.0.20-57.el8.x86_64	RHSA-2021:4404	CVE-2021-20269	Low/Sec.
libsolv-0.7.19-1.el8.x86_64	RHSA-2021:4408	CVE-2021-3200	Low/Sec.
libgcrypt-1.8.5-6.el8.x86_64	RHSA-2021:4409	CVE-2021-33560	Moderate/Sec.
openssl-1:1.1.1k-4.el8.x86_64 openssl-libs-1:1.1.1k-4.el8.x86_64 openssl-perl-1:1.1.1k-4.el8.x86_64	RHSA-2021:4424 RHSA-2021:5226	CVE-2021-23840 CVE-2021-23841	Moderate/Sec. Moderate/Sec.
ncurses-6.1-9.20180224.el8.x86_64 ncurses-base-6.1-9.20180224.el8.noarch ncurses-libs-6.1-9.20180224.el8.x86_64	RHSA-2021:4426	CVE-2019-17594 CVE-2019-17595	Moderate/Sec.
bluez-libs-5.56-1.el8.x86_64	RHSA-2021:4432	CVE-2020-26558	Moderate/Sec.
gnutls-3.6.16-4.el8.x86_64 nettle-3.4.1-7.el8.x86_64	RHSA-2021:4451	CVE-2021-20231 CVE-2021-20232 CVE-2021-3580	Moderate/Sec.
platform-python-pip-9.0.3-20.el8.noarch python3-pip-9.0.3-20.el8.noarch python3-pip-wheel-9.0.3-20.el8.noarch	RHSA-2021:4455	CVE-2021-3572	Low/Sec.
dnf-4.7.0-4.el8.noarch dnf-data-4.7.0-4.el8.noarch libdnf-0.63.0-3.el8.x86_64 python3-dnf-4.7.0-4.el8.noarch python3-hawkey-0.63.0-3.el8.x86_64 python3-libdnf-0.63.0-3.el8.x86_64 yum-4.7.0-4.el8.noarch	RHSA-2021:4464	CVE-2021-3445	Moderate/Sec.
python3-rpm-4.14.3-19.el8.x86_64 rpm-4.14.3-19.el8.x86_64 rpm-build-libs-4.14.3-19.el8.x86_64 rpm-libs-4.14.3-19.el8.x86_64 rpm-plugin-selinux-4.14.3-19.el8.x86_64 rpm-plugin-systemd-inhibit-4.14.3-19.el8.x86_64	RHSA-2021:4489	CVE-2021-20266	Low/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

lua-5.3.4-12.el8.x86_64 lua-libs-5.3.4-12.el8.x86_64	RHSA-2021:4510	CVE-2020-24370	Low/Sec.
curl-7.61.1-22.el8.x86_64 libcurl-7.61.1-22.el8.x86_64	RHSA-2021:4511	CVE-2021-22876 CVE-2021-22898 CVE-2021-22925	Moderate/Sec.
libsepol-2.9-3.el8.x86_64	RHSA-2021:4513	CVE-2021-36084 CVE-2021-36085 CVE-2021-36086 CVE-2021-36087	Moderate/Sec.
vim-minimal-2:8.0.1763-16.el8.x86_64	RHSA-2021:4517	CVE-2021-3778 CVE-2021-3796	Moderate/Sec.
libgcc-8.5.0-4.el8_5.x86_64 libgfortran-8.5.0-4.el8_5.x86_64 libgomp-8.5.0-4.el8_5.x86_64 libquadmath-8.5.0-4.el8_5.x86_64 libstdc++-8.5.0-4.el8_5.x86_64	RHSA-2021:4587	CVE-2021-42574	Moderate/Sec.
kernel-4.18.0-348.2.1.el8_5.x86_64 kernel-core-4.18.0-348.2.1.el8_5.x86_64 kernel-modules-4.18.0-348.2.1.el8_5.x86_64 kernel-tools-4.18.0-348.2.1.el8_5.x86_64 kernel-tools-libs-4.18.0-348.2.1.el8_5.x86_64 python3-perf-4.18.0-348.2.1.el8_5.x86_64	RHSA-2021:4647	CVE-2021-20317 CVE-2021-43267	Important/Sec.
nss-3.67.0-7.el8_5.x86_64 nss-softokn-3.67.0-7.el8_5.x86_64 nss-softokn-freebl-3.67.0-7.el8_5.x86_64 nss-sysinit-3.67.0-7.el8_5.x86_64 nss-util-3.67.0-7.el8_5.x86_64	RHSA-2021:4903	CVE-2021-43527	Critical/Sec.
kernel-4.18.0-348.7.1.el8_5.x86_64 kernel-core-4.18.0-348.7.1.el8_5.x86_64 kernel-modules-4.18.0-348.7.1.el8_5.x86_64 kernel-tools-4.18.0-348.7.1.el8_5.x86_64 kernel-tools-libs-4.18.0-348.7.1.el8_5.x86_64 python3-perf-4.18.0-348.7.1.el8_5.x86_64	RHSA-2021:5227	CVE-2021-20321	Moderate/Sec.
qemu-guest-agent-15:4.2.0-59.module+el8.5.0+13495+8166cdf8.1.x86_64	RHSA-2021:5238	CVE-2021-20257 CVE-2021-3930	Low/Sec.
kernel-4.18.0-348.12.2.el8_5.x86_64 kernel-core-4.18.0-348.12.2.el8_5.x86_64 kernel-modules-4.18.0-348.12.2.el8_5.x86_64 kernel-tools-4.18.0-348.12.2.el8_5.x86_64 kernel-tools-libs-4.18.0-348.12.2.el8_5.x86_64 python3-perf-4.18.0-348.12.2.el8_5.x86_64	RHSA-2022:0188	CVE-2021-4155 CVE-2022-0185	Important/Sec.
polkit-0.115-13.el8_5.1.x86_64 polkit-libs-0.115-13.el8_5.1.x86_64	RHSA-2022:0267	CVE-2021-4034	Important/Sec.
java-1.8.0-openjdk-1:1.8.0.322.b06-2.el8_5.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.322.b06-2.el8_5.x86_64	RHSA-2022:0307	CVE-2022-21248 CVE-2022-21282 CVE-2022-21283 CVE-2022-21293 CVE-2022-21294	Moderate/Sec.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

		CVE-2022-21296 CVE-2022-21299 CVE-2022-21305 CVE-2022-21340 CVE-2022-21341 CVE-2022-21360 CVE-2022-21365	
vim-minimal-2:8.0.1763-16.el8_5.4.x86_64	RHSA-2022:0366	CVE-2021-3872 CVE-2021-3984 CVE-2021-4019 CVE-2021-4192 CVE-2021-4193	Moderate/Sec.
python3-rpm-4.14.3-19.el8_5.2.x86_64 rpm-4.14.3-19.el8_5.2.x86_64 rpm-build-libs-4.14.3-19.el8_5.2.x86_64 rpm-libs-4.14.3-19.el8_5.2.x86_64 rpm-plugin-selinux-4.14.3-19.el8_5.2.x86_64 rpm-plugin-systemd-inhibit-4.14.3-19.el8_5.2.x86_64	RHSA-2022:0368	CVE-2021-3521	Moderate/Sec.
cryptsetup-libs-2.3.3-4.el8_5.1.x86_64	RHSA-2022:0370	CVE-2021-4122	Moderate/Sec.
cyrus-sasl-2.1.27-6.el8_5.x86_64 cyrus-sasl-lib-2.1.27-6.el8_5.x86_64	RHSA-2022:0658	CVE-2022-24407	Important/Sec.
kernel-4.18.0-348.20.1.el8_5.x86_64 kernel-core-4.18.0-348.20.1.el8_5.x86_64 kernel-modules-4.18.0-348.20.1.el8_5.x86_64 kernel-tools-4.18.0-348.20.1.el8_5.x86_64 kernel-tools-libs-4.18.0-348.20.1.el8_5.x86_64 python3-perf-4.18.0-348.20.1.el8_5.x86_64	RHSA-2022:0825	CVE-2021-0920 CVE-2021-4154 CVE-2022-0330 CVE-2022-0435 CVE-2022-0492 CVE-2022-0516 CVE-2022-0847 CVE-2022-22942	Important/Sec.

Mitigation: N/A

SECTION 1C – ENTITLEMENTS AND CONTACTS

Material Coverage Entitlements: This PCN is being offered at no charge to the customer with valid support / upgrade contracts. The software updates are available on support.avaya.com and from plds.avaya.com.

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

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

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

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.

© 2022-2026 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.