Product Correction Notice (PCN)

Issue Date: 18-April-2022
Supplement Date: 18-March-2024
Expiration Date: NA
PCN Number: 2140S

SECTION 1 - CUSTOMER NOTICE

Products affected by this PCN:

Avaya Aura® Application Enablement Services 10.1 vAppliance running on Avaya provided servers: Avaya Solutions Platform 130 R5.x (Dell® PowerEdge R640).
Avaya Aura® Application Enablement Services 10.1 vAppliance running on Customer provided VMware® certified hardware.
Reference the Avaya Aura® Platform Offer Definition for details.

Description:

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

18 March 2024 – Supplement 21 of this PCN introduces **Avaya Aura® Application Enablement Services 10.1 (AES) 10.1 Security Service Pack #22**.
(**AV-AES10.1-RHEL8.4-SSP-022-01.tar.bz2; PLDS ID** AES000001020**)**

- AES 10.1 security updates are now provided in a Security Service Pack (SSP). There will no longer be a Linux Security Update (LSU).
- AES SSP #22 is only applicable to AES 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later or on 10.1.0.1 or later that has SSP #1-21 installed.
- **Critical Note:** AES SSP #22 **must** be installed after applying the 10.1.0.1 or later Service Pack/Feature Pack to ensure robust security protection. Reference **PCN2139S** for additional details on the mandatory AES 10.1.0.1 Service Pack and subsequent Service Packs/Feature Packs.
- Installation of AES SSP #22 will fail unless Service Pack 10.1.0.1 or later is installed first.
- Security Service Packs should NOT be applied on the Software Only offer.
- 10.1 SSPs will not work on the 10.2 release and there will be different SSPs for both 10.1 and 10.2.
- 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 #22.

16 January 2024 – Supplement 20 of this PCN introduces **Avaya Aura® Application Enablement Services 10.1 (AES) 10.1 Security Service Pack #21**.
(**AV-AES10.1-RHEL8.4-SSP-021-01.tar.bz2; PLDS ID** AES000001015**)**

- AES 10.1 security updates are now provided in a Security Service Pack (SSP). There will no longer be a Linux Security Update (LSU).
- AES SSP #21 is only applicable to AES 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later or on 10.1.0.1 or later that has SSP #1-20 installed.
- **Critical Note:** AES SSP #21 **must** be installed after applying the 10.1.0.1 or later Service

© 2022-2024 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.

Pack/Feature Pack to ensure robust security protection. Reference **PCN2139S** for additional details on the mandatory AES 10.1.0.1 Service Pack and subsequent Service Packs/Feature Packs.
- Installation of AES SSP #21 will fail unless Service Pack 10.1.0.1 or later is installed first.
- Security Service Packs should NOT be applied on the Software Only offer.
- 10.1 SSPs will not work on the 10.2 release and there will be different SSPs for both 10.1 and 10.2.
- 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 #21.

18 December 2023 – Supplement 19 of this PCN introduces **Avaya Aura® Application Enablement Services 10.1 (AES) 10.1 Security Service Pack #20**.
(**AV-AES10.1-RHEL8.4-SSP-020-01.tar.bz2; PLDS ID** AES00000988**)**

- AES 10.1 security updates are now provided in a Security Service Pack (SSP). There will no longer be a Linux Security Update (LSU).
- AES SSP #20 is only applicable to AES 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later or on 10.1.0.1 or later that has SSP #1-19 installed.
- **Critical Note:** AES SSP #20 **must** be installed after applying the 10.1.0.1 or later Service Pack/Feature Pack to ensure robust security protection. Reference **PCN2139S** for additional details on the mandatory AES 10.1.0.1 Service Pack and subsequent Service Packs/Feature Packs.
- Installation of AES SSP #20 will fail unless Service Pack 10.1.0.1 or later is installed first.
- Security Service Packs should NOT be applied on the Software Only offer.
- 10.1 SSPs will not work on the 10.2 release and there will be different SSPs for both 10.1 and 10.2.
- 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 #20.

20 November 2023 – Supplement 18 of this PCN introduces **Avaya Aura® Application Enablement Services 10.1 (AES) 10.1 Security Service Pack #19**.
(**AV-AES10.1-RHEL8.4-SSP-019-03.tar.bz2; PLDS ID** AES00000985**)**

- AES 10.1 security updates are now provided in a Security Service Pack (SSP). There will no longer be a Linux Security Update (LSU).
- AES SSP #19 is only applicable to AES 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later or on 10.1.0.1 or later that has SSP #1-18 installed.
- **Critical Note:** AES SSP #19 **must** be installed after applying the 10.1.0.1 or later Service Pack/Feature Pack to ensure robust security protection. Reference **PCN2139S** for additional details on the mandatory AES 10.1.0.1 Service Pack and subsequent Service Packs/Feature Packs.
- Installation of AES SSP #19 will fail unless Service Pack 10.1.0.1 or later is installed first.
- 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 #19.

© 2022-2024 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.

16 October 2023 – Supplement 17 of this PCN introduces **Avaya Aura® Application Enablement Services 10.1 (AES) 10.1 Security Service Pack #18**.
(**AV-AES10.1-RHEL8.4-SSP-018-01.tar.bz2; PLDS ID** AES00000984**)**

- AES 10.1 security updates are now provided in a Security Service Pack (SSP). There will no longer be a Linux Security Update (LSU).
- AES SSP #18 is only applicable to AES 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later or on 10.1.0.1 or later that has SSP #1-17 installed.
- **Critical Note:** AES SSP #18 **must** be installed after applying the 10.1.0.1 or later Service Pack/Feature Pack to ensure robust security protection. Reference **PCN2139S** for additional details on the mandatory AES 10.1.0.1 Service Pack and subsequent Service Packs/Feature Packs.
- Installation of AES SSP #18 will fail unless Service Pack 10.1.0.1 or later is installed first.
- 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 #18.

18 September 2023 – Supplement 16 of this PCN introduces **Avaya Aura® Application Enablement Services 10.1 (AES) 10.1 Security Service Pack #17**.
(**AV-AES10.1-RHEL8.4-SSP-017-01.tar.bz2; PLDS ID** AES00000983**)**

- AES 10.1 security updates are now provided in a Security Service Pack (SSP). There will no longer be a Linux Security Update (LSU).
- AES SSP #17 is only applicable to AES 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later or on 10.1.0.1 or later that has SSP #1-16 installed.
- **Critical Note:** AES SSP #17 **must** be installed after applying the 10.1.0.1 or later Service Pack/Feature Pack to ensure robust security protection. Reference **PCN2139S** for additional details on the mandatory AES 10.1.0.1 Service Pack and subsequent Service Packs/Feature Packs.
- Installation of AES SSP #17 will fail unless Service Pack 10.1.0.1 or later is installed first.
- 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.

28 August 2023 – Supplement 15 of this PCN introduces **Avaya Aura® Application Enablement Services 10.1 (AES) 10.1 Security Service Pack #16**.
(**AV-AES10.1-RHEL8.4-SSP-016-01.tar.bz2; PLDS ID AES00000974)**

- AES 10.1 security updates are now provided in a Security Service Pack (SSP). There will no longer be a Linux Security Update (LSU).
- AES SSP #16 is only applicable to AES 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later or on 10.1.0.1 or later that has SSP #1-15 installed.
- **Critical Note:** AES SSP #16 **must** be installed after applying the 10.1.0.1 or later Service Pack/Feature Pack to ensure robust security protection. Reference **PCN2139S** for additional details on the mandatory AES 10.1.0.1. Service Pack and subsequent Service Packs/Feature Packs.
- Installation of AES SSP #16 will fail unless Service Pack 10.1.0.1 or later is installed first.

© 2022-2024 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 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.

17 July 2023 – Supplement 14 of this PCN introduces **Avaya Aura® Application Enablement Services 10.1 (AES) 10.1 Security Service Pack #15**.
(**AV-AES10.1-RHEL8.4-SSP-015-01.tar.bz2; PLDS ID AES00000970)**

- AES 10.1 security updates are now provided in a Security Service Pack (SSP). There will no longer be a Linux Security Update (LSU).
- AES SSP #15 is only applicable to AES 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later or on 10.1.0.1 or later that has SSP #1-14 installed.
- **Critical Note:** AES SSP #15 **must** be installed after applying the 10.1.0.1 or later Service Pack/Feature Pack to ensure robust security protection. Reference **PCN2139S** for additional details on the mandatory AES 10.1.0.1. Service Pack and subsequent Service Packs/Feature Packs.
- Installation of AES SSP #15 will fail unless Service Pack 10.1.0.1 or later is installed first.
- 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.

20 June 2023 – Supplement 13 of this PCN introduces **Avaya Aura® Application Enablement Services 10.1 (AES) 10.1 Security Service Pack #14**.
(**AV-AES10.1-RHEL8.4-SSP-014-01.tar.bz2; PLDS ID AES00000969)**

- AES 10.1 security updates are now provided in a Security Service Pack (SSP). There will no longer be a Linux Security Update (LSU).
- AES SSP #14 is only applicable to AES 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later or on 10.1.0.1 or later that has SSP #1-13 installed.
- **Critical Note:** AES SSP #14 **must** be installed after applying the 10.1.0.1 or later Service Pack/Feature Pack to ensure robust security protection. Reference **PCN2139S** for additional details on the mandatory AES 10.1.0.1. Service Pack and subsequent Service Packs/Feature Packs.
- Installation of AES SSP #14 will fail unless Service Pack 10.1.0.1 or later is installed first.
- 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.

22 May 2023 – Supplement 12 of this PCN introduces **Avaya Aura® Application Enablement Services 10.1 (AES) 10.1 Security Service Pack #13**.
(**AV-AES10.1-RHEL8.4-SSP-013-01.tar.bz2; PLDS ID AES00000966)**

- AES 10.1 security updates are now provided in a Security Service Pack (SSP). There will no longer be a Linux Security Update (LSU).
- AES SSP #13 is only applicable to AES 10.1.0.1 or later. It can be installed directly on 10.1.0.1

© 2022-2024 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.

or later or on 10.1.0.1 or later that has SSP #1-12 installed.

- **Critical Note:** AES SSP #13 **must** be installed after applying the 10.1.0.1 or later Service Pack/Feature Pack to ensure robust security protection. Reference **PCN2139S** for additional details on the mandatory AES 10.1.0.1. Service Pack and subsequent Service Packs/Feature Packs.
- Installation of AES SSP #13 will fail unless Service Pack 10.1.0.1 or later is installed first.
- 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 #13.

17 April 2023 – Supplement 11 of this PCN introduces **Avaya Aura® Application Enablement Services 10.1 (AES) 10.1 Security Service Pack #12.**
(**AV-AES10.1-RHEL8.4-SSP-012-01.tar.bz2; PLDS ID AES00000964)**

- AES 10.1 security updates are now provided in a Security Service Pack (SSP). There will no longer be a Linux Security Update (LSU).
- AES SSP #12 is only applicable to AES 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later or on 10.1.0.1 or later that has SSP #1-11 installed.
- **Critical Note:** AES SSP #12 **must** be installed after applying the 10.1.0.1 or later Service Pack/Feature Pack to ensure robust security protection. Reference **PCN2139S** for additional details on the mandatory AES 10.1.0.1. Service Pack and subsequent Service Packs/Feature Packs.
- Installation of AES SSP #12 will fail unless Service Pack 10.1.0.1 or later is installed first.
- 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.

20 March 2023 – Supplement 10 of this PCN introduces **Avaya Aura® Application Enablement Services 10.1 (AES) 10.1 Security Service Pack #11.**
(**AV-AES10.1-RHEL8.4-SSP-011-01.tar.bz2; PLDS ID AES00000963)**

- AES 10.1 security updates are now provided in a Security Service Pack (SSP). There will no longer be a Linux Security Update (LSU).
- AES SSP #11 is only applicable to AES 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later or on 10.1.0.1 or later that has SSP #1-10 installed.
- **Critical Note:** AES SSP #11 **must** be installed after applying the 10.1.0.1 or later Service Pack to ensure robust security protection. Reference **PCN2139S** for additional details on the mandatory AES 10.1.0.1. Service Pack and subsequent Service Packs.
- Installation of AES SSP #11 will fail unless Service Pack 10.1.0.1 or later is installed first.
- 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.
- There was no Aura February 2023 Security Service Pack update required for Communication Manager, Session Manager, System Manager and Application Enablement Services. Only WebLM required a February 2023 Security Service Pack update.

© 2022-2024 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.

23 January 2023 – Supplement 9 of this PCN introduces **Avaya Aura® Application Enablement Services 10.1 (AES) 10.1 Security Service Pack #10.**
(**AV-AES10.1-RHEL8.4-SSP-010-01.tar.bz2; PLDS ID AES00000960)**

- AES 10.1 security updates are now provided in a Security Service Pack (SSP). There will no longer be a Linux Security Update (LSU).
- AES SSP #10 is only applicable to AES 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later or on 10.1.0.1 or later that has SSP #1-9 installed.
- **Critical Note:** AES SSP #10 **must** be installed after applying the 10.1.0.1 or later Service Pack to ensure robust security protection. Reference **PCN2139S** for additional details on the mandatory AES 10.1.0.1. Service Pack and subsequent Service Packs.
- Installation of AES SSP #10 will fail unless Service Pack 10.1.0.1 or later is installed first.
- 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.

19 December 2022 – Supplement 8 of this PCN introduces **Avaya Aura® Application Enablement Services 10.1 (AES) 10.1 Security Service Pack #9.**
(**AV-AES10.1-RHEL8.4-SSP-009-01.tar.bz2; PLDS ID AES00000955)**

- AES 10.1 security updates are now provided in a Security Service Pack (SSP). There will no longer be a Linux Security Update (LSU).
- AES SSP #9 is only applicable to AES 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later or on 10.1.0.1 or later that has SSP #1-8 installed.
- **Critical Note:** AES SSP #9 **must** be installed after applying the 10.1.0.1 or later Service Pack to ensure robust security protection. Reference **PCN2139S** for additional details on the mandatory AES 10.1.0.1. Service Pack and subsequent Service Packs.
- Installation of AES SSP #9 will fail unless Service Pack 10.1.0.1 or later is installed first.
- 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.

28 November 2022 – Supplement 7 of this PCN introduces **Avaya Aura® Application Enablement Services 10.1 (AES) 10.1 Security Service Pack #8.**
(**AV-AES10.1-RHEL8.4-SSP-008-01.tar.bz2; PLDS ID AES00000953)**

- AES 10.1 security updates are now provided in a Security Service Pack (SSP). There will no longer be a Linux Security Update (LSU).
- AES SSP #8 is only applicable to AES 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later or on 10.1.0.1 or later that has SSP #1-7 installed.
- **Critical Note:** AES SSP #8 **must** be installed after applying the 10.1.0.1 or later Service Pack to ensure robust security protection. Reference **PCN2139S** for additional details on the mandatory AES 10.1.0.1. Service Pack and subsequent Service Packs.
- Installation of AES SSP #8 will fail unless Service Pack 10.1.0.1 or later is installed first.
- 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.

© 2022-2024 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 "***Security Information"*** section of this PCN for updates to the rpm and RHSAs for SSP #8.

17 October 2022 – Supplement 6 of this PCN introduces **Avaya Aura® Application Enablement Services 10.1 (AES) 10.1 Security Service Pack #7.**
(**AV-AES10.1-RHEL8.4-SSP-007-01.tar.bz2; PLDS ID AES00000945)**

- AES 10.1 security updates are now provided in a Security Service Pack (SSP). There will no longer be a Linux Security Update (LSU).
- AES SSP #7 is only applicable to AES 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later or on 10.1.0.1 or later that has SSP #1-6 installed.
- **Critical Note:** AES SSP #7 **must** be installed after applying the 10.1.0.1 or later Service Pack to ensure robust security protection. Reference **PCN2139S** for additional details on the mandatory AES 10.1.0.1. Service Pack and subsequent Service Packs.
- Installation of AES SSP #7 will fail unless Service Pack 10.1.0.1 or later is installed first.
- 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.

26 September 2022 – Supplement 5 of this PCN introduces **Avaya Aura® Application Enablement Services 10.1 (AES) 10.1 Security Service Pack #6.**
(**AV-AES10.1-RHEL8.4-SSP-006-01.tar.bz2; PLDS ID AES00000930)**

- AES 10.1 security updates are now provided in a Security Service Pack (SSP). There will no longer be a Linux Security Update (LSU).
- AES SSP #6 is only applicable to AES 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later or on 10.1.0.1 or later that has SSP #1-5 installed.
- **Critical Note:** AES SSP #6 **must** be installed after applying the 10.1.0.1 or later Service Pack to ensure robust security protection. Reference **PCN2139S** for additional details on the mandatory AES 10.1.0.1. Service Pack and subsequent Service Packs.
- Installation of AES SSP #6 will fail unless Service Pack 10.1.0.1 or later is installed first.
- 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 #6.

16 August 2022 – Supplement 4 of this PCN introduces **Avaya Aura® Application Enablement Services 10.1 (AES) 10.1 Security Service Pack #5.**
(**AV-AES10.1-RHEL8.4-SSP-005-02.tar.bz2; PLDS ID AES00000927)**

- AES 10.1 security updates are now provided in a Security Service Pack (SSP). There will no longer be a Linux Security Update (LSU).
- AES SSP #5 is only applicable to AES 10.1.0.1. It can be installed directly on 10.1.0.1 or on 10.1.0.1 that has SSP #1-4 installed.
- **Critical Note:** AES SSP #5 **must** be installed after applying the 10.1.0.1 Service Pack to ensure robust security protection. Reference **PCN2139S** for additional details on the mandatory AES 10.1.0.1. Service Pack.
- Installation of AES SSP #5 will fail unless Service Pack 10.1.0.1 is installed first.

© 2022-2024 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 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 #5.

22 July 2022 – Supplement 3 of this PCN introduces **Avaya Aura® Application Enablement Services 10.1 (AES) 10.1 Security Service Pack #4.**
(**AV-AES10.1-RHEL8.4-SSP-004-01.tar.bz2; PLDS ID AES00000925)**

- AES 10.1 security updates are now provided in a Security Service Pack (SSP). There will no longer be a Linux Security Update (LSU).
- AES SSP #4 is only applicable to AES 10.1.0.1. It can be installed directly on 10.1.0.1 or on 10.1.0.1 that has SSP #1-3 installed.
- **Critical Note:** AES SSP #4 **must** be installed after applying the 10.1.0.1 Service Pack to ensure robust security protection. Reference **PCN2139S** for additional details on the mandatory AES 10.1.0.1. Service Pack.
- Installation of AES SSP #4 will fail unless Service Pack 10.1.0.1 is installed first.
- 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 #4.

21 June 2022 – Supplement 2 of this PCN introduces **Avaya Aura® Application Enablement Services 10.1 (AES) 10.1 Security Service Pack #3.**
(**AV-AES10.1-RHEL8.4-SSP-003-02.tar.bz2; PLDS ID AES00000923)**

- AES 10.1 security updates are now provided in a Security Service Pack (SSP). There will no longer be a Linux Security Update (LSU).
- AES SSP #3 is only applicable to AES 10.1.0.1. It can be installed directly on 10.1.0.1 or on 10.1.0.1 that has SSP #1 or SSP #2 installed.
- **Critical Note:** AES SSP #3 **must** be installed after applying the 10.1.0.1 Service Pack to ensure robust security protection. Reference **PCN2139S** for additional details on the mandatory AES 10.1.0.1. Service Pack.
- Installation of AES SSP #3 will fail unless Service Pack 10.1.0.1 is installed first.
- 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 #3.

16 May 2022 – Supplement 1 of this PCN introduces **Avaya Aura® Application Enablement Services 10.1 (AES) 10.1 Security Service Pack #2** and **updates to the RHSAs and rpms for SSP #1.**
(**AV-AES10.1-RHEL8.4-SSP-002-01.tar.bz2; PLDS ID AES00000916)**

- AES 10.1 security updates are now provided in a Security Service Pack (SSP). There will no longer be a Linux Security Update (LSU).
- AES SSP #2 is only applicable to AES 10.1.0.1. It can be installed directly on 10.1.0.1 or on 10.1.0.1 that has SSP #1 installed.
- **Critical Note:** AES SSP #2 **must** be installed after applying the 10.1.0.1 Service Pack to ensure

© 2022-2024 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.

robust security protection. Reference **PCN2139S** for additional details on the mandatory AES 10.1.0.1. Service Pack.

- Installation of AES SSP #2 will fail unless Service Pack 10.1.0.1 is installed first.
- 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 #2.

18 April 2022 – This PCN introduces **Avaya Aura® Application Enablement Services 10.1 (AES) 10.1 Security Service Pack #1**
(**AV-AES10.1-RHEL8.4-SSP-001-01.tar.bz2; PLDS ID AES00000909)**

- AES 10.1 security updates are now provided in a Security Service Pack (SSP). There will no longer be a Linux Security Update (LSU).
- AES SSP #1 is only applicable to AES 10.1.0.1.
- **Critical Note:** AES SSP #1 **must** be installed after applying the 10.1.0.1 Service Pack to ensure robust security protection. Reference **PCN2139S** for additional details on the mandatory AES 10.1.0.1. Service Pack.
- Installation of AES SSP #1 will fail unless Service Pack 10.1.0.1 is installed first.
- 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.

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 Application Enablement Services 10.1.x. It is not applicable to the Software Only offer. **The latest SSP must be installed** after applying the 10.1.0.1 Service Pack to ensure robust security protection.
The risk if this PCN is not installed:	The system will be exposed to the security vulnerabilities referenced in Section 1B.
Is this PCN for US customers, non-US customers, or both?	This PCN applies to both US and non-US customers.
Does applying this PCN disrupt my service	Activation of the Security Service Pack will disrupt service since it requires a full reboot of the Application Enablement Services Virtual Machine (VM) to take effect.

© 2022-2024 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.

during installation?	
Installation of this PCN is required by:	Customer or Avaya Authorized Service Provider. This upgrade is customer installable and remotely installable.
Release notes and workarounds are located:	The **Security Service Pack** resolves vulnerabilities described by Avaya Security Advisories (ASA) referenced in section 1B – Security information. **NOTE**: The Avaya Security Advisory (ASA) process is being reworked to provide more timely updates. As that process is finalized, this PCN will be updated to reflect the new process and associated ASA information The ASAs referenced in section 1B can be viewed by performing the following steps in a browser: 1. Go to http://support.avaya.com then enter your **Username** and **Password** and **LOG IN.** 2. Mouse over Search at the top of the page. 3. Type the ASA number of interest into the search field and Enter. 4. Click on the Security Advisory document link to read the Avaya Security Advisory. You can also access the ASAs by performing the following steps from a browser: 1. Go to http://support.avaya.com then enter your **Username** and **Password** and **LOG IN.** 2. Scroll to the bottom of the page and click **Community -> Avaya Security**. 3. Click on the link for the year the security advisory was published, which is part of the ASA number. 4. Page through the advisory numbers to find the link of interest. The **Avaya Aura® Application Enablement Services 10.1 Release Notes** can be obtained by performing the following steps from a browser: 1. Go to http://support.avaya.com then enter your **Username** and **Password** and select **LOG IN.** 2. Mouse over **Search Product** at the top of the page. 3. Begin to type **Application Enablement Services** and when Avaya Aura® Application Enablement Services appears as a selection below, select it. 4. Select **10.1.x** from the **Choose Release** pull down menu to the right. 5. Select **Product Documents** on the new page that is displayed. Scroll down (if necessary) and select **View All Product Documents.** 6. Under **Filters,** for category **TYPE** select **Manuals** and for category **SUB TYPE** select **Release Notes & Software Update Notes.** 7. Select the document titled **Avaya Aura® 10.1.x.x Release Notes**. Security Service Packs (SSPs) are cumulative. This means that all fixes in previous 10.1.x SSPs are included in the most recent SSP.
What materials are required to	This PCN is being issued as a customer installable PCN. The specified Application Enablement Services files are required. To obtain the update files refer to the **How do I order this PCN** section of this PCN.

© 2022-2024 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.

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

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

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

The 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 **Search Product** at the top of the page.
3. Begin to type **Application Enablement Services** and when Avaya Aura® Application Enablement Services appears as a selection below, select it.
4. Select 10.1.x from the **Choose Release** pull down menu to the right.
5. Select **Downloads** on the new page that is displayed. Scroll down (if necessary) and select **View All Downloads**.
6. Select **Avaya Aura AE Services 10.x Super Patches and Service Packs.**
7. Scroll down the page to find the download link for the required Security Service Pack. This link will take you to the PLDS system with the **Download pub ID** already entered.
8. Select the **Download** link in PLDS to begin the download.

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

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

PLDS Hints:

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

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

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

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

With this release Avaya introduces a common version on RedHat Enterprise Linux (RHEL 8.4) to its Avaya Aura platform. Common versions of RPMs are supported and consumed by the components. This results in a change to how security updates are provided for AES.

© 2022-2024 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.

Important Security Service Pack Installation Notes:

- AES 10.1 security updates are now provided in a Security Service Pack (SSP). There will no longer be a Linux Security Update (LSU).
- The SSP update process will utilize the new Common framework that utilizes a new "*av-update-os*" command for installation and a new "*av-version*" command that will show the SSP version currently running on AES.
- Installing AES 10.1 SSPs through Solution Deployment Manager (SDM). The SSP can only be installed using the Command Line Interfaces (CLI).
- Once an SSP is activated, it cannot be deactivated/removed. It is advised to have both a backup and snapshot prior to activation of the SSP.
- Security Service Packs are independent of other AES software updates activated on a server including AES Service Packs, Super Patches or Hot Fixes. None of these other software updates should be deactivated before installing a Security Service Pack.
- SSPs should NOT be installed on AES 10.1.x Software Only deployments.
- Security Service Packs are cumulative for the release they apply to. The current Security Service Pack for a release will include the fixes from all previous Security Service Packs for that release.

Execute the following instructions to apply the AES Security Service Pack
Note: root credentials required.
Examples below are for AES 10.1 SSP #1

1. Ensure that a maintenance window has been obtained as application of the SSP will result in a reboot.
2. Ensure that AES Service Pack #1 (10.1.0.1) or later is installed.
3. Download the SSP from PLDS and copy to /tmp directory on AES.
4. Perform a backup of the AES application.
5. Perform a snapshot of the AES VM. Follow instructions for performing snapshots as noted in *Deploying Avaya Aura® Application Enablement Services in Virtualized Environment.*
6. Login to the AES CLI utilizing root or sroot credentials.
7. Change directory to /tmp.
8. Ensure the MD5sum matches what is provided in the PLDS Download ID description.
9. Execute the following command to install the SSP. Note that there is NO prompt to ask if you want to proceed. Output of the installation is written to a log file under /var/log/avaya with the name of the SSP and the date/timestamp.
   # av-update-os AV-AES10.1-RHEL8.4-SSP-001-01.tar.bz2

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

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

Confirmation of successful update will be shown and the system will go for automatic reboot. After the reboot, nothing else needs to be done as the Security Service Pack will be fully activated and in

© 2022-2024 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.

use by the AES Virtual Machine. A new session will need to be opened to the CLI as the previous session will disconnect when AES reboots.

SECTION 1A – SOFTWARE SERVICE PACK INFORMATION

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

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

Examples below are for AES 10.1 SSP #1.

Using the Command Line Interface (CLI), run the command "*av-version*" on the server.

```
[root@AES-srv]# av-version
-----------------------------------
OS_VERSION: Red Hat Enterprise Linux release 8.4 (Ootpa)
AV_SSP_VERSION : 001
AV_BUILD_NUMBER : 01
```

The CLI can also be utilized to run the command "*swversion*" on the server.
The following is an example with AES Service Pack #1 and AES SSP #1 installed.

```
[root@aes101ova cust]# swversion
********************************************************************************
Application Enablement Services
********************************************************************************
Version: 10.1.0.1.0.7-0
Server Type: OTHER
Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
RTS Version:AES-10.1.0.1.0.7-0

********************************************************************************
Operating System Version: Linux 4.18.0-348.20.1.el8_5.x86_64

************* Patch Numbers Installed in this system are  *************
FP10.1.0.1.0.7 (AES 10.1.0)
AES-10.1-SSP-001
********************************************************************************
Use "swversion [-a | --all | -s]" to get a complete list of AE Services RPMS and
Patches/Updates
```

What you should do if the Service Pack installation fails?

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

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

Security Service Packs cannot be deactivated.

SECTION 1B – SECURITY INFORMATION

© 2022-2024 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.

Are there any security risks involved?	Issues described by the RHSAs listed in the next section are corrected by the Security Service Pack as noted. Security Service Packs (SSPs) include the fixes from all previous SSPs respectively for a given AES release.
Avaya Security Vulnerability Classification:	***The Avaya Security Advisory (ASA) process is being reworked to provide more timely updates. As that process is finalized, this PCN will be updated to reflect the new process and associated ASA information.***

Security Service Packs (SSPs) are cumulative.
This means that all fixes in previous 10.1.x SSPs are included in the most recent SSP.
Individual rpms and RHSAs listed per SSP below are the new ones for that SSP.

AES 10.1.x SSP #22 includes the following rpm updates:

kernel-4.18.0-513.18.1.el8_9.x86_64.rpm	kernel-tools-libs-4.18.0-513.18.1.el8_9.x86_64.rpm
kernel-core-4.18.0-513.18.1.el8_9.x86_64.rpm	oniguruma-6.8.2-2.1.el8_9.x86_64.rpm
kernel-headers-4.18.0-513.18.1.el8_9.x86_64.rpm	python3-perf-4.18.0-513.18.1.el8_9.x86_64.rpm
kernel-modules-4.18.0-513.18.1.el8_9.x86_64.rpm	python3-unbound-1.16.2-5.el8_9.2.x86_64.rpm
kernel-tools-4.18.0-513.18.1.el8_9.x86_64.rpm	unbound-libs-1.16.2-5.el8_9.2.x86_64.rpm

AES 10.1.x SSP #21 includes the following rpm updates:

avahi-0.7-21.el8_9.1.x86_64.rpm	kernel-tools-libs-4.18.0-513.9.1.el8_9.x86_64.rpm
avahi-libs-0.7-21.el8_9.1.x86_64.rpm	libsmbclient-4.18.6-2.el8_9.x86_64.rpm
kernel-4.18.0-513.9.1.el8_9.x86_64.rpm	libwbclient-4.18.6-2.el8_9.x86_64.rpm
kernel-core-4.18.0-513.9.1.el8_9.x86_64.rpm	python3-perf-4.18.0-513.9.1.el8_9.x86_64.rpm
kernel-headers-4.18.0-513.9.1.el8_9.x86_64.rpm	samba-client-libs-4.18.6-2.el8_9.x86_64.rpm
kernel-modules-4.18.0-513.9.1.el8_9.x86_64.rpm	samba-common-4.18.6-2.el8_9.noarch.rpm
kernel-tools-4.18.0-513.9.1.el8_9.x86_64.rpm	samba-common-libs-4.18.6-2.el8_9.x86_64.rpm

Security vulnerabilities resolved in AES 10.1 Security Service Pack #22
Delivered under Fix Id AES-33338.

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
oniguruma	RHSA-2024:0889	CVE-2019-13224 CVE-2019-16163 CVE-2019-19012 CVE-2019-19203 CVE-2019-19204	Moderate

© 2022-2024 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 kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	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
python3-unbound unbound-libs	RHSA-2024:0965	CVE-2023-50387 CVE-2023-50868	Important

Security vulnerabilities resolved in AES 10.1 Security Service Pack #21
Delivered under Fix Id AES-32996.

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
libsmbclient libwbclient samba-client-libs samba-common samba-common-libs	RHSA-2023:7467	CVE-2023-3961 CVE-2023-4091 CVE-2023-42669	Moderate	NA	NA
kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2023:7549	CVE-2022-45884 CVE-2022-45886 CVE-2022-45919 CVE-2023-1192 CVE-2023-2163 CVE-2023-3812 CVE-2023-5178	Important	NA	NA
avahi avahi-libs	RHSA-2023:7836	CVE-2021-3468 CVE-2023-38469 CVE-2023-38470 CVE-2023-38471 CVE-2023-38472 CVE-2023-38473	Moderate	NA	NA

AES 10.1.x SSP #20 includes the following rpm updates:

avahi-0.7-21.el8.x86_64.rpm	libX11-xcb-1.6.8-6.el8.x86_64.rpm
avahi-libs-0.7-21.el8.x86_64.rpm	linux-firmware-20230824-119.git0e048b06.el8_9.noarch.rpm
bind-export-libs-9.11.36-11.el8_9.x86_64.rpm	open-vm-tools-12.2.5-3.el8_9.1.x86_64.rpm

© 2022-2024 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-libs-9.11.36-11.el8_9.x86_64.rpm	perl-HTTP-Tiny-0.074-2.el8.noarch.rpm
bind-libs-lite-9.11.36-11.el8_9.x86_64.rpm	platform-python-3.6.8-51.el8_8.2.x86_64.rpm
bind-license-9.11.36-11.el8_9.noarch.rpm	platform-python-3.6.8-56.el8_9.x86_64.rpm
bind-utils-9.11.36-11.el8_9.x86_64.rpm	platform-python-pip-9.0.3-23.el8.noarch.rpm
binutils-2.30-119.el8_8.2.x86_64.rpm	procps-ng-3.3.15-14.el8.x86_64.rpm
c-ares-1.13.0-8.el8.x86_64.rpm	protobuf-c-1.3.0-8.el8.x86_64.rpm
c-ares-1.13.0-9.el8_9.1.x86_64.rpm	python3-bind-9.11.36-11.el8_9.noarch.rpm
cups-libs-2.2.6-54.el8_9.x86_64.rpm	python3-libs-3.6.8-51.el8_8.2.x86_64.rpm
fwupd-1.7.8-2.el8.x86_64.rpm	python3-libs-3.6.8-56.el8_9.x86_64.rpm
kernel-4.18.0-513.5.1.el8_9.x86_64.rpm	python3-perf-4.18.0-513.5.1.el8_9.x86_64.rpm
kernel-core-4.18.0-513.5.1.el8_9.x86_64.rpm	python3-pip-9.0.3-23.el8.noarch.rpm
kernel-headers-4.18.0-513.5.1.el8_9.x86_64.rpm	python3-pip-wheel-9.0.3-23.el8.noarch.rpm
kernel-modules-4.18.0-513.5.1.el8_9.x86_64.rpm	qemu-guest-agent-6.2.0-40.module+el8.9.0+20056+d9fb1ac3.1.x86_64.rpm
kernel-tools-4.18.0-513.5.1.el8_9.x86_64.rpm	samba-client-libs-4.18.6-1.el8.x86_64.rpm
kernel-tools-libs-4.18.0-513.5.1.el8_9.x86_64.rpm	samba-common-4.18.6-1.el8.noarch.rpm
libfastjson-0.99.9-2.el8.x86_64.rpm	samba-common-libs-4.18.6-1.el8.x86_64.rpm
libpq-13.11-1.el8.x86_64.rpm	shadow-utils-4.6-19.el8.x86_64.rpm
libsmbclient-4.18.6-1.el8.x86_64.rpm	sysstat-11.7.3-11.el8.x86_64.rpm
libwbclient-4.18.6-1.el8.x86_64.rpm	tpm2-tss-2.3.2-5.el8.x86_64.rpm
libX11-1.6.8-6.el8.x86_64.rpm	
libX11-common-1.6.8-6.el8.noarch.rpm	

Security vulnerabilities resolved in AES 10.1 Security Service Pack #20
Delivered under Fix Id AES-32883.

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
platform-python python3-libs	RHSA-2023:5997	CVE-2023-40217	Important	NA	NA
binutils	RHSA-2023:6236	CVE-2022-4285	Moderate	NA	NA
protobuf-c	RHSA-2023:6944	CVE-2022-48468	Moderate	NA	NA
libfastjson	RHSA-2023:6976	CVE-2020-12762	Moderate	NA	NA
qemu-guest-agent	RHSA-2023:6980	CVE-2021-3750 CVE-2023-3301	Moderate	NA	NA
sysstat	RHSA-2023:7010	CVE-2023-33204	Moderate	NA	NA
libpq	RHSA-2023:7016	CVE-2022-41862	Low	NA	NA
libX11 libX11-common libX11-xcb	RHSA-2023:7029	CVE-2023-3138	Moderate	NA	NA

© 2022-2024 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 kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	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 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	Important	NA	NA
linux-firmware	RHSA-2023:7109	CVE-2023-20569	Moderate	NA	NA
shadow-utils	RHSA-2023:7112	CVE-2023-4641	Low	NA	NA
c-ares	RHSA-2023:7116	CVE-2022-4904	Moderate	NA	NA
libsmbclient libwbclient samba-client-libs samba-common samba-common-libs	RHSA-2023:7139	CVE-2022-2127 CVE-2023-34966 CVE-2023-34967 CVE-2023-34968	Moderate	NA	NA
platform-python python3-libs	RHSA-2023:7151	CVE-2007-4559	Moderate	NA	NA
cups-libs	RHSA-2023:7165	CVE-2023-32324 CVE-2023-34241	Moderate	NA	NA

© 2022-2024 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.

tpm2-tss	RHSA-2023:7166	CVE-2023-22745	Low	NA	NA
perl-HTTP-Tiny	RHSA-2023:7174	CVE-2023-31486	Moderate	NA	NA
platform-python-pip python3-pip python3-pip-wheel	RHSA-2023:7176	CVE-2007-4559	Moderate	NA	NA
bind-export-libs bind-libs bind-libs-lite bind-license bind-utils python3-bind	RHSA-2023:7177	CVE-2022-3094	Moderate	NA	NA
procps-ng	RHSA-2023:7187	CVE-2023-4016	Low	NA	NA
fwupd	RHSA-2023:7189	CVE-2022-3287	Moderate	NA	NA
avahi avahi-libs	RHSA-2023:7190	CVE-2023-1981	Moderate	NA	NA
c-ares	RHSA-2023:7207	CVE-2020-22217 CVE-2023-31130	Moderate	NA	NA
open-vm-tools	RHSA-2023:7265	CVE-2023-34058 CVE-2023-34059	Important	NA	NA

AES 10.1.x SSP #19 includes the following rpm updates:

bind-export-libs-9.11.36-8.el8_8.2.x86_64.rpm	java-1.8.0-openjdk-1.8.0.392.b08-4.el8.x86_64.rpm
bind-libs-9.11.36-8.el8_8.2.x86_64.rpm	java-1.8.0-openjdk-devel-1.8.0.392.b08-4.el8.x86_64.rpm
bind-libs-lite-9.11.36-8.el8_8.2.x86_64.rpm	java-1.8.0-openjdk-headless-1.8.0.392.b08-4.el8.x86_64.rpm
bind-license-9.11.36-8.el8_8.2.noarch.rpm	libnghttp2-1.33.0-5.el8_8.i686.rpm
bind-utils-9.11.36-8.el8_8.2.x86_64.rpm	libnghttp2-1.33.0-5.el8_8.x86_64.rpm
glibc-2.28-225.el8_8.6.i686.rpm	libtiff-4.0.9-29.el8_8.i686.rpm
glibc-2.28-225.el8_8.6.x86_64.rpm	libtiff-4.0.9-29.el8_8.x86_64.rpm
glibc-all-langpacks-2.28-225.el8_8.6.x86_64.rpm	nginx-filesystem-1.20.1-1.module+el8.8.0+20359+9bd89172.1.noarch.rpm
glibc-common-2.28-225.el8_8.6.x86_64.rpm	nscd-2.28-225.el8_8.6.x86_64.rpm
glibc-devel-2.28-225.el8_8.6.x86_64.rpm	open-vm-tools-12.1.5-2.el8_8.3.x86_64.rpm
glibc-headers-2.28-225.el8_8.6.x86_64.rpm	python3-bind-9.11.36-8.el8_8.2.noarch.rpm
glibc-langpack-en-2.28-225.el8_8.6.x86_64.rpm	

Security vulnerabilities resolved in AES 10.1 Security Service Pack #19 Delivered under Fix Id AES-32605.

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
open-vm-tools	RHSA-2023:5312	CVE-2023-20900	Important	ASA-2023-122	High
libtiff libtiff	RHSA-2023:5353	CVE-2023-0800 CVE-2023-0801 CVE-2023-0802 CVE-2023-0803 CVE-2023-0804	Moderate	ASA-2023-138	Medium

© 2022-2024 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 glibc glibc-all-langpacks glibc-common glibc-devel glibc-headers glibc-langpack-en nscd	RHSA-2023:5455	CVE-2023-4527 CVE-2023-4806 CVE-2023-4813 CVE-2023-4911	Important	NA	NA
bind-export-libs bind-libs bind-libs-lite bind-license bind-utils python3-bind	RHSA-2023:5474	CVE-2023-3341	Important	ASA-2023-132	High
nginx-filesystem	RHSA-2023:5712	CVE-2023-44487	Moderate	NA	NA
java java java	RHSA-2023:5731	CVE-2022-40433 CVE-2023-22067 CVE-2023-22081	Moderate	NA	NA
libnghttp2 libnghttp2	RHSA-2023:5837	CVE-2023-44487	Important	NA	NA

AES 10.1.x SSP #18 includes the following rpm updates:

cups-libs-2.2.6-51.el8_8.1.x86_64.rpm	mod_http2-1.15.7-8.module+el8.8.0+18751+b4557bca.3.x86_64.rpm
dmidecode-3.3-4.el8_8.1.x86_64.rpm	mod_session-2.4.37-56.module+el8.8.0+19808+379766d6.7.x86_64.rpm
dnf-plugin-subscription-manager-1.28.36-3.el8_8.x86_64.rpm	mod_ssl-2.4.37-56.module+el8.8.0+19808+379766d6.7.x86_64.rpm
httpd-2.4.37-56.module+el8.8.0+19808+379766d6.7.x86_64.rpm	ncurses-6.1-9.20180224.el8_8.1.x86_64.rpm
httpd-filesystem-2.4.37-56.module+el8.8.0+19808+379766d6.7.noarch.rpm	ncurses-base-6.1-9.20180224.el8_8.1.noarch.rpm
httpd-tools-2.4.37-56.module+el8.8.0+19808+379766d6.7.x86_64.rpm	ncurses-libs-6.1-9.20180224.el8_8.1.x86_64.rpm
kernel-4.18.0-477.27.1.el8_8.x86_64.rpm	python3-perf-4.18.0-477.27.1.el8_8.x86_64.rpm
kernel-core-4.18.0-477.27.1.el8_8.x86_64.rpm	python3-subscription-manager-rhsm-1.28.36-3.el8_8.x86_64.rpm
kernel-headers-4.18.0-477.27.1.el8_8.x86_64.rpm	python3-syspurpose-1.28.36-3.el8_8.x86_64.rpm
kernel-modules-4.18.0-477.27.1.el8_8.x86_64.rpm	qemu-guest-agent-6.2.0-
kernel-tools-4.18.0-477.27.1.el8_8.x86_64.rpm	33.module+el8.8.0+19768+98f68f21.x86_64.rpm
kernel-tools-libs-4.18.0-477.27.1.el8_8.x86_64.rpm	subscription-manager-1.28.36-3.el8_8.x86_64.rpm
linux-firmware-20230404-117.git2e92a49f.el8_8.noarch.rpm	subscription-manager-rhsm-certificates-1.28.36-3.el8_8.x86_64.rpm

Security vulnerabilities resolved in AES 10.1 Security Service Pack #18
Delivered under Fix Id AES-32494.

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

© 2022-2024 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.

dnf-plugin-subscription-manager python3-subscription-manager-rhsm python3-syspurpose subscription-manager subscription-manager-rhsm-certificates	RHSA-2023:4706	CVE-2023-3899	Important	ASA-2023-114	High
cups-libs	RHSA-2023:4864	CVE-2023-32360	Important	ASA-2023-116	Medium
httpd httpd-filesystem httpd-tools mod_http2 mod_session mod_ssl	RHSA-2023:5050	CVE-2023-27522	Moderate	ASA-2023-115	High
kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	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	ASA-2023-119	High
linux-firmware	RHSA-2023:5245	CVE-2023-20593	Moderate	NA	NA
ncurses ncurses-base ncurses-libs	RHSA-2023:5249	CVE-2023-29491	Moderate	NA	NA
dmidecode	RHSA-2023:5252	CVE-2023-30630	Moderate	ASA-2023-118	High
qemu-guest-agent	RHSA-2023:5264	CVE-2022-40284 CVE-2023-3354	Important	NA	NA
ncurses ncurses-base ncurses-libs	RHSA-2023:5249	CVE-2023-29491	Moderate	NA	NA

AES 10.1.x SSP #17 includes the following rpm updates:

bind-export-libs-9.11.36-8.el8_8.1.x86_64.rpm	kernel-tools-libs-4.18.0-477.21.1.el8_8.x86_64.rpm
bind-libs-9.11.36-8.el8_8.1.x86_64.rpm	libcap-2.48-5.el8_8.i686.rpm
bind-libs-lite-9.11.36-8.el8_8.1.x86_64.rpm	libcap-2.48-5.el8_8.x86_64.rpm
bind-license-9.11.36-8.el8_8.1.noarch.rpm	libcurl-7.61.1-30.el8_8.3.i686.rpm
bind-utils-9.11.36-8.el8_8.1.x86_64.rpm	libcurl-7.61.1-30.el8_8.3.x86_64.rpm
curl-7.61.1-30.el8_8.3.x86_64.rpm	libsmbclient-4.17.5-3.el8_8.x86_64.rpm
dbus-1.12.8-24.el8_8.1.x86_64.rpm	libwbclient-4.17.5-3.el8_8.x86_64.rpm
dbus-common-1.12.8-24.el8_8.1.noarch.rpm	libxml2-2.9.7-16.el8_8.1.x86_64.rpm
dbus-daemon-1.12.8-24.el8_8.1.x86_64.rpm	openssh-8.0p1-19.el8_8.x86_64.rpm
dbus-libs-1.12.8-24.el8_8.1.x86_64.rpm	openssh-clients-8.0p1-19.el8_8.x86_64.rpm
dbus-tools-1.12.8-24.el8_8.1.x86_64.rpm	openssh-server-8.0p1-19.el8_8.x86_64.rpm
java-1.8.0-openjdk-1.8.0.382.b05-2.el8.x86_64.rpm	python3-bind-9.11.36-8.el8_8.1.noarch.rpm
java-1.8.0-openjdk-devel-1.8.0.382.b05-2.el8.x86_64.rpm	python3-libxml2-2.9.7-16.el8_8.1.x86_64.rpm
java-1.8.0-openjdk-headless-1.8.0.382.b05-2.el8.x86_64.rpm	python3-perf-4.18.0-477.21.1.el8_8.x86_64.rpm
kernel-4.18.0-477.21.1.el8_8.x86_64.rpm	python3-requests-2.20.0-3.el8_8.noarch.rpm
kernel-core-4.18.0-477.21.1.el8_8.x86_64.rpm	samba-client-libs-4.17.5-3.el8_8.x86_64.rpm
kernel-headers-4.18.0-477.21.1.el8_8.x86_64.rpm	samba-common-4.17.5-3.el8_8.noarch.rpm
kernel-modules-4.18.0-477.21.1.el8_8.x86_64.rpm	samba-common-libs-4.17.5-3.el8_8.x86_64.rpm
kernel-tools-4.18.0-477.21.1.el8_8.x86_64.rpm	

© 2022-2024 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 vulnerabilities resolved in AES 10.1 Security Service Pack #17
Delivered under Fix Id AES-32411.

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
bind-export-libs bind-libs bind-libs-lite bind-license bind-utils python3-bind	RHSA-2023:4102	CVE-2023-2828	Important	ASA-2023-089	High
java java java	RHSA-2023:4176	CVE-2023-22045 CVE-2023-22049	Moderate	NA	NA
libsmbclient libwbclient samba-client-libs samba-common samba-common-libs	RHSA-2023:4328	CVE-2023-3347	Moderate	NA	NA
openssh openssh-clients openssh-server	RHSA-2023:4419	CVE-2023-38408	Important	NA	NA
dbus dbus-common dbus-daemon dbus-libs dbus-tools	RHSA-2023:4498	CVE-2023-34969	Moderate	ASA-2023-099	Medium
kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2023:4517	CVE-2022-42896 CVE-2023-1281 CVE-2023-1829 CVE-2023-2124 CVE-2023-2194 CVE-2023-2235	Important	ASA-2023-095	High
python3-requests	RHSA-2023:4520	CVE-2023-32681	Moderate		
curl libcurl libcurl	RHSA-2023:4523	CVE-2023-27536 CVE-2023-28321	Moderate	ASA-2023-096	Medium
libcap libcap	RHSA-2023:4524	CVE-2023-2602 CVE-2023-2603	Moderate	NA	NA
libxml2 python3-libxml2	RHSA-2023:4529	CVE-2023-28484 CVE-2023-29469	Moderate	ASA-2023-097	Medium

AES 10.1.x SSP #16 includes the following rpm updates:

c-ares-1.13.0-6.el8_8.2.x86_64.rpm	open-vm-tools-12.1.5-2.el8_8.x86_64.rpm
kernel-4.18.0-477.15.1.el8_8.x86_64.rpm	platform-python-3.6.8-51.el8_8.1.x86_64.rpm
kernel-core-4.18.0-477.15.1.el8_8.x86_64.rpm	python3-libs-3.6.8-51.el8_8.1.x86_64.rpm
kernel-headers-4.18.0-477.15.1.el8_8.x86_64.rpm	python3-perf-4.18.0-477.15.1.el8_8.x86_64.rpm
kernel-modules-4.18.0-477.15.1.el8_8.x86_64.rpm	qemu-guest-agent-6.2.0-32.module+el8.8.0+18361+9f407f6e.x86_64.rpm
kernel-tools-4.18.0-477.15.1.el8_8.x86_64.rpm	sqlite-3.26.0-18.el8_8.x86_64.rpm
kernel-tools-libs-4.18.0-477.15.1.el8_8.x86_64.rpm	sqlite-libs-3.26.0-18.el8_8.i686.rpm
libssh-0.9.6-10.el8_8.i686.rpm	sqlite-libs-3.26.0-18.el8_8.x86_64.rpm
libssh-0.9.6-10.el8_8.x86_64.rpm	systemd-239-74.el8_8.2.x86_64.rpm
libssh-config-0.9.6-10.el8_8.noarch.rpm	systemd-libs-239-74.el8_8.2.x86_64.rpm
libtiff-4.0.9-28.el8_8.i686.rpm	systemd-pam-239-74.el8_8.2.x86_64.rpm

© 2022-2024 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-4.0.9-28.el8_8.x86_64.rpm	systemd-udev-239-74.el8_8.2.x86_64.rpm

Security vulnerabilities resolved in AES 10.1 Security Service Pack #16
Delivered under Fix Id AES-32265.

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
c-ares	RHSA-2023:3584	CVE-2023-32067	Important	ASA-2023-056	High
platform-python python3-libs	RHSA-2023:3591	CVE-2023-24329	Important	ASA-2023-080	High
qemu-guest-agent	RHSA-2023:3822	CVE-2023-2700	Moderate	ASA-2023-077	Medium
libtiff libtiff	RHSA-2023:3827	CVE-2022-48281	Moderate	ASA-2023-070	Medium
systemd systemd-libs systemd-pam systemd-udev	RHSA-2023:3837	CVE-2023-26604	Moderate	ASA-2023-063	High
libssh libssh libssh-config	RHSA-2023:3839	CVE-2023-1667 CVE-2023-2283	Moderate	ASA-2023-086	Medium
sqlite sqlite-libs sqlite-libs	RHSA-2023:3840	CVE-2020-24736	Moderate	ASA-2023-061	Medium
kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2023:3847	CVE-2023-28466	Moderate	ASA-2023-068	High
open-vm-tools	RHSA-2023:3949	CVE-2023-20867	Low	ASA-2023-073	Low

AES 10.1.x SSP #15 includes the following rpm updates:

apr-util-1.6.1-6.el8_8.1.x86_64.rpm	libtiff-4.0.9-27.el8.i686.rpm
apr-util-bdb-1.6.1-6.el8_8.1.x86_64.rpm	libtiff-4.0.9-27.el8.x86_64.rpm
apr-util-openssl-1.6.1-6.el8_8.1.x86_64.rpm	libwayland-client-1.21.0-1.el8.x86_64.rpm
bind-export-libs-9.11.36-8.el8.x86_64.rpm	libwayland-server-1.21.0-1.el8.i686.rpm
bind-libs-9.11.36-8.el8.x86_64.rpm	libwayland-server-1.21.0-1.el8.x86_64.rpm
bind-libs-lite-9.11.36-8.el8.x86_64.rpm	libwbclient-4.17.5-2.el8.x86_64.rpm
bind-license-9.11.36-8.el8.noarch.rpm	libzip-1.6.1-1.module+el8.3.0+6678+b09f589e.x86_64.rpm
bind-utils-9.11.36-8.el8.x86_64.rpm	net-snmp-5.8-27.el8.x86_64.rpm
curl-7.61.1-30.el8_8.2.x86_64.rpm	net-snmp-agent-libs-5.8-27.el8.i686.rpm
curl-7.61.1-30.el8.x86_64.rpm	net-snmp-agent-libs-5.8-27.el8.x86_64.rpm
dhcp-client-4.3.6-49.el8.x86_64.rpm	net-snmp-libs-5.8-27.el8.i686.rpm
dhcp-common-4.3.6-49.el8.noarch.rpm	net-snmp-libs-5.8-27.el8.x86_64.rpm
dhcp-libs-4.3.6-49.el8.x86_64.rpm	net-snmp-utils-5.8-27.el8.x86_64.rpm
kernel-4.18.0-477.10.1.el8_8.x86_64.rpm	php-7.4.33-1.module+el8.8.0+17865+ef7eddfa.x86_64.rpm
kernel-4.18.0-477.13.1.el8_8.x86_64.rpm	php-cli-7.4.33-1.module+el8.8.0+17865+ef7eddfa.x86_64.rpm
kernel-core-4.18.0-477.10.1.el8_8.x86_64.rpm	php-common-7.4.33-1.module+el8.8.0+17865+ef7eddfa.x86_64.rpm
kernel-core-4.18.0-477.13.1.el8_8.x86_64.rpm	php-fpm-7.4.33-1.module+el8.8.0+17865+ef7eddfa.x86_64.rpm
kernel-headers-4.18.0-477.10.1.el8_8.x86_64.rpm	php-mbstring-7.4.33-1.module+el8.8.0+17865+ef7eddfa.x86_64.rpm
kernel-headers-4.18.0-477.13.1.el8_8.x86_64.rpm	php-soap-7.4.33-1.module+el8.8.0+17865+ef7eddfa.x86_64.rpm
kernel-modules-4.18.0-477.10.1.el8_8.x86_64.rpm	php-xml-7.4.33-1.module+el8.8.0+17865+ef7eddfa.x86_64.rpm
kernel-modules-4.18.0-477.13.1.el8_8.x86_64.rpm	postgresql-jdbc-42.2.14-2.el8.noarch.rpm
kernel-tools-4.18.0-477.10.1.el8_8.x86_64.rpm	python3-bind-9.11.36-8.el8.noarch.rpm
kernel-tools-4.18.0-477.13.1.el8_8.x86_64.rpm	python3-perf-4.18.0-477.10.1.el8_8.x86_64.rpm

© 2022-2024 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-4.18.0-477.10.1.el8_8.x86_64.rpm	python3-perf-4.18.0-477.13.1.el8_8.x86_64.rpm
kernel-tools-libs-4.18.0-477.13.1.el8_8.x86_64.rpm	python3-unbound-1.16.2-5.el8.x86_64.rpm
kpartx-0.8.4-37.el8.x86_64.rpm	qemu-guest-agent-6.2.0-32.module+el8.8.0+18361+9f407f6e.x86_64.rpm
libarchive-3.3.3-5.el8.x86_64.rpm	samba-client-libs-4.17.5-2.el8.x86_64.rpm
libcurl-7.61.1-30.el8_8.2.i686.rpm	samba-common-4.17.5-2.el8.noarch.rpm
libcurl-7.61.1-30.el8_8.2.x86_64.rpm	samba-common-libs-4.17.5-2.el8.x86_64.rpm
libcurl-7.61.1-30.el8.i686.rpm	sysstat-11.7.3-9.el8.x86_64.rpm
libcurl-7.61.1-30.el8.x86_64.rpm	tzdata-2023c-1.el8.noarch.rpm
libsmbclient-4.17.5-2.el8.x86_64.rpm	unbound-libs-1.16.2-5.el8.x86_64.rpm

Security vulnerabilities resolved in AES 10.1 Security Service Pack #15
Delivered under Fix Id AES-32141.

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
tzdata	RHBA-2023:3103	NA	bugfix	NA	NA
qemu-guest-agent	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	NA	NA
python3-unbound unbound-libs	RHSA-2023:2771	CVE-2022-3204	Moderate	NA	NA
libwayland-client libwayland-server libwayland-server	RHSA-2023:2786	CVE-2021-3782	Moderate	NA	NA
sysstat	RHSA-2023:2800	CVE-2022-39377	Moderate	ASA-2023-041	High
postgresql-jdbc	RHSA-2023:2867	CVE-2022-41946	Moderate	ASA-2023-046	Medium
libtiff libtiff	RHSA-2023:2883	CVE-2022-3627 CVE-2022-3970	Moderate	NA	NA
libzip php php-cli php-common php-fpm php-mbstring php-soap php-xml	RHSA-2023:2903	CVE-2022-31628 CVE-2022-31629 CVE-2022-31630 CVE-2022-31631 CVE-2022-37454	Moderate	ASA-2023-038	High
kpartx	RHSA-2023:2948	CVE-2022-41973	Moderate	NA	NA

© 2022-2024 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 kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	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	NA	NA
curl libcurl libcurl	RHSA-2023:2963	CVE-2022-35252 CVE-2022-43552	Low	NA	NA
net-snmp net-snmp-agent-libs net-snmp-agent-libs net-snmp-libs net-snmp-libs net-snmp-utils	RHSA-2023:2969	CVE-2022-44792 CVE-2022-44793	Moderate	NA	NA
libsmbclient libwbclient samba-client-libs samba-common samba-common-libs	RHSA-2023:2987	CVE-2022-1615	Low	ASA-2023-040	Medium
dhcp-client dhcp-common dhcp-libs	RHSA-2023:3000	CVE-2022-2928 CVE-2022-2929	Moderate	NA	NA

© 2022-2024 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 bind-libs bind-libs-lite bind-license bind-utils python3-bind	RHSA-2023:3002	CVE-2022-2795	Moderate	NA	NA
libarchive	RHSA-2023:3018	CVE-2022-36227	Low	ASA-2023-047	Medium
curl libcurl libcurl	RHSA-2023:3106	CVE-2023-27535	Moderate	ASA-2023-043	Medium
apr-util apr-util-bdb apr-util-openssl	RHSA-2023:3109	CVE-2022-25147	Important	ASA-2023-048	Medium
kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2023:3349	CVE-2023-32233	Important	NA	NA

AES 10.1.x SSP #14 includes the following rpm updates:

java-1.8.0-openjdk-1.8.0.372.b07-1.el8_7.x86_64.rpm java-1.8.0-openjdk-devel-1.8.0.372.b07-1.el8_7.x86_64.rpm	java-1.8.0-openjdk-headless-1.8.0.372.b07-1.el8_7.x86_64.rpm

Security vulnerabilities resolved in AES 10.1 Security Service Pack #14
Delivered under Fix Id AES-31932.

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
java	RHSA-2023:1908	CVE-2023-21930 CVE-2023-21937 CVE-2023-21938 CVE-2023-21939 CVE-2023-21954 CVE-2023-21967 CVE-2023-21968	Important	ASA-2023-037	High

AES 10.1.x SSP #13 includes the following rpm updates:

gnutls-3.6.16-6.el8_7.i686.rpm	mod_session-2.4.37-51.module+el8.7.0+18499+2e106f0b.5.x86_64.rpm
gnutls-3.6.16-6.el8_7.x86_64.rpm	mod_ssl-2.4.37-51.module+el8.7.0+18499+2e106f0b.5.x86_64.rpm
httpd-2.4.37-51.module+el8.7.0+18499+2e106f0b.5.x86_64.rpm	nss-softokn-3.79.0-11.el8_7.x86_64.rpm
httpd-filesystem-2.4.37-51.module+el8.7.0+18499+2e106f0b.5.noarch.rpm	nss-softokn-freebl-3.79.0-11.el8_7.x86_64.rpm
httpd-tools-2.4.37-51.module+el8.7.0+18499+2e106f0b.5.x86_64.rpm	nss-sysinit-3.79.0-11.el8_7.x86_64.rpm
kernel-4.18.0-425.19.2.el8_7.x86_64.rpm	nss-util-3.79.0-11.el8_7.x86_64.rpm
kernel-core-4.18.0-425.19.2.el8_7.x86_64.rpm	openssl-1.1.1k-9.el8_7.x86_64.rpm
kernel-headers-4.18.0-425.19.2.el8_7.x86_64.rpm	openssl-libs-1.1.1k-9.el8_7.i686.rpm
kernel-modules-4.18.0-425.19.2.el8_7.x86_64.rpm	openssl-libs-1.1.1k-9.el8_7.x86_64.rpm
kernel-tools-4.18.0-425.19.2.el8_7.x86_64.rpm	python3-perf-4.18.0-425.19.2.el8_7.x86_64.rpm
kernel-tools-libs-4.18.0-425.19.2.el8_7.x86_64.rpm	tzdata-2023b-1.el8.noarch.rpm
mod_http2-1.15.7-5.module+el8.7.0+18499+2e106f0b.4.x86_64.rpm	tzdata-2023c-1.el8.noarch.rpm

© 2022-2024 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 vulnerabilities resolved in AES 10.1 Security Service Pack #13
Delivered under Fix Id AES-31779.

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
nss nss-softokn nss-softokn-freebl nss-sysinit nss-util	RHSA-2023:1252	CVE-2023-0767	Important	ASA-2023-028	High
openssl openssl-libs openssl-libs	RHSA-2023:1405	CVE-2022-4304 CVE-2022-4450 CVE-2023-0215 CVE-2023-0286	Important	ASA-2023-031	High
kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2023:1566	CVE-2022-4269 CVE-2022-4378 CVE-2023-0266 CVE-2023-0386	Important	None	None
gnutls gnutls	RHSA-2023:1569	CVE-2023-0361	Moderate	ASA-2023-033	High
httpd httpd-filesystem httpd-tools mod_http2 mod_session mod_ssl	RHSA-2023:1673	CVE-2023-25690	Important	None	None
tzdata	RHBA-2023:1491	NA	bugfix	None	None
tzdata	RHBA-2023:1534	NA	bugfix	None	None

AES 10.1.x SSP #12 includes the following rpm updates:

curl-7.61.1-25.el8_7.3.x86_64.rpm	platform-python-3.6.8-48.el8_7.1.x86_64.rpm
httpd-2.4.37-51.module+el8.7.0+18026+7b169787.1.x86_64.rpm	platform-python-setuptools-39.2.0-6.el8_7.1.noarch.rpm
httpd-filesystem-2.4.37-51.module+el8.7.0+18026+7b169787.1.noarch.rpm	python3-libs-3.6.8-48.el8_7.1.x86_64.rpm
httpd-tools-2.4.37-51.module+el8.7.0+18026+7b169787.1.x86_64.rpm	python3-perf-4.18.0-425.13.1.el8_7.x86_64.rpm
kernel-4.18.0-425.13.1.el8_7.x86_64.rpm	python3-setuptools-39.2.0-6.el8_7.1.noarch.rpm
kernel-core-4.18.0-425.13.1.el8_7.x86_64.rpm	python3-setuptools-wheel-39.2.0-6.el8_7.1.noarch.rpm
kernel-headers-4.18.0-425.13.1.el8_7.x86_64.rpm	samba-client-libs-4.16.4-4.el8_7.x86_64.rpm
kernel-modules-4.18.0-425.13.1.el8_7.x86_64.rpm	samba-common-4.16.4-4.el8_7.noarch.rpm
kernel-tools-4.18.0-425.13.1.el8_7.x86_64.rpm	samba-common-libs-4.16.4-4.el8_7.x86_64.rpm
kernel-tools-libs-4.18.0-425.13.1.el8_7.x86_64.rpm	systemd-239-68.el8_7.4.x86_64.rpm
libcurl-7.61.1-25.el8_7.3.i686.rpm	systemd-libs-239-68.el8_7.4.x86_64.rpm
libcurl-7.61.1-25.el8_7.3.x86_64.rpm	systemd-pam-239-68.el8_7.4.x86_64.rpm
libsmbclient-4.16.4-4.el8_7.x86_64.rpm	systemd-udev-239-68.el8_7.4.x86_64.rpm
libwbclient-4.16.4-4.el8_7.x86_64.rpm	tar-1.30-6.el8_7.1.x86_64.rpm
mod_http2-1.15.7-5.module+el8.6.0+13996+01710940.x86_64.rpm	

© 2022-2024 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.

mod_session-2.4.37 51.module+el8.7.0+18026+7b169787.1.x86_64.rpm mod_ssl-2.4.37-51.module+el8.7.0+18026+7b169787.1.x86_64.rpm	

Security vulnerabilities resolved in AES 10.1 Security Service Pack #12
Delivered under Fix Id AES-31530.

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2023:0832	CVE-2022-2873 CVE-2022-41222 CVE-2022-43945	Important	None	None
platform-python python3-libs	RHSA-2023:0833	CVE-2020-10735 CVE-2021-28861 CVE-2022-45061	Moderate	None	None
platform-python-setuptools python3-setuptools python3-setuptools-wheel	RHSA-2023:0835	CVE-2022-40897	Moderate	ASA-2023-023	Medium
systemd systemd-libs systemd-pam systemd-udev	RHSA-2023:0837	CVE-2022-4415	Moderate	None	None
libsmbclient libwbclient samba-client-libs samba-common samba-common-libs	RHSA-2023:0838	CVE-2022-38023	Important	ASA-2023-025	High
tar	RHSA-2023:0842	CVE-2022-48303	Moderate	ASA-2023-024	High
httpd httpd-filesystem httpd-tools mod_http2 mod_session mod_ssl	RHSA-2023:0852	CVE-2006-20001 CVE-2022-36760 CVE-2022-37436	Moderate	ASA-2023-022	Low
curl libcurl libcurl	RHSA-2023:1140	CVE-2023-23916	Moderate	None	None

© 2022-2024 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.

AES 10.1.x SSP #11 includes the following rpm updates:

dbus-1.12.8-23.el8_7.1.x86_64.rpm	libksba-1.3.5-9.el8_7.x86_64.rpm
dbus-common-1.12.8-23.el8_7.1.noarch.rpm	kernel-tools-4.18.0-425.10.1.el8_7.x86_64.rpm
dbus-daemon-1.12.8-23.el8_7.1.x86_64.rpm	kernel-tools-libs-4.18.0-425.10.1.el8_7.x86_64.rpm
dbus-libs-1.12.8-23.el8_7.1.x86_64.rpm	libtasn1-4.13-4.el8_7.i686.rpm
dbus-tools-1.12.8-23.el8_7.1.x86_64.rpm	libtasn1-4.13-4.el8_7.x86_64.rpm
expat-2.2.5-10.el8_7.1.i686.rpm	libtiff-4.0.9-26.el8_7.i686.rpm
expat-2.2.5-10.el8_7.1.x86_64.rpm	libtiff-4.0.9-26.el8_7.x86_64.rpm
grub2-common-2.02-142.el8_7.1.noarch.rpm	libxml2-2.9.7-15.el8_7.1.x86_64.rpm
grub2-efi-x64-2.02-142.el8_7.1.x86_64.rpm	python3-libxml2-2.9.7-15.el8_7.1.x86_64.rpm
grub2-tools-2.02-142.el8_7.1.x86_64.rpm	python3-perf-4.18.0-425.10.1.el8_7.x86_64.rpm
grub2-tools-extra-2.02-142.el8_7.1.x86_64.rpm	qemu-guest-agent-6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64.rpm
grub2-tools-minimal-2.02-142.el8_7.1.x86_64.rpm	sqlite-3.26.0-17.el8_7.x86_64.rpm
java-1.8.0-openjdk-1.8.0.362.b09-2.el8_7.x86_64.rpm	sqlite-libs-3.26.0-17.el8_7.i686.rpm
java-1.8.0-openjdk-devel-1.8.0.362.b09-2.el8_7.x86_64.rpm	sqlite-libs-3.26.0-17.el8_7.x86_64.rpm
java-1.8.0-openjdk-headless-1.8.0.362.b09-2.el8_7.x86_64.rpm	sudo-1.8.29-8.el8_7.1.x86_64.rpm
kernel-4.18.0-425.10.1.el8_7.x86_64.rpm	systemd-239-68.el8_7.1.x86_64.rpm
kernel-core-4.18.0-425.10.1.el8_7.x86_64.rpm	systemd-libs-239-68.el8_7.1.x86_64.rpm
kernel-headers-4.18.0-425.10.1.el8_7.x86_64.rpm	systemd-pam-239-68.el8_7.1.x86_64.rpm
kernel-modules-4.18.0-425.10.1.el8_7.x86_64.rpm	systemd-udev-239-68.el8_7.1.x86_64.rpm

Security vulnerabilities resolved in AES 10.1 Security Service Pack #11
Delivered under Fix Id AES-31460.

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
grub2-common grub2-efi-x64 grub2-tools grub2-tools-extra grub2-tools-minimal	RHSA-2023:0049	CVE-2022-2601 CVE-2022-3775	Moderate	ASA-2023-002	Medium
libtiff libtiff	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	ASA-2023-005	Medium
dbus dbus-common dbus-daemon dbus-libs dbus-tools	RHSA-2023:0096	CVE-2022-42010 CVE-2022-42011 CVE-2022-42012	Moderate	None	None
qemu-guest-agent	RHSA-2023:0099	CVE-2022-4144	Moderate	ASA-2023-021	Medium
systemd systemd-libs systemd-pam systemd-udev	RHSA-2023:0100	CVE-2022-3821	Moderate	ASA-2023-006	Medium

© 2022-2024 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 kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2023:0101	CVE-2022-2964 CVE-2022-4139	Important	ASA-2023-004	High
expat expat	RHSA-2023:0103	CVE-2022-43680	Moderate	ASA-2023-008	High
sqlite sqlite-libs sqlite-libs	RHSA-2023:0110	CVE-2022-35737	Moderate	ASA-2023-009	Medium
libtasn1 libtasn1	RHSA-2023:0116	CVE-2021-46848	Moderate	ASA-2023-019	Medium
libxml2 python3-libxml2	RHSA-2023:0173	CVE-2022-40303 CVE-2022-40304	Moderate	ASA-2023-007	High
java java java	RHSA-2023:0208	CVE-2023-21830 CVE-2023-21843	Moderate	ASA-2023-016	Medium
sudo	RHSA-2023:0284	CVE-2023-22809	Important	ASA-2023-010	High
libksba	RHSA-2023:0625	CVE-2022-47629	Important	ASA-2023-017	High

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

AES 10.1.x SSP #10 includes the following rpm updates:

tzdata-2022d-1.el8.noarch.rpm tzdata-2022e-1.el8.noarch.rpm	tzdata-2022f-1.el8.noarch.rpm tzdata-2022g-1.el8.noarch.rpm

Security vulnerabilities resolved in AES 10.1 Security Service Pack #10
Delivered under Fix Id AES-31196.

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
tzdata	RHBA-2022:6827	NA	bugfix	NA	NA
tzdata	RHBA-2022:7067	NA	bugfix	NA	NA
tzdata	RHBA-2022:7404	NA	bugfix	NA	NA
tzdata	RHBA-2022:7824	NA	bugfix	NA	NA
tzdata	RHBA-2022:7884	NA	bugfix	NA	NA
tzdata	RHBA-2022:8785	NA	bugfix	NA	NA

AES 10.1.x SSP #9 includes the following rpm updates:

bind-export-libs-9.11.36-5.el8.x86_64.rpm bind-libs-9.11.36-5.el8.x86_64.rpm bind-libs-lite-9.11.36-5.el8.x86_64.rpm	libcom_err-1.45.6-5.el8.i686.rpm libcom_err-1.45.6-5.el8.x86_64.rpm libcom_err-devel-1.45.6-5.el8.x86_64.rpm

© 2022-2024 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-license-9.11.36-5.el8.noarch.rpm	libkadm5-1.18.2-22.el8_7.x86_64.rpm
bind-utils-9.11.36-5.el8.x86_64.rpm	libldb-2.5.2-2.el8.x86_64.rpm
e2fsprogs-1.45.6-5.el8.x86_64.rpm	libss-1.45.6-5.el8.x86_64.rpm
e2fsprogs-devel-1.45.6-5.el8.x86_64.rpm	libtiff-4.0.9-23.el8.i686.rpm
e2fsprogs-libs-1.45.6-5.el8.x86_64.rpm	libtiff-4.0.9-23.el8.x86_64.rpm
freetype-2.9.1-9.el8.x86_64.rpm	libxml2-2.9.7-15.el8.x86_64.rpm
fribidi-1.0.4-9.el8.x86_64.rpm	libzip-1.6.1-1.module+el8.3.0+6678+b09f589e.x86_64.rpm
gdisk-1.0.3-11.el8.x86_64.rpm	mod_http2-1.15.7-5.module+el8.6.0+13996+01710940.x86_64.rpm
glib2-2.56.4-159.el8.i686.rpm	mod_session-2.4.37-51.module+el8.7.0+16050+02173b8e.x86_64.rpm
glib2-2.56.4-159.el8.x86_64.rpm	mod_ssl-2.4.37-51.module+el8.7.0+16050+02173b8e.x86_64.rpm
httpd-2.4.37-51.module+el8.7.0+16050+02173b8e.x86_64.rpm	php-7.4.30-1.module+el8.7.0+15886+8e29b882.x86_64.rpm
httpd-filesystem-2.4.37-51.module+el8.7.0+16050+02173b8e.noarch.rpm	php-cli-7.4.30-1.module+el8.7.0+15886+8e29b882.x86_64.rpm
	php-common-7.4.30-1.module+el8.7.0+15886+8e29b882.x86_64.rpm
httpd-tools-2.4.37-51.module+el8.7.0+16050+02173b8e.x86_64.rpm	php-fpm-7.4.30-1.module+el8.7.0+15886+8e29b882.x86_64.rpm
	php-mbstring-7.4.30-1.module+el8.7.0+15886+8e29b882.x86_64.rpm
kernel-4.18.0-425.3.1.el8.x86_64.rpm	php-soap-7.4.30-1.module+el8.7.0+15886+8e29b882.x86_64.rpm
kernel-core-4.18.0-425.3.1.el8.x86_64.rpm	php-xml-7.4.30-1.module+el8.7.0+15886+8e29b882.x86_64.rpm
kernel-headers-4.18.0-425.3.1.el8.x86_64.rpm	python3-bind-9.11.36-5.el8.noarch.rpm
kernel-modules-4.18.0-425.3.1.el8.x86_64.rpm	python3-libxml2-2.9.7-15.el8.x86_64.rpm
kernel-tools-4.18.0-425.3.1.el8.x86_64.rpm	python3-perf-4.18.0-425.3.1.el8.x86_64.rpm
kernel-tools-libs-4.18.0-425.3.1.el8.x86_64.rpm	python3-unbound-1.16.2-2.el8.x86_64.rpm
kpartx-0.8.4-28.el8_7.1.x86_64.rpm	qemu-guest-agent-6.2.0-20.module+el8.7.0+16689+53d59bc2.1.x86_64.rpm
krb5-libs-1.18.2-22.el8_7.i686.rpm	qt5-srpm-macros-5.15.3-1.el8.noarch.rpm
krb5-libs-1.18.2-22.el8_7.x86_64.rpm	rsync-3.1.3-19.el8.x86_64.rpm
krb5-workstation-1.18.2-22.el8_7.x86_64.rpm	unbound-libs-1.16.2-2.el8.x86_64.rpm

Security vulnerabilities resolved in AES 10.1 Security Service Pack #9
Delivered under Fix Id AES-31081

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
qemu-guest-agent	RHSA-2022:7472	CVE-2021-3507 CVE-2022-0897 CVE-2022-2211 CVE-2022-23645	Low	ASA-2022-147	Medium
qt5-srpm-macros	RHSA-2022:7482	CVE-2022-25255	Moderate	None	None
fribidi	RHSA-2022:7514	CVE-2022-25308 CVE-2022-25309 CVE-2022-25310	Moderate	None	None
libtiff libtiff	RHSA-2022:7585	CVE-2022-0561 CVE-2022-0562 CVE-2022-0865 CVE-2022-0891 CVE-2022-0908 CVE-2022-0909 CVE-2022-0924 CVE-2022-1355 CVE-2022-22844	Moderate	ASA-2022-151	High
python3-unbound unbound-libs	RHSA-2022:7622	CVE-2022-30698 CVE-2022-30699	Moderate	ASA-2022-150	Medium
libzip php php-cli php-common php-fpm php-mbstring php-soap php-xml	RHSA-2022:7628	CVE-2021-21707 CVE-2021-21708 CVE-2021-32610	Moderate	ASA-2022-143	Critical

© 2022-2024 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.

httpd httpd-filesystem httpd-tools mod_http2 mod_session mod_ssl	RHSA-2022:7647	CVE-2022-22719 CVE-2022-22721 CVE-2022-23943 CVE-2022-26377 CVE-2022-28614 CVE-2022-28615 CVE-2022-29404 CVE-2022-30522 CVE-2022-30556 CVE-2022-31813	Moderate	ASA-2022-145	High
kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	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	ASA-2022-144	High
gdisk	RHSA-2022:7700	CVE-2020-0256 CVE-2021-0308	Moderate	ASA-2022-142	Medium
glib2 glib2	RHSA-2022:7704	CVE-2022-22624 CVE-2022-22628 CVE-2022-22629 CVE-2022-22662 CVE-2022-26700 CVE-2022-26709 CVE-2022-26710 CVE-2022-26716 CVE-2022-26717 CVE-2022-26719 CVE-2022-30293	Moderate	ASA-2022-146	High
libxml2 python3-libxml2	RHSA-2022:7715	CVE-2016-3709	Moderate	ASA-2022-138	Medium
e2fsprogs e2fsprogs-devel e2fsprogs-libs libcom_err libcom_err libcom_err-devel libss	RHSA-2022:7720	CVE-2022-1304	Moderate	ASA-2022-141	High
libldb	RHSA-2022:7730	CVE-2022-32746	Moderate	None	None

© 2022-2024 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.

freetype	RHSA-2022:7745	CVE-2022-27404 CVE-2022-27405 CVE-2022-27406	Moderate	None	None
bind-export-libs bind-libs bind-libs-lite bind-license bind-utils python3-bind	RHSA-2022:7790	CVE-2021-25220	Moderate	ASA-2022-155	Medium
rsync	RHSA-2022:7793	CVE-2022-37434	Moderate		
kpartx	RHSA-2022:7928	CVE-2022-3787	Important	ASA-2022-149	High
krb5-libs krb5-libs krb5-workstation libkadm5	RHSA-2022:8638	CVE-2022-42898	Important	None	None

AES 10.1.x SSP #8 includes the following rpm updates:

bind-export-libs-9.11.36-3.el8_6.1.x86_64.rpm	kernel-tools-4.18.0-372.32.1.el8_6.x86_64.rpm
bind-libs-9.11.36-3.el8_6.1.x86_64.rpm	kernel-tools-libs-4.18.0-372.32.1.el8_6.x86_64.rpm
bind-libs-lite-9.11.36-3.el8_6.1.x86_64.rpm	kpartx-0.8.4-22.el8_6.2.x86_64.rpm
bind-license-9.11.36-3.el8_6.1.noarch.rpm	libksba-1.3.5-8.el8_6.x86_64.rpm
bind-utils-9.11.36-3.el8_6.1.x86_64.rpm	libsmbclient-4.15.5-10.el8_6.x86_64.rpm
expat-2.2.5-8.el8_6.3.i686.rpm	libwbclient-4.15.5-10.el8_6.x86_64.rpm
expat-2.2.5-8.el8_6.3.x86_64.rpm	python3-bind-9.11.36-3.el8_6.1.noarch.rpm
gnutls-3.6.16-5.el8_6.i686.rpm	python3-perf-4.18.0-372.32.1.el8_6.x86_64.rpm
gnutls-3.6.16-5.el8_6.x86_64.rpm	samba-client-libs-4.15.5-10.el8_6.x86_64.rpm
java-1.8.0-openjdk-1.8.0.352.b08-2.el8_6.x86_64.rpm	samba-common-4.15.5-10.el8_6.noarch.rpm
java-1.8.0-openjdk-devel-1.8.0.352.b08-2.el8_6.x86_64.rpm	samba-common-libs-4.15.5-10.el8_6.x86_64.rpm
java-1.8.0-openjdk-headless-1.8.0.352.b08-2.el8_6.x86_64.rpm	sqlite-3.26.0-16.el8_6.x86_64.rpm
kernel-4.18.0-372.32.1.el8_6.x86_64.rpm	sqlite-libs-3.26.0-16.el8_6.i686.rpm
kernel-core-4.18.0-372.32.1.el8_6.x86_64.rpm	sqlite-libs-3.26.0-16.el8_6.x86_64.rpm
kernel-headers-4.18.0-372.32.1.el8_6.x86_64.rpm	zlib-1.2.11-19.el8_6.i686.rpm
kernel-modules-4.18.0-372.32.1.el8_6.x86_64.rpm	zlib-1.2.11-19.el8_6.x86_64.rpm

Security vulnerabilities resolved in AES 10.1 Security Service Pack #8
Delivered under Fix Id AES-30695

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
bind-export-libs bind-libs bind-libs-lite bind-license bind-utils python3-bind	RHSA-2022:6778	CVE-2022-38177 CVE-2022-38178	Important	None	None
expat expat	RHSA-2022:6878	CVE-2022-40674	Important	None	None
java java java	RHSA-2022:7006	CVE-2022-21619 CVE-2022-21624 CVE-2022-21626 CVE-2022-21628	Moderate	None	None
libksba	RHSA-2022:7089	CVE-2022-3515	Important	None	None
gnutls	RHSA-2022:7105	CVE-2022-2509	Moderate	None	None

© 2022-2024 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	RHSA-2022:7106	CVE-2022-37434	Moderate	ASA-2022-129	Critical
sqlite sqlite-libs	RHSA-2022:7108	CVE-2020-35525 CVE-2020-35527	Moderate	ASA-2022-130	High
kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2022:7110	CVE-2022-0494 CVE-2022-1353 CVE-2022-23825 CVE-2022-2588 CVE-2022-29901	Important	ASA-2022-132	High
libsmbclient libwbclient samba-client-libs samba-common samba-common-libs	RHSA-2022:7111	CVE-2022-32742	Moderate	None	None
kpartx	RHSA-2022:7192	CVE-2022-41974	Important	ASA-2022-128	High

AES 10.1.x SSP #7 includes the following rpm updates:

curl-7.61.1-22.el8_6.4.x86_64.rpm	php-common-7.4.19-4.module+el8.6.0+16316+906f6c6d.x86_64.rpm
gnupg2-2.2.20-3.el8_6.x86_64.rpm	php-fpm-7.4.19-4.module+el8.6.0+16316+906f6c6d.x86_64.rpm
gnupg2-smime-2.2.20-3.el8_6.x86_64.rpm	php-mbstring-7.4.19-4.module+el8.6.0+16316+906f6c6d.x86_64.rpm
kernel-4.18.0-372.26.1.el8_6.x86_64.rpm	php-soap-7.4.19-4.module+el8.6.0+16316+906f6c6d.x86_64.rpm
kernel-core-4.18.0-372.26.1.el8_6.x86_64.rpm	php-xml-7.4.19-4.module+el8.6.0+16316+906f6c6d.x86_64.rpm
kernel-headers-4.18.0-372.26.1.el8_6.x86_64.rpm	platform-python-3.6.8-47.el8_6.x86_64.rpm
kernel-modules-4.18.0-372.26.1.el8_6.x86_64.rpm	python3-libs-3.6.8-47.el8_6.x86_64.rpm
kernel-tools-4.18.0-372.26.1.el8_6.x86_64.rpm	python3-perf-4.18.0-372.26.1.el8_6.x86_64.rpm
kernel-tools-libs-4.18.0-372.26.1.el8_6.x86_64.rpm	rsync-3.1.3-14.el8_6.3.x86_64.rpm
libcurl-7.61.1-22.el8_6.4.i686.rpm	systemd-239-58.el8_6.4.x86_64.rpm
libcurl-7.61.1-22.el8_6.4.x86_64.rpm	systemd-libs-239-58.el8_6.4.x86_64.rpm
libzip-1.6.1-1.module+el8.3.0+6678+b09f589e.x86_64.rpm	systemd-pam-239-58.el8_6.4.x86_64.rpm
open-vm-tools-11.3.5-1.el8_6.1.x86_64.rpm	systemd-udev-239-58.el8_6.4.x86_64.rpm
php-7.4.19-4.module+el8.6.0+16316+906f6c6d.x86_64.rpm	tzdata-2022c-1.el8.noarch.rpm
php-cli-7.4.19-4.module+el8.6.0+16316+906f6c6d.x86_64.rpm	

Security vulnerabilities resolved in AES 10.1 Security Service Pack #7
Delivered under Fix Id AES-30528

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
libzip php php-cli php-common php-fpm php-mbstring php-soap php-xml	RHSA-2022:6158	CVE-2022-31625	Moderate	ASA-2022-117	High

© 2022-2024 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.

curl libcurl	RHSA-2022:6159	CVE-2022-32206 CVE-2022-32208	Moderate		
rsync	RHSA-2022:6180	CVE-2022-29154	Important	ASA-2022-116	High
systemd systemd-libs systemd-pam systemd-udev	RHSA-2022:6206	CVE-2022-2526	Important	ASA-2022-118	High
open-vm-tools	RHSA-2022:6357	CVE-2022-31676	Important	None	None
platform-python python3-libs	RHSA-2022:6457	CVE-2015-20107 CVE-2022-0391	Moderate	None	None
kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2022:6460	CVE-2022-21123 CVE-2022-21125 CVE-2022-21166	Moderate	None	None
gnupg2 gnupg2-smime	RHSA-2022:6463	CVE-2022-34903	Moderate	ASA-2022-121	Medium
libzip php php-cli php-common php-fpm php-mbstring php-soap php-xml	RHSA-2022:6542	CVE-2020-28948 CVE-2020-28949 CVE-2020-36193	Moderate	ASA-2022-122	High
tzdata	RHBA-2021:3790 RHBA-2021:4003 RHBA-2021:4543 RHBA-2022:1032 RHBA-2022:6138	NA	Bug Fix	NA	NA

AES 10.1.x SSP #6 includes the following rpm updates:

kernel-4.18.0-372.19.1.el8_6.x86_64.rpm	openssl-libs-1.1.1k-7.el8_6.i686.rpm
kernel-core-4.18.0-372.19.1.el8_6.x86_64.rpm	openssl-libs-1.1.1k-7.el8_6.x86_64.rpm
kernel-headers-4.18.0-372.19.1.el8_6.x86_64.rpm	pcre2-10.32-3.el8_6.i686.rpm
kernel-modules-4.18.0-372.19.1.el8_6.x86_64.rpm	pcre2-10.32-3.el8_6.x86_64.rpm
kernel-tools-4.18.0-372.19.1.el8_6.x86_64.rpm	python3-perf-4.18.0-372.19.1.el8_6.x86_64.rpm
kernel-tools-libs-4.18.0-372.19.1.el8_6.x86_64.rpm	qemu-guest-agent-6.2.0-11.module+el8.6.0+15668+464a1f31.2.x86_64.rpm
openssl-1.1.1k-7.el8_6.x86_64.rpm	vim-minimal-8.0.1763-19.el8_6.4.x86_64.rpm

Security vulnerabilities resolved in AES 10.1 Security Service Pack #6
Delivered under Fix Id AES-30308

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

© 2022-2024 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.

pcre2 pcre2	RHSA-2022:5809	CVE-2022-1586	Moderate	ASA-2022-112	High
vim-minimal	RHSA-2022:5813	CVE-2022-1785 CVE-2022-1897 CVE-2022-1927	Moderate	ASA-2022-110	Critical
openssl openssl-libs openssl-libs	RHSA-2022:5818	CVE-2022-1292 CVE-2022-2068 CVE-2022-2097	Moderate	ASA-2022-111	Medium
kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2022:5819	CVE-2022-1012 CVE-2022-32250	Important	None	None
qemu-guest-agent	RHSA-2022:5821	CVE-2021-4206 CVE-2021-4207 CVE-2022-26353 CVE-2022-26354	Moderate	None	None

AES 10.1.x SSP #5 includes the following rpm updates:

compat-openssl10-1.0.2o-4.el8_6.x86_64.rpm	libgcrypt-1.8.5-7.el8_6.x86_64.rpm
curl-7.61.1-22.el8_6.3.x86_64.rpm	libxml2-2.9.7-13.el8_6.1.x86_64.rpm
expat-2.2.5-8.el8_6.2.i686.rpm	libzip-1.6.1-1.module+el8.3.0+6678+b09f589e.x86_64.rpm
expat-2.2.5-8.el8_6.2.x86_64.rpm	mod_http2-1.15.7-5.module+el8.6.0+13996+01710940.x86_64.rpm
httpd-2.4.37-47.module+el8.6.0+15654+427eba2e.2.x86_64.rpm	mod_session-2.4.37-47.module+el8.6.0+15654+427eba2e.2.x86_64.rpm
httpd-filesystem-2.4.37-47.module+el8.6.0+15654+427eba2e.2.noarch.rpm	mod_ssl-2.4.37-47.module+el8.6.0+15654+427eba2e.2.x86_64.rpm
httpd-tools-2.4.37-47.module+el8.6.0+15654+427eba2e.2.x86_64.rpm	php-7.4.19-3.module+el8.6.0+15726+994cde98.x86_64.rpm
java-1.8.0-openjdk-1.8.0.342.b07-2.el8_6.x86_64.rpm	php-cli-7.4.19-3.module+el8.6.0+15726+994cde98.x86_64.rpm
java-1.8.0-openjdk-devel-1.8.0.342.b07-2.el8_6.x86_64.rpm	php-common-7.4.19-3.module+el8.6.0+15726+994cde98.x86_64.rpm
java-1.8.0-openjdk-headless-1.8.0.342.b07-2.el8_6.x86_64.rpm	php-fpm-7.4.19-3.module+el8.6.0+15726+994cde98.x86_64.rpm
kernel-4.18.0-372.16.1.el8_6.x86_64.rpm	php-mbstring-7.4.19-3.module+el8.6.0+15726+994cde98.x86_64.rpm
kernel-core-4.18.0-372.16.1.el8_6.x86_64.rpm	php-soap-7.4.19-3.module+el8.6.0+15726+994cde98.x86_64.rpm
kernel-headers-4.18.0-372.16.1.el8_6.x86_64.rpm	php-xml-7.4.19-3.module+el8.6.0+15726+994cde98.x86_64.rpm
kernel-modules-4.18.0-372.16.1.el8_6.x86_64.rpm	python3-libxml2-2.9.7-13.el8_6.1.x86_64.rpm
kernel-tools-4.18.0-372.16.1.el8_6.x86_64.rpm	python3-perf-4.18.0-372.16.1.el8_6.x86_64.rpm
kernel-tools-libs-4.18.0-372.16.1.el8_6.x86_64.rpm	vim-minimal-8.0.1763-19.el8_6.2.x86_64.rpm
libcurl-7.61.1-22.el8_6.3.i686.rpm	
libcurl-7.61.1-22.el8_6.3.x86_64.rpm	

Security vulnerabilities resolved in AES 10.1 Security Service Pack #5
Delivered under Fix Id AES-30078

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

© 2022-2024 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.

httpd httpd-filesystem httpd-tools mod_http2 mod_session mod_ssl	RHSA-2022:5163	CVE-2020-13950	Low	ASA-2022-083	High
libgcrypt	RHSA-2022:5311	CVE-2021-40528	Moderate	ASA-2022-103	Medium
curl libcurl	RHSA-2022:5313	CVE-2022-22576 CVE-2022-27774 CVE-2022-27776 CVE-2022-27782	Moderate	None	None
expat expat	RHSA-2022:5314	CVE-2022-25313 CVE-2022-25314	Moderate	ASA-2022-102	High
kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2022:5316	CVE-2020-28915 CVE-2022-27666	Important	ASA-2022-101	High
libxml2 python3-libxml2	RHSA-2022:5317	CVE-2022-29824	Moderate	ASA-2022-100	High
vim-minimal	RHSA-2022:5319	CVE-2022-1621 CVE-2022-1629	Moderate	ASA-2022-104	High
compat-openssl10	RHSA-2022:5326	CVE-2022-0778	Low	ASA-2022-099	High
libzip php php-cli php-common php-fpm php-mbstring php-soap php-xml	RHSA-2022:5467	CVE-2022-31626	Important	None	None
kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2022:5564	CVE-2022-1729	Important	ASA-2022-109	Medium
java java java	RHSA-2022:5696	CVE-2022-21540 CVE-2022-21541 CVE-2022-34169	Important	ASA-2022-107	High

AES 10.1.x SSP #4 includes the following rpm updates:

apache-commons-logging-1.2-13.module+el8+2452+b359bfcd.noarch.rpm cups-libs-2.2.6-45.el8_6.2.x86_64.rpm grub2-common-2.02-123.el8_6.8.noarch.rpm grub2-efi-x64-2.02-123.el8_6.8.x86_64.rpm grub2-tools-2.02-123.el8_6.8.x86_64.rpm	php-fpm-7.4.19-1.module+el8.5.0+11143+cc873159.x86_64.rpm php-fpm-7.4.19-2.module+el8.6.0+13953+0a59ce9f.x86_64.rpm php-mbstring-7.4.19-1.module+el8.5.0+11143+cc873159.x86_64.rpm php-mbstring-7.4.19-2.module+el8.6.0+13953+0a59ce9f.x86_64.rpm php-soap-7.4.19-1.module+el8.5.0+11143+cc873159.x86_64.rpm

© 2022-2024 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-2.02-123.el8_6.8.x86_64.rpm grub2-tools-minimal-2.02-123.el8_6.8.x86_64.rpm libzip-1.6.1-1.module+el8.3.0+6678+b09f589e.x86_64.rpm mokutil-0.3.0-11.el8_6.1.x86_64.rpm nginx-filesystem-1.20.1-1.module+el8.5.0+13723+ab304644.noarch.rpm php-7.4.19-1.module+el8.5.0+11143+cc873159.x86_64.rpm php-7.4.19-2.module+el8.6.0+13953+0a59ce9f.x86_64.rpm php-cli-7.4.19-1.module+el8.5.0+11143+cc873159.x86_64.rpm php-cli-7.4.19-2.module+el8.6.0+13953+0a59ce9f.x86_64.rpm php-common-7.4.19-1.module+el8.5.0+11143+cc873159.x86_64.rpm php-common-7.4.19-2.module+el8.6.0+13953+0a59ce9f.x86_64.rpm	php-soap-7.4.19-2.module+el8.6.0+13953+0a59ce9f.x86_64.rpm php-xml-7.4.19-1.module+el8.5.0+11143+cc873159.x86_64.rpm php-xml-7.4.19-2.module+el8.6.0+13953+0a59ce9f.x86_64.rpm rsyslog-8.2102.0-7.el8_6.1.x86_64.rpm rsyslog-gnutls-8.2102.0-7.el8_6.1.x86_64.rpm shim-x64-15.6-1.el8.x86_64.rpm xz-5.2.4-4.el8_6.x86_64.rpm xz-libs-5.2.4-4.el8_6.i686.rpm xz-libs-5.2.4-4.el8_6.x86_64.rpm

Security vulnerabilities resolved in AES 10.1 Security Service Pack #4
Delivered under Fix Id AES-29913

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
libzip php php-cli php-common php-fpm php-mbstring php-soap php-xml	RHSA-2021:4213	CVE-2020-7068 CVE-2020-7069 CVE-2020-7070 CVE-2020-7071 CVE-2021-21702	Moderate	None	None
nginx-filesystem	RHSA-2022:0323	CVE-2021-23017	Important	ASA-2022-013	High
libzip php php-cli php-common php-fpm php-mbstring php-soap php-xml	RHSA-2022:1935	CVE-2021-21703 CVE-2021-21705	Moderate	ASA-2022-047	Medium
apache-commons-logging	RHSA-2022:4798	CVE-2022-29599	Important	ASA-2022-077	Critical
rsyslog rsyslog-gnutls	RHSA-2022:4799	CVE-2022-24903	Important	ASA-2022-078	High
xz xz-libs	RHSA-2022:4991	CVE-2022-1271	Important	ASA-2022-080	High
cups-libs	RHSA-2022:5056	CVE-2022-26691	Important	ASA-2022-091	High
grub2-common grub2-efi-x64 grub2-tools grub2-tools-extra grub2-tools-minimal mokutil shim-x64	RHSA-2022:5095	CVE-2021-3695 CVE-2021-3696 CVE-2021-3697 CVE-2022-28733 CVE-2022-28734 CVE-2022-28735 CVE-2022-28736 CVE-2022-28737	Important	ASA-2022-098	High

© 2022-2024 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.

AES 10.1.x SSP #3 includes the following rpm updates:

apache-commons-logging-1.2-13.module+el8+2452+b359bfcd.noarch.rpm	libssh-0.9.6-3.el8.i686.rpm
bind-export-libs-9.11.36-3.el8.x86_64.rpm	libssh-0.9.6-3.el8.x86_64.rpm
bind-libs-9.11.36-3.el8.x86_64.rpm	libssh-config-0.9.6-3.el8.noarch.rpm
bind-libs-lite-9.11.36-3.el8.x86_64.rpm	libtiff-4.0.9-21.el8.i686.rpm
bind-license-9.11.36-3.el8.noarch.rpm	libtiff-4.0.9-21.el8.x86_64.rpm
bind-utils-9.11.36-3.el8.x86_64.rpm	libudisks2-2.9.0-9.el8.x86_64.rpm
cairo-1.15.12-6.el8.x86_64.rpm	libwbclient-4.15.5-5.el8.x86_64.rpm
c-ares-1.13.0-6.el8.x86_64.rpm	mod_http2-1.15.7-5.module+el8.6.0+13996+01710940.x86_64.rpm
cpio-2.12-11.el8.x86_64.rpm	mod_session-2.4.37-47.module+el8.6.0+14529+083145da.1.x86_64.rpm
grub2-common-2.02-123.el8.noarch.rpm	mod_ssl-2.4.37-47.module+el8.6.0+14529+083145da.1.x86_64.rpm
grub2-efi-x64-2.02-123.el8.x86_64.rpm	openssh-8.0p1-13.el8.x86_64.rpm
grub2-tools-2.02-123.el8.x86_64.rpm	openssh-clients-8.0p1-13.el8.x86_64.rpm
grub2-tools-extra-2.02-123.el8.x86_64.rpm	openssh-server-8.0p1-13.el8.x86_64.rpm
grub2-tools-minimal-2.02-123.el8.x86_64.rpm	pixman-0.38.4-2.el8.x86_64.rpm
gzip-1.9-13.el8_5.x86_64.rpm	platform-python-3.6.8-45.el8.x86_64.rpm
httpd-2.4.37-47.module+el8.6.0+14529+083145da.1.x86_64.rpm	polkit-0.115-13.el8_5.2.x86_64.rpm
httpd-filesystem-2.4.37-47.module+el8.6.0+14529+083145da.1.noarch.rpm	polkit-libs-0.115-13.el8_5.2.x86_64.rpm
httpd-tools-2.4.37-47.module+el8.6.0+14529+083145da.1.x86_64.rpm	python3-bind-9.11.36-3.el8.noarch.rpm
java-1.8.0-openjdk-1.8.0.332.b09-1.el8_5.x86_64.rpm	python3-libs-3.6.8-45.el8.x86_64.rpm
java-1.8.0-openjdk-devel-1.8.0.332.b09-1.el8_5.x86_64.rpm	python3-lxml-4.2.3-4.el8.x86_64.rpm
java-1.8.0-openjdk-headless-1.8.0.332.b09-1.el8_5.x86_64.rpm	python3-perf-4.18.0-348.23.1.el8_5.x86_64.rpm
kernel-4.18.0-348.23.1.el8_5.x86_64.rpm	python3-perf-4.18.0-372.9.1.el8.x86_64.rpm
kernel-4.18.0-372.9.1.el8.x86_64.rpm	qemu-guest-agent-6.2.0-11.module+el8.6.0+14707+5aa4b42d.x86_64.rpm
kernel-core-4.18.0-348.23.1.el8_5.x86_64.rpm	rsync-3.1.3-14.el8_6.2.x86_64.rpm
kernel-core-4.18.0-372.9.1.el8.x86_64.rpm	samba-client-libs-4.15.5-5.el8.x86_64.rpm
kernel-headers-4.18.0-348.23.1.el8_5.x86_64.rpm	samba-common-4.15.5-5.el8.noarch.rpm
kernel-headers-4.18.0-372.9.1.el8.x86_64.rpm	samba-common-libs-4.15.5-5.el8.x86_64.rpm
kernel-modules-4.18.0-348.23.1.el8_5.x86_64.rpm	udisks2-2.9.0-9.el8.x86_64.rpm
kernel-modules-4.18.0-372.9.1.el8.x86_64.rpm	vim-minimal-8.0.1763-16.el8_5.13.x86_64.rpm
kernel-tools-4.18.0-348.23.1.el8_5.x86_64.rpm	zlib-1.2.11-18.el8_5.i686.rpm
kernel-tools-4.18.0-372.9.1.el8.x86_64.rpm	zlib-1.2.11-18.el8_5.x86_64.rpm
kernel-tools-libs-4.18.0-348.23.1.el8_5.x86_64.rpm	
kernel-tools-libs-4.18.0-372.9.1.el8.x86_64.rpm	
libpq-13.5-1.el8.x86_64.rpm	
libsmbclient-4.15.5-5.el8.x86_64.rpm	

Security vulnerabilities resolved in AES 10.1 Security Service Pack #3
Delivered under Fix Id AES-29701

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
java java java	RHSA-2022:1491	CVE-2022-21426 CVE-2022-21434 CVE-2022-21443 CVE-2022-21476 CVE-2022-21496	Important		
gzip	RHSA-2022:1537	CVE-2022-1271	Important	ASA-2022-041	High
polkit polkit-libs	RHSA-2022:1546	CVE-2021-4115	Moderate	ASA-2022-040	Medium
kernel kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2022:1550	CVE-2021-4028 CVE-2022-25636	Important		
vim-minimal	RHSA-2022:1552	CVE-2022-1154	Moderate	ASA-2022-042	Critical

© 2022-2024 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	RHSA-2022:1642	CVE-2018-25032	Important	ASA-2022-044	High
qemu-guest-agent	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 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	Moderate	ASA-2022-062	High
libtiff	RHSA-2022:1810	CVE-2020-19131	Moderate	ASA-2022-050	High
libudisks2 udisks2	RHSA-2022:1820	CVE-2021-3802	Low	ASA-2022-048	Low
apache-commons-logging	RHSA-2022:1861	CVE-2020-13956	Moderate	ASA-2022-073	Medium
libpq	RHSA-2022:1891	CVE-2021-23222	Low	ASA-2022-060	Low
httpd httpd-filesystem httpd-tools mod_http2 mod_session mod_ssl	RHSA-2022:1915	CVE-2020-35452 CVE-2021-33193 CVE-2021-36160 CVE-2021-44224	Moderate	ASA-2022-053	High
python3-lxml	RHSA-2022:1932	CVE-2021-43818	Moderate	ASA-2022-071	High
cairo pixman	RHSA-2022:1961	CVE-2020-35492	Moderate	ASA-2022-052	High
platform-python python3-libs	RHSA-2022:1986	CVE-2021-3737 CVE-2021-4189	Moderate	ASA-2022-049	Medium

© 2022-2024 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 kernel-core kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	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 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	Important	ASA-2022-055	Critical
cpio	RHSA-2022:1991	CVE-2021-38185	Moderate	ASA-2022-054	High
openssh openssh-clients openssh-server	RHSA-2022:2013	CVE-2021-41617	Moderate	ASA-2022-056	High
libssh libssh-config	RHSA-2022:2031	CVE-2021-3634	Low	ASA-2022-057	Medium
c-ares	RHSA-2022:2043	CVE-2021-3672	Moderate	None	NA
libsmbclient libwbclient samba-client-libs samba-common samba-common-libs	RHSA-2022:2074	CVE-2021-20316 CVE-2021-44141	Moderate	None	NA
bind-export-libs bind-libs bind-libs-lite bind-license bind-utils python3-bind	RHSA-2022:2092	CVE-2021-25219	Moderate	ASA-2022-069	Medium
grub2-common grub2-efi-x64 grub2-tools grub2-tools-extra grub2-tools-minimal	RHSA-2022:2110	CVE-2021-3981	Low	ASA-2022-051	Low

© 2022-2024 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.

rsync	RHSA-2022:2201	CVE-2018-25032	Important	ASA-2022-063	High

AES 10.1.x SSP #2 includes the following rpm updates:

expat-2.2.5-4.el8_5.3.i686.rpm expat-2.2.5-4.el8_5.3.x86_64.rpm expat-devel-2.2.5-4.el8_5.3.i686.rpm expat-devel-2.2.5-4.el8_5.3.x86_64.rpm glibc-2.28-164.el8_5.3.i686.rpm glibc-2.28-164.el8_5.3.x86_64.rpm glibc-common-2.28-164.el8_5.3.x86_64.rpm glibc-devel-2.28-164.el8_5.3.i686.rpm glibc-devel-2.28-164.el8_5.3.x86_64.rpm glibc-headers-2.28-164.el8_5.3.i686.rpm glibc-headers-2.28-164.el8_5.3.x86_64.rpm glibc-langpack-en-2.28-164.el8_5.3.x86_64.rpm httpd-2.4.37-43.module+el8.5.0+14370+51c6d843.2.x86_64.rpm httpd-2.4.37-43.module+el8.5.0+14530+6f259f31.3.x86_64.rpm httpd-filesystem-2.4.37-43.module+el8.5.0+14370+51c6d843.2.noarch.rpm httpd-filesystem-2.4.37-43.module+el8.5.0+14530+6f259f31.3.noarch.rpm httpd-tools-2.4.37-43.module+el8.5.0+14370+51c6d843.2.x86_64.rpm httpd-tools-2.4.37-43.module+el8.5.0+14530+6f259f31.3.x86_64.rpm libarchive-3.3.3-3.el8_5.x86_64.rpm	libxml2-2.9.7-12.el8_5.i686.rpm libxml2-2.9.7-12.el8_5.x86_64.rpm libxml2-devel-2.9.7-12.el8_5.i686.rpm libxml2-devel-2.9.7-12.el8_5.x86_64.rpm openssl-1.1.1k-6.el8_5.x86_64.rpm openssl-devel-1.1.1k-6.el8_5.i686.rpm openssl-devel-1.1.1k-6.el8_5.x86_64.rpm openssl-libs-1.1.1k-6.el8_5.i686.rpm openssl-libs-1.1.1k-6.el8_5.x86_64.rpm python3-libxml2-2.9.7-12.el8_5.x86_64.rpm vim-common-8.0.1763-16.el8_5.12.x86_64.rpm vim-enhanced-8.0.1763-16.el8_5.12.x86_64.rpm vim-filesystem-8.0.1763-16.el8_5.12.noarch.rpm vim-minimal-8.0.1763-16.el8_5.12.x86_64.rpm qemu-guest-agent-4.2.0-59.module+el8.5.0+14169+68d2f392.2.x86_64.rpm

Security vulnerabilities resolved in AES 10.1 Security Service Pack #2
Delivered under Fix Id AES-29419

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
httpd httpd-filesystem httpd-tools	RHSA-2022:0891	CVE-2021-39275 CVE-2021-34798	Moderate	ASA-2022-029	High
libarchive	RHSA-2022:0892	CVE-2021-31566 CVE-2021-23177	Moderate	None	NA
vim-common vim-enhanced vim-filesystem vim-minimal	RHSA-2022:0894	CVE-2022-0413 CVE-2022-0392 CVE-2022-0361 CVE-2022-0359 CVE-2022-0318 CVE-2022-0261	Moderate	ASA-2022-030	High
glibc glibc-common glibc-devel glibc-headers glibc-langpack-en	RHSA-2022:0896	CVE-2022-23219 CVE-2022-23218 CVE-2021-3999	Moderate	ASA-2022-074	High
libxml2 libxml2-devel python3-libxml2	RHSA-2022:0899	CVE-2022-23308	Moderate	ASA-2022-033	High

© 2022-2024 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.

expat expat-devel	RHSA-2022:0951	CVE-2022-25315 CVE-2022-25236 CVE-2022-25235 CVE-2022-23852 CVE-2022-22827 CVE-2022-22826 CVE-2022-22825 CVE-2022-22824 CVE-2022-22823 CVE-2022-22822 CVE-2021-46143 CVE-2021-45960	Important	ASA-2022-031	Critical
httpd httpd-filesystem httpd-tools	RHSA-2022:1049	CVE-2022-22720	Important	ASA-2022-034	Critical
openssl openssl-devel openssl-libs	RHSA-2022:1065	CVE-2022-0778	Important	ASA-2022-036	High
qemu-guest-agent	RHSA-2022:0886	CVE-2022-0358	Moderate	ASA-2022-032	High

SSP#1 rpm and RHSA info updated May 16

AES 10.1.x SSP #1 includes the following rpm updates:

aide-0.16-14.el8_5.1.x86_64	libsmbclient-4.13.3-5.el8_4.x86_64
annobin-9.72-1.el8_5.2.x86_64	libsmbclient-4.14.5-7.el8_5.x86_64
bind-export-libs-32:9.11.26-6.el8.x86_64	libsmbclient-4.14.5-9.el8_5.x86_64
bind-libs-32:9.11.26-6.el8.x86_64	libsolv-0.7.16-3.el8_4.x86_64
bind-libs-lite-32:9.11.26-6.el8.x86_64	libsolv-0.7.19-1.el8.x86_64
bind-license-32:9.11.26-6.el8.noarch	libssh-0.9.4-3.el8.i686
bind-utils-32:9.11.26-6.el8.x86_64	libssh-0.9.4-3.el8.x86_64
binutils-2.30-108.el8_5.1.x86_64	libssh-config-0.9.4-3.el8.noarch
binutils-2.30-108.el8.x86_64	libstdc++-8.5.0-3.el8.i686
cpp-8.5.0-3.el8.x86_64	libstdc++-8.5.0-3.el8.x86_64
cpp-8.5.0-4.el8_5.x86_64	libstdc++-8.5.0-4.el8_5.i686
cryptsetup-2.3.3-4.el8_5.1.x86_64	libstdc++-8.5.0-4.el8_5.x86_64
cryptsetup-libs-2.3.3-4.el8_5.1.x86_64	libtiff-4.0.9-20.el8.i686
cups-libs-1:2.2.6-40.el8.x86_64	libtiff-4.0.9-20.el8.x86_64
curl-7.61.1-18.el8_4.2.x86_64	libwbclient-4.13.3-5.el8_4.x86_64
curl-7.61.1-22.el8.x86_64	libwbclient-4.14.5-7.el8_5.x86_64
cyrus-sasl-gssapi-2.1.27-6.el8_5.x86_64	libwbclient-4.14.5-9.el8_5.x86_64
cyrus-sasl-lib-2.1.27-6.el8_5.i686	libX11-1.6.8-5.el8.x86_64
cyrus-sasl-lib-2.1.27-6.el8_5.x86_64	libX11-common-1.6.8-5.el8.noarch
dnf-4.7.0-4.el8.noarch	libX11-xcb-1.6.8-5.el8.x86_64
dnf-data-4.7.0-4.el8.noarch	lua-5.3.4-12.el8.x86_64
dnf-plugins-core-4.0.21-3.el8.noarch	lua-libs-5.3.4-12.el8.i686
file-5.33-20.el8.x86_64	lua-libs-5.3.4-12.el8.x86_64
file-libs-5.33-20.el8.x86_64	mod_session-2.4.37-41.module+el8.5.0+11772+c8e0c271.x86_64
gcc-8.5.0-3.el8.x86_64	mod_session-2.4.37-43.module+el8.5.0+13064+c4b14997.x86_64
gcc-8.5.0-4.el8_5.x86_64	mod_session-2.4.37-43.module+el8.5.0+13806+b30d9eec.1.x86_64
gcc-gdb-plugin-8.5.0-3.el8.x86_64	mod_ssl-1:2.4.37-41.module+el8.5.0+11772+c8e0c271.x86_64
gcc-gdb-plugin-8.5.0-4.el8_5.x86_64	mod_ssl-1:2.4.37-43.module+el8.5.0+13064+c4b14997.x86_64
glib2-2.56.4-156.el8.i686	mod_ssl-1:2.4.37-43.module+el8.5.0+13806+b30d9eec.1.x86_64
glib2-2.56.4-156.el8.x86_64	ncurses-6.1-9.20180224.el8.x86_64
glibc-2.28-164.el8.i686	ncurses-base-6.1-9.20180224.el8.noarch
glibc-2.28-164.el8.x86_64	ncurses-libs-6.1-9.20180224.el8.x86_64
glibc-all-langpacks-2.28-164.el8.x86_64	nettle-3.4.1-7.el8.i686
glibc-common-2.28-164.el8.x86_64	nettle-3.4.1-7.el8.x86_64
glibc-devel-2.28-164.el8.x86_64	NetworkManager-1:1.32.10-4.el8.x86_64
glibc-headers-2.28-164.el8.x86_64	NetworkManager-libnm-1:1.32.10-4.el8.x86_64
glibc-langpack-en-2.28-164.el8.x86_64	NetworkManager-team-1:1.32.10-4.el8.x86_64

© 2022-2024 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.

gnutls-3.6.16-4.el8.i686	NetworkManager-tui-1:1.32.10-4.el8.x86_64
gnutls-3.6.16-4.el8.x86_64	nscd-2.28-164.el8.x86_64
gtk-update-icon-cache-3.22.30-8.el8.x86_64	nss-3.67.0-7.el8_5.x86_64
httpd-2.4.37-41.module+el8.5.0+11772+c8e0c271.x86_64	nss-softokn-3.67.0-7.el8_5.x86_64
httpd-2.4.37-43.module+el8.5.0+13064+c4b14997.x86_64	nss-softokn-freebl-3.67.0-7.el8_5.x86_64
httpd-2.4.37-43.module+el8.5.0+13806+b30d9eec.1.x86_64	nss-sysinit-3.67.0-7.el8_5.x86_64
httpd-filesystem-2.4.37-41.module+el8.5.0+11772+c8e0c271.noarch	nss-util-3.67.0-7.el8_5.x86_64
	openssh-8.0p1-10.el8.x86_64
httpd-filesystem-2.4.37-43.module+el8.5.0+13064+c4b14997.noarch	openssh-clients-8.0p1-10.el8.x86_64
	openssh-server-8.0p1-10.el8.x86_64
httpd-filesystem-2.4.37-43.module+el8.5.0+13806+b30d9eec.1.noarch	openssl-1:1.1.1k-4.el8.x86_64
	openssl-1:1.1.1k-5.el8_5.x86_64
httpd-tools-2.4.37-41.module+el8.5.0+11772+c8e0c271.x86_64	openssl-libs-1:1.1.1k-4.el8.i686
	openssl-libs-1:1.1.1k-4.el8.x86_64
httpd-tools-2.4.37-43.module+el8.5.0+13064+c4b14997.x86_64	openssl-libs-1:1.1.1k-5.el8_5.i686
	openssl-libs-1:1.1.1k-5.el8_5.x86_64
httpd-tools-2.4.37-43.module+el8.5.0+13806+b30d9eec.1.x86_64	pcre-8.42-6.el8.i686
	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-devel-1:1.8.0.322.b06-2.el8_5.x86_64	platform-python-pip-9.0.3-20.el8.noarch
java-1.8.0-openjdk-headless-1:1.8.0.322.b06-2.el8_5.x86_64	polkit-0.115-13.el8_5.1.x86_64
json-c-0.13.1-2.el8.x86_64	polkit-libs-0.115-13.el8_5.1.x86_64
kernel-4.18.0-305.25.1.el8_4.x86_64	python36-3.6.8-38.module+el8.5.0+12207+5c5719bc.x86_64
kernel-4.18.0-348.12.2.el8_5.x86_64	python3-bind-32:9.11.26-6.el8.noarch
kernel-4.18.0-348.20.1.el8_5.x86_64	python3-dnf-4.7.0-4.el8.noarch
kernel-4.18.0-348.2.1.el8_5.x86_64	python3-dnf-plugins-core-4.0.21-3.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-4.18.0-348.20.1.el8_5.x86_64	python3-lxml-4.2.3-3.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-4.18.0-348.7.1.el8_5.x86_64	python3-perf-4.18.0-348.12.2.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-headers-4.18.0-348.12.2.el8_5.x86_64	python3-perf-4.18.0-348.2.1.el8_5.x86_64
kernel-headers-4.18.0-348.20.1.el8_5.x86_64	python3-perf-4.18.0-348.7.1.el8_5.x86_64
kernel-headers-4.18.0-348.2.1.el8_5.x86_64	python3-perf-4.18.0-348.el8.x86_64
kernel-headers-4.18.0-348.7.1.el8_5.x86_64	python3-pip-9.0.3-20.el8.noarch
kernel-headers-4.18.0-348.el8.x86_64	python3-pip-wheel-9.0.3-20.el8.noarch
kernel-modules-4.18.0-305.25.1.el8_4.x86_64	python3-rpm-4.14.3-19.el8_5.2.x86_64
kernel-modules-4.18.0-348.12.2.el8_5.x86_64	python3-rpm-4.14.3-19.el8.x86_64
kernel-modules-4.18.0-348.20.1.el8_5.x86_64	qemu-guest-agent-15:4.2.0-48.module+el8.4.0+11909+3300d70f.3.x86_64
kernel-modules-4.18.0-348.2.1.el8_5.x86_64	qemu-guest-agent-15:4.2.0-59.module+el8.5.0+12817+cb650d43.x86_64
kernel-modules-4.18.0-348.7.1.el8_5.x86_64	qemu-guest-agent-15:4.2.0-59.module+el8.5.0+13495+8166cdf8.1.x86_64
kernel-modules-4.18.0-348.el8.x86_64	qt5-srpm-macros-5.15.2-1.el8.noarch
kernel-tools-4.18.0-305.25.1.el8_4.x86_64	rpm-4.14.3-19.el8_5.2.x86_64
kernel-tools-4.18.0-348.12.2.el8_5.x86_64	rpm-4.14.3-19.el8.x86_64
kernel-tools-4.18.0-348.20.1.el8_5.x86_64	rpm-build-libs-4.14.3-19.el8_5.2.x86_64
kernel-tools-4.18.0-348.2.1.el8_5.x86_64	rpm-build-libs-4.14.3-19.el8.x86_64
kernel-tools-4.18.0-348.7.1.el8_5.x86_64	rpm-libs-4.14.3-19.el8_5.2.i686
kernel-tools-4.18.0-348.el8.x86_64	rpm-libs-4.14.3-19.el8_5.2.x86_64
kernel-tools-libs-4.18.0-305.25.1.el8_4.x86_64	rpm-libs-4.14.3-19.el8.i686
kernel-tools-libs-4.18.0-348.12.2.el8_5.x86_64	rpm-libs-4.14.3-19.el8.x86_64
kernel-tools-libs-4.18.0-348.20.1.el8_5.x86_64	rpm-plugin-selinux-4.14.3-19.el8_5.2.x86_64
kernel-tools-libs-4.18.0-348.2.1.el8_5.x86_64	rpm-plugin-selinux-4.14.3-19.el8.x86_64
kernel-tools-libs-4.18.0-348.7.1.el8_5.x86_64	rpm-plugin-systemd-inhibit-4.14.3-19.el8_5.2.x86_64
kernel-tools-libs-4.18.0-348.el8.x86_64	rpm-plugin-systemd-inhibit-4.14.3-19.el8.x86_64
kexec-tools-2.0.20-57.el8.x86_64	samba-client-libs-4.13.3-5.el8_4.x86_64

© 2022-2024 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.i686	samba-client-libs-4.14.5-7.el8_5.x86_64
libcurl-7.61.1-18.el8_4.2.x86_64	samba-client-libs-4.14.5-9.el8_5.x86_64
libcurl-7.61.1-22.el8.i686	samba-common-4.13.3-5.el8_4.noarch
libcurl-7.61.1-22.el8.x86_64	samba-common-4.14.5-7.el8_5.noarch
libdnf-0.63.0-3.el8.x86_64	samba-common-4.14.5-9.el8_5.noarch
libgcc-8.5.0-3.el8.i686	samba-common-libs-4.13.3-5.el8_4.x86_64
libgcc-8.5.0-3.el8.x86_64	samba-common-libs-4.14.5-7.el8_5.x86_64
libgcc-8.5.0-4.el8_5.i686	samba-common-libs-4.14.5-9.el8_5.x86_64
libgcc-8.5.0-4.el8_5.x86_64	sqlite-3.26.0-15.el8.x86_64
libgcrypt-1.8.5-6.el8.x86_64	sqlite-libs-3.26.0-15.el8.i686
libgomp-8.5.0-3.el8.x86_64	sqlite-libs-3.26.0-15.el8.x86_64
libgomp-8.5.0-4.el8_5.x86_64	tpm2-tools-4.1.1-5.el8.x86_64
libjpeg-turbo-1.5.3-12.el8.i686	vim-minimal-2:8.0.1763-16.el8_5.4.x86_64
libjpeg-turbo-1.5.3-12.el8.x86_64	vim-minimal-2:8.0.1763-16.el8.x86_64
libsepol-2.9-3.el8.i686	yum-4.7.0-4.el8.noarch
libsepol-2.9-3.el8.x86_64	

Security vulnerabilities resolved in AES 10.1 Security Service Pack #1
Delivered under Fix Id AES-29096

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
kernel-core kernel-devel kernel-headers kernel kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2021:4056	CVE-2021-3656 CVE-2021-0512 CVE-2020-36385	Important	NA	NA
platform-python-devel platform-python python3-libs	RHSA-2021:4057	CVE-2021-3733	Moderate	ASA-2021-133	Medium
curl libcurl	RHSA-2021:4059	CVE-2021-22947 CVE-2021-22946	Moderate	NA	NA
libsolv	RHSA-2021:4060	CVE-2021-33938 CVE-2021-33930 CVE-2021-33929 CVE-2021-33928	Moderate	NA	NA
python36-devel python36	RHSA-2021:4150	CVE-2021-27291 CVE-2021-20270	Moderate	ASA-2021-142	High
qt5-srpm-macros	RHSA-2021:4172	CVE-2021-3481	Moderate	NA	NA
jasper-libs	RHSA-2021:4235	CVE-2021-3272 CVE-2021-26927 CVE-2021-26926 CVE-2020-27828	Moderate	NA	NA
libtiff	RHSA-2021:4241	CVE-2020-35524 CVE-2020-35523 CVE-2020-35522 CVE-2020-35521	Moderate	NA	NA
httpd-filesystem httpd httpd-tools	RHSA-2021:4257	CVE-2021-30641 CVE-2021-26690	Moderate	NA	NA
libjpeg-turbo	RHSA-2021:4288	CVE-2020-17541	Moderate	ASA-2021-148	High
libX11-common libX11	RHSA-2021:4326	CVE-2021-31535	Moderate	NA	NA

© 2022-2024 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 kernel-devel kernel-headers kernel kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2021:4356	CVE-2021-3732 CVE-2021-3679 CVE-2021-3659 CVE-2021-3635 CVE-2021-3600 CVE-2021-3573 CVE-2021-3564 CVE-2021-3489 CVE-2021-3348 CVE-2021-33200 CVE-2021-33033 CVE-2021-31916 CVE-2021-31829 CVE-2021-31440 CVE-2021-29650 CVE-2021-29646 CVE-2021-29155 CVE-2021-28971 CVE-2021-28950 CVE-2021-23133 CVE-2021-20239 CVE-2021-20194 CVE-2021-0129 CVE-2020-36386 CVE-2020-36312 CVE-2020-36158 CVE-2020-29660 CVE-2020-29368 CVE-2020-27777 CVE-2020-26147 CVE-2020-26146 CVE-2020-26145 CVE-2020-26144 CVE-2020-26143 CVE-2020-26141 CVE-2020-26140 CVE-2020-26139 CVE-2020-24588 CVE-2020-24587 CVE-2020-24586 CVE-2020-24504 CVE-2020-24503 CVE-2020-24502 CVE-2020-0427 CVE-2019-14615	Moderate	ASA-2021-147	High
glibc-common glibc-devel glibc glibc-headers glibc-langpack-en	RHSA-2021:4358	CVE-2021-35942 CVE-2021-33574 CVE-2021-27645	Moderate	NA	NA
NetworkManager-libnm NetworkManager NetworkManager-team NetworkManager-tui	RHSA-2021:4361	CVE-2020-13529	Moderate	NA	NA
binutils	RHSA-2021:4364	CVE-2021-3487 CVE-2021-20284 CVE-2021-20197 CVE-2020-35448	Moderate	ASA-2021-145	Medium
openssh-clients openssh openssh-server	RHSA-2021:4368	CVE-2020-14145	Moderate	ASA-2021-140	Medium

© 2022-2024 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.

pcre-cpp pcre-devel pcre pcre-utf16 pcre-utf32	RHSA-2021:4373	CVE-2020-14155 CVE-2019-20838	Low	NA	NA
file file-libs	RHSA-2021:4374	CVE-2019-18218	Moderate	NA	NA
gtk-update-icon-cache	RHSA-2021:4381	CVE-2021-30799 CVE-2021-30797 CVE-2021-30795 CVE-2021-30758 CVE-2021-30749 CVE-2021-30744 CVE-2021-30734 CVE-2021-30720 CVE-2021-30689 CVE-2021-30682 CVE-2021-30665 CVE-2021-30663 CVE-2021-28650 CVE-2021-21806 CVE-2021-21779 CVE-2021-21775 CVE-2021-1871 CVE-2021-1870 CVE-2021-1844 CVE-2021-1801 CVE-2021-1799 CVE-2021-1789 CVE-2021-1788 CVE-2021-1765 CVE-2020-36241 CVE-2020-29623 CVE-2020-27918 CVE-2020-24870 CVE-2020-13558	Moderate	ASA-2021-144	Critical
json-c	RHSA-2021:4382	CVE-2020-12762	Moderate	NA	NA
bind-export-libs	RHSA-2021:4384	CVE-2021-25214	Moderate	NA	NA
glib2	RHSA-2021:4385	CVE-2021-3800 CVE-2021-28153	Moderate	NA	NA
cpp gcc-c++ gcc gcc-gdb-plugin libgcc libgomp libstdc++-devel	RHSA-2021:4386	CVE-2018-20673	Low	NA	NA
libssh-config libssh-devel libssh	RHSA-2021:4387	CVE-2020-16135	Low	NA	NA
cups-libs	RHSA-2021:4393	CVE-2020-10001	Moderate	NA	NA
sqlite-libs	RHSA-2021:4396	CVE-2020-13435 CVE-2019-5827 CVE-2019-19603 CVE-2019-13751 CVE-2019-13750	Moderate	ASA-2021-141	High
platform-python-devel platform-python python3-libs	RHSA-2021:4399	CVE-2021-3426	Moderate	NA	NA
kexec-tools	RHSA-2021:4404	CVE-2021-20269	Low	ASA-2021-151	Medium
libsolv	RHSA-2021:4408	CVE-2021-3200	Low	NA	NA
libgcrypt	RHSA-2021:4409	CVE-2021-33560	Moderate	NA	NA

© 2022-2024 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-devel openssl-libs openssl	RHSA-2021:4424	CVE-2021-23841 CVE-2021-23840	Moderate	ASA-2021-134	High
ncurses-base ncurses-c++-libs ncurses-devel ncurses-libs ncurses	RHSA-2021:4426	CVE-2019-17595 CVE-2019-17594	Moderate	ASA-2021-146	Medium
gnutls nettle	RHSA-2021:4451	CVE-2021-3580 CVE-2021-20232 CVE-2021-20231	Moderate	ASA-2021-149	High
platform-python-pip python3-pip python3-pip-wheel	RHSA-2021:4455	CVE-2021-3572	Low	ASA-2021-139	Medium
dnf-data dnf dnf-plugins-core libdnf python3-dnf-plugins-core python3-dnf python3-hawkey python3-libdnf yum	RHSA-2021:4464	CVE-2021-3445	Moderate	NA	NA
python3-rpm rpm-build-libs rpm-build rpm-libs rpm-plugin-selinux rpm-plugin-systemd-inhibit rpm rpm-sign	RHSA-2021:4489	CVE-2021-20266	Low	ASA-2021-136	Medium
lua-devel lua-libs lua	RHSA-2021:4510	CVE-2020-24370	Low	ASA-2021-137	Medium
curl libcurl	RHSA-2021:4511	CVE-2021-22925 CVE-2021-22898 CVE-2021-22876	Moderate	NA	NA
libsepol-devel libsepol	RHSA-2021:4513	CVE-2021-36087 CVE-2021-36086 CVE-2021-36085 CVE-2021-36084	Moderate	NA	NA
vim-common vim-enhanced vim-filesystem vim-minimal	RHSA-2021:4517	CVE-2021-3796 CVE-2021-3778	Moderate	ASA-2021-150	High
httpd-filesystem httpd httpd-tools	RHSA-2021:4537	CVE-2021-20325	Important	NA	NA
annobin binutils cpp gcc-c++ gcc gcc-gdb-plugin libgcc libgomp libstdc++-devel libstdc++	RHSA-2021:4587	CVE-2021-42574	Moderate	NA	NA

© 2022-2024 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.

annobin binutils cpp gcc-c++ gcc gcc-gdb-plugin libgcc libgomp libstdc++-devel libstdc++	RHSA-2021:4593	CVE-2021-42574	Moderate	NA	NA
annobin binutils cpp gcc-c++ gcc gcc-gdb-plugin libgcc libgomp libstdc++-devel libstdc++	RHSA-2021:4595	CVE-2021-42574	Moderate	ASA-2021-152	High
kernel-core kernel-devel kernel-headers kernel kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2021:4647	CVE-2021-43267 CVE-2021-20317	Important	ASA-2021-178	High
nss nss-softokn-freebl nss-softokn nss-sysinit nss-tools nss-util	RHSA-2021:4903	CVE-2021-43527	Critical	NA	NA
openssl-devel openssl-libs openssl	RHSA-2021:5226	CVE-2021-3712	Moderate	ASA-2022-002	High
kernel-core kernel-devel kernel-headers kernel kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2021:5227	CVE-2021-20321	Moderate	ASA-2021-187	Medium
kernel-core kernel-devel kernel-headers kernel kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2022:0188	CVE-2022-0185 CVE-2021-4155	Important	ASA-2022-006	High
httpd-filesystem httpd httpd-tools	RHSA-2022:0258	CVE-2021-44790	Important	ASA-2022-020	Critical
polkit-libs polkit	RHSA-2022:0267	CVE-2021-4034	Important	ASA-2022-007	High

© 2022-2024 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-1.8.0-openjdk-devel java-1.8.0-openjdk-headless java-1.8.0-openjdk	RHSA-2022:0307	CVE-2022-21365 CVE-2022-21360 CVE-2022-21341 CVE-2022-21340 CVE-2022-21305 CVE-2022-21299 CVE-2022-21296 CVE-2022-21294 CVE-2022-21293 CVE-2022-21283 CVE-2022-21282 CVE-2022-21248	Moderate	ASA-2022-008	Medium
vim-common vim-enhanced vim-filesystem vim-minimal	RHSA-2022:0366	CVE-2021-4193 CVE-2021-4192 CVE-2021-4019 CVE-2021-3984 CVE-2021-3872	Moderate	ASA-2022-015	High
python3-rpm rpm-build-libs rpm-build rpm-libs rpm-plugin-selinux rpm-plugin-systemd-inhibit rpm rpm-sign	RHSA-2022:0368	CVE-2021-3521	Moderate	ASA-2022-016	Medium
cryptsetup-libs	RHSA-2022:0370	CVE-2021-4122	Moderate	ASA-2022-019	Medium
cyrus-sasl cyrus-sasl-devel cyrus-sasl-lib	RHSA-2022:0658	CVE-2022-24407	Important	NA	NA
kernel-core kernel-devel kernel-headers kernel kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2022:0825	CVE-2022-22942 CVE-2022-0847 CVE-2022-0516 CVE-2022-0492 CVE-2022-0435 CVE-2022-0330 CVE-2021-4154 CVE-2021-0920	Important	NA	NA

© 2022-2024 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.

hivex libguestfs libvirt-bash-completion libvirt-client libvirt-daemon libvirt-daemon-config-network libvirt-daemon-driver-interface libvirt-daemon-driver-network libvirt-daemon-driver-nodedev libvirt-daemon-driver-nwfilter libvirt-daemon-driver-qemu libvirt-daemon-driver-secret libvirt-daemon-driver-storage libvirt-daemon-driver-storage-core libvirt-daemon-driver-storage-disk libvirt-daemon-driver-storage-gluster libvirt-daemon-driver-storage-iscsi libvirt-daemon-driver-storage-iscsi-direct libvirt-daemon-driver-storage-logical libvirt-daemon-driver-storage-mpath libvirt-daemon-driver-storage-rbd libvirt-daemon-driver-storage-scsi libvirt-daemon-kvm libvirt-libs qemu-guest-agent qemu-img qemu-kvm qemu-kvm-block-curl qemu-kvm-block-gluster qemu-kvm-block-iscsi qemu-kvm-block-rbd qemu-kvm-block-ssh qemu-kvm-common qemu-kvm-core	RHSA-2021:3061	CVE-2021-3504 CVE-2021-3416 CVE-2021-20221 CVE-2020-27617 CVE-2020-13754	Moderate	NA	NA
libsmbclient libwbclient samba-client-libs samba-common samba-common-libs	RHSA-2021:4058	CVE-2021-20254	Moderate	ASA-2021-131	Medium
python3-lxml	RHSA-2021:4158	CVE-2021-28957	Moderate	NA	NA

© 2022-2024 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	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	NA	NA
tpm2-tools	RHSA-2021:4413	CVE-2021-3565	Moderate	NA	NA
libsmbclient libwbclient samba-client-libs samba-common samba-common-libs	RHSA-2021:5082	CVE-2016-2124 CVE-2020-25717 CVE-2021-23192	Moderate	NA	NA
qemu-guest-agent	RHSA-2021:5238	CVE-2021-20257 CVE-2021-3930	Moderate	ASA-2021-189	Low
libsmbclient libwbclient samba-client-libs samba-common samba-common-libs	RHSA-2022:0332	CVE-2021-44142	Moderate	ASA-2022-017	Critical
aide	RHSA-2022:0441	CVE-2021-45417	Moderate	ASA-2022-021	High

Mitigation: N/A

SECTION 1C – ENTITLEMENTS AND CONTACTS

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

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

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

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

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

© 2022-2024 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: -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.

© 2022-2024 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.