

Product Correction Notice (PCN)

Issue Date: 18-April-2022
 Supplement Date: 8-April-2024
 Expiration Date: NA
 PCN Number: 2134S

SECTION 1 - CUSTOMER NOTICE

**Products
 affected by this
 PCN:**

Avaya Aura® Communication Manager 10.1 vAppliance running on Avaya provided servers: Avaya Solutions Platform 130 R5.x (Dell® PowerEdge R640), Avaya Solutions Platform S8300E R5.1.
 Avaya Aura® Communication Manager 10.1 vAppliance running on Customer provided VMware® certified hardware.
 Reference the Avaya Aura® Platform Offer Definition for details.

Description:**CRITICAL Notes:**

- Reference *PSN020621u - Avaya Aura® Communication Manager SMI Network changes may result in segmentation fault* prior to applying SSP #18 or later.
- The Security Service Pack installation framework for Communication Manager 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 a Communication Manager 10.1.x system.

8 April 2024 – Supplement 22-1 of this PCN announces the removal of Avaya Aura® Communication Manager (CM) 10.1 Security Service Pack #21 from PLDS and support.avaya.com. Avaya has identified an issue with CM 10.1 SSP #21 where after application of SSP #21 the following messages is seen when logging into the CM CLI.

`sudo: /etc/sudoers.d/sudoers_cm:21:23: unknown defaults entry "cmdnd_no_wait"`

While not service impacting, Avaya has decided to remove SSP #21 from PLDS/support to minimize concerns due to these messages.

The next Security Service Pack (SSP #22) will resolve this issue.

Tentative target GA for SSP #22 is April 22, 2024.

Customers who have applied SSP #21 should plan to apply SSP #22 as soon as it is available so that these errant messages are resolved.

Also reference *PSN020635u - Avaya Aura® Communication Manager 10.1 SSP #21 no longer available*.

18 March 2024 – Supplement 22 of this PCN introduces **Avaya Aura® Communication Manager (CM) 10.1 Security Service Pack #21**

(AV-CM10.1-RHEL8.4-SSP-021-01.tar.bz2; ~~PLDS ID CM000002041~~) Updated: See Supplement 22-1 above.

- CM 10.1 security updates (both Linux and Kernel) are now provided in a Security Service Pack (SSP). There will no longer be a separate Kernel Service Pack (KSP).
- CM SSP #21 is only applicable to CM 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later Service Pack/Feature Pack or on 10.1.0.1 or later Service Pack/Feature Pack that has an earlier SSP installed. CM 10.1 SSPs CANNOT be installed on CM 10.2.
- **Critical Note:** CM SSP #21 **must** be installed after applying the 10.1.0.1 or later Service Pack

to ensure robust security protection. Reference **PCN2133S** for additional details on the mandatory CM 10.1.0.1 Service Pack and subsequent Service Packs/Feature Packs.

- Installation of CM 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 #20.
- Beginning with CM 10.1.3 which launched May 22, 2023, the following methods are supported for installation of CM 10.1 SSPs. Prior to CM 10.1.3, only the CM Command Line Interface (CLI) was supported for installation of CM 10.1 SSPs.
 - i. Solution Deployment Manager (SDM)
 - ii. CM System Management Interface (SMI)
 - iii. CM Command Line Interface (CLI)

Additional information can be found in Appendix C of [Upgrading Avaya Aura® Communication Manager](#)

16 January 2024 – Supplement 21 of this PCN introduces **Avaya Aura® Communication Manager (CM) 10.1 Security Service Pack #20**

(AV-CM10.1-RHEL8.4-SSP-020-01.tar.bz2; **PLDS ID CM000002035**)

- CM 10.1 security updates (both Linux and Kernel) are now provided in a Security Service Pack (SSP). There will no longer be a separate Kernel Service Pack (KSP).
- CM SSP #20 is only applicable to CM 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later Service Pack/Feature Pack or on 10.1.0.1 or later Service Pack/Feature Pack that has an earlier SSP installed. CM 10.1 SSPs CANNOT be installed on CM 10.2.
- **Critical Note:** CM SSP #20 **must** be installed after applying the 10.1.0.1 or later Service Pack to ensure robust security protection. Reference **PCN2133S** for additional details on the mandatory CM 10.1.0.1 Service Pack and subsequent Service Packs/Feature Packs.
- Installation of CM 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.
- Beginning with CM 10.1.3 which launched May 22, 2023, the following methods are supported for installation of CM 10.1 SSPs. Prior to CM 10.1.3, only the CM Command Line Interface (CLI) was supported for installation of CM 10.1 SSPs.
 - iv. Solution Deployment Manager (SDM)
 - v. CM System Management Interface (SMI)
 - vi. CM Command Line Interface (CLI)

Additional information can be found in Appendix C of [Upgrading Avaya Aura® Communication Manager](#)

18 December 2023 – Supplement 20 of this PCN introduces **Avaya Aura® Communication Manager**

(CM) 10.1 Security Service Pack #19

(AV-CM10.1-RHEL8.4-SSP-019-02.tar.bz2; PLDS ID CM000002033)

- CM 10.1 security updates (both Linux and Kernel) are now provided in a Security Service Pack (SSP). There will no longer be a separate Kernel Service Pack (KSP).
- CM SSP #19 is only applicable to CM 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later Service Pack/Feature Pack or on 10.1.0.1 or later Service Pack/Feature Pack that has an earlier SSP installed. CM 10.1 SSPs CANNOT be installed on CM 10.2.
- **Critical Note:** CM SSP #19 **must** be installed after applying the 10.1.0.1 or later Service Pack to ensure robust security protection. Reference **PCN2133S** for additional details on the mandatory CM 10.1.0.1 Service Pack and subsequent Service Packs/Feature Packs.
- Installation of CM 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.
- 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 #19.
- Beginning with CM 10.1.3 which launched May 22, 2023, the following methods are supported for installation of CM 10.1 SSPs. Prior to CM 10.1.3, only the CM Command Line Interface (CLI) was supported for installation of CM 10.1 SSPs.
 - vii. Solution Deployment Manager (SDM)
 - viii. CM System Management Interface (SMI)
 - ix. CM Command Line Interface (CLI)

Additional information can be found in Appendix C of [Upgrading Avaya Aura® Communication Manager](#)

20 November 2023 – Supplement 19 of this PCN introduces **Avaya Aura® Communication Manager**

(CM) 10.1 Security Service Pack #18

(AV-CM10.1-RHEL8.4-SSP-018-09.tar.bz2; PLDS ID CM000002032)

- CM 10.1 security updates (both Linux and Kernel) are now provided in a Security Service Pack (SSP). There will no longer be a separate Kernel Service Pack (KSP).
- CM SSP #18 is only applicable to CM 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later Service Pack/Feature Pack or on 10.1.0.1 or later Service Pack/Feature Pack that has an earlier SSP installed.
- **Critical Note:** CM SSP #18 **must** be installed after applying the 10.1.0.1 or later Service Pack to ensure robust security protection. Reference **PCN2133S** for additional details on the mandatory CM 10.1.0.1 Service Pack and subsequent Service Packs/Feature Packs.
- Installation of CM 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.
- Beginning with CM 10.1.3 which launched May 22, 2023, the following methods are supported for installation of CM 10.1 SSPs. Prior to CM 10.1.3, only the CM Command Line Interface (CLI) was supported for installation of CM 10.1 SSPs.
 - x. Solution Deployment Manager (SDM)
 - xi. CM System Management Interface (SMI)

xii. CM Command Line Interface (CLI)

Additional information can be found in Appendix C of [Upgrading Avaya Aura® Communication Manager](#)

16 October 2023 – Supplement 18 of this PCN introduces **Avaya Aura® Communication Manager (CM) 10.1 Security Service Pack #17**

(AV-CM10.1-RHEL8.4-SSP-017-02.tar.bz2; **PLDS ID CM000002031**)

- CM 10.1 security updates (both Linux and Kernel) are now provided in a Security Service Pack (SSP). There will no longer be a separate Kernel Service Pack (KSP).
- CM SSP #17 is only applicable to CM 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later Service Pack/Feature Pack or on 10.1.0.1 or later Service Pack/Feature Pack that has an earlier SSP installed.
- **Critical Note:** CM SSP #17 **must** be installed after applying the 10.1.0.1 or later Service Pack to ensure robust security protection. Reference **PCN2133S** for additional details on the mandatory CM 10.1.0.1 Service Pack and subsequent Service Packs/Feature Packs.
- Installation of CM 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.
- Beginning with CM 10.1.3 which launched May 22, 2023, the following methods are supported for installation of CM 10.1 SSPs. Prior to CM 10.1.3, only the CM Command Line Interface (CLI) was supported for installation of CM 10.1 SSPs.
 - xiii. Solution Deployment Manager (SDM)
 - xiv. CM System Management Interface (SMI)
 - xv. CM Command Line Interface (CLI)

Additional information can be found in Appendix C of [Upgrading Avaya Aura® Communication Manager](#).

18 September 2023 – Supplement 17 of this PCN introduces **Avaya Aura® Communication Manager (CM) 10.1 Security Service Pack #16**

(AV-CM10.1-RHEL8.4-SSP-016-02.tar.bz2; **PLDS ID CM000002030**)

- CM 10.1 security updates (both Linux and Kernel) are now provided in a Security Service Pack (SSP). There will no longer be a separate Kernel Service Pack (KSP).
- CM SSP #16 is only applicable to CM 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later Service Pack/Feature Pack or on 10.1.0.1 or later Service Pack/Feature Pack that has an earlier SSP installed.
- **Critical Note:** CM SSP #16 **must** be installed after applying the 10.1.0.1 or later Service Pack to ensure robust security protection. Reference **PCN2133S** for additional details on the mandatory CM 10.1.0.1 Service Pack and subsequent Service Packs/Feature Packs.
- Installation of CM SSP #16 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 #16.

- Beginning with CM 10.1.3 which launched May 22, 2023, the following methods are supported for installation of CM 10.1 SSPs. Prior to CM 10.1.3, only the CM Command Line Interface (CLI) was supported for installation of CM 10.1 SSPs.
 - xvi. Solution Deployment Manager (SDM)
 - xvii. CM System Management Interface (SMI)
 - xviii. CM Command Line Interface (CLI)

Additional information can be found in Appendix C of [Upgrading Avaya Aura® Communication Manager](#).

28 August 2023 – Supplement 16 of this PCN introduces Avaya Aura® Communication Manager (CM) 10.1 Security Service Pack #15

(AV-CM10.1-RHEL8.4-SSP-015-01.tar.bz2; PLDS ID CM000002028)

- CM 10.1 security updates (both Linux and Kernel) are now provided in a Security Service Pack (SSP). There will no longer be a separate Kernel Service Pack (KSP).
- CM SSP #15 is only applicable to CM 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later Service Pack/Feature Pack or on 10.1.0.1 or later Service Pack/Feature Pack that has an earlier SSP installed.
- Critical Note:** CM SSP #15 **must** be installed after applying the 10.1.0.1 or later Service Pack to ensure robust security protection. Reference **PCN2133S** for additional details on the mandatory CM 10.1.0.1 Service Pack and subsequent Service Packs/Feature Packs.
- Installation of CM 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.
- Beginning with CM 10.1.3 which launched May 22, 2023, the following methods are supported for installation of CM 10.1 SSPs. Prior to CM 10.1.3, only the CM Command Line Interface (CLI) was supported for installation of CM 10.1 SSPs.
 - xix. Solution Deployment Manager (SDM)
 - xx. CM System Management Interface (SMI)
 - xxi. CM Command Line Interface (CLI)

Additional information can be found in Appendix C of [Upgrading Avaya Aura® Communication Manager](#).

17 July 2023 – Supplement 15 of this PCN introduces Avaya Aura® Communication Manager (CM) 10.1 Security Service Pack #14

(AV-CM10.1-RHEL8.4-SSP-014-01.tar.bz2; PLDS ID CM000002027)

- CM 10.1 security updates (both Linux and Kernel) are now provided in a Security Service Pack (SSP). There will no longer be a separate Kernel Service Pack (KSP).
- CM SSP #14 is only applicable to CM 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later Service Pack/Feature Pack or on 10.1.0.1 or later Service Pack/Feature Pack that has an earlier SSP installed.
- Critical Note:** CM SSP #14 **must** be installed after applying the 10.1.0.1 or later Service Pack to ensure robust security protection. Reference **PCN2133S** for additional details on the mandatory CM 10.1.0.1 Service Pack and subsequent Service Packs/Feature Packs.
- Installation of CM 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.
- Beginning with CM 10.1.3 which launched May 22, 2023, the following methods are supported for installation of CM 10.1 SSPs. Prior to CM 10.1.3, only the CM Command Line Interface (CLI) was supported for installation of CM 10.1 SSPs.
 - xxii. Solution Deployment Manager (SDM)
 - xxiii. CM System Management Interface (SMI)
 - xxiv. CM Command Line Interface (CLI)

Additional information can be found in Appendix C of [Upgrading Avaya Aura® Communication Manager](#).

20 June 2023 – Supplement 14 of this PCN introduces Avaya Aura® Communication Manager (CM) 10.1 Security Service Pack #13

(AV-CM10.1-RHEL8.4-SSP-013-01.tar.bz2; PLDS ID CM000002026)

- CM 10.1 security updates (both Linux and Kernel) are now provided in a Security Service Pack (SSP). There will no longer be a separate Kernel Service Pack (KSP).
- CM SSP #13 is only applicable to CM 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later Service Pack/Feature Pack or on 10.1.0.1 or later Service Pack/Feature Pack that has an earlier SSP installed.
- **Critical Note:** CM SSP #13 **must** be installed after applying the 10.1.0.1 or later Service Pack to ensure robust security protection. Reference **PCN2133S** for additional details on the mandatory CM 10.1.0.1 Service Pack and subsequent Service Packs/Feature Packs.
- Installation of CM 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.
- Beginning with CM 10.1.3 which launches May 22, 2023, the following methods are supported for installation of CM 10.1 SSPs. Prior to CM 10.1.3, only the CM Command Line Interface (CLI) was supported for installation of CM 10.1 SSPs.
 - xxv. Solution Deployment Manager (SDM)
 - xxvi. CM System Management Interface (SMI)
 - xxvii. CM Command Line Interface (CLI)

Additional information can be found in Appendix C of [Upgrading Avaya Aura® Communication Manager](#).

22 May 2023 – Supplement 13 of this PCN introduces Avaya Aura® Communication Manager (CM) 10.1 Security Service Pack #12

(AV-CM10.1-RHEL8.4-SSP-012-06.tar.bz2; PLDS ID CM000002023)

- CM 10.1 security updates (both Linux and Kernel) are now provided in a Security Service Pack (SSP). There will no longer be a separate Kernel Service Pack (KSP).
- CM SSP #12 is only applicable to CM 10.1.0.1 or later. It can be installed directly on 10.1.0.1

or later Service Pack/Feature Pack or on 10.1.0.1 or later Service Pack/Feature Pack that has an earlier SSP installed.

- **Critical Note:** CM SSP #12 **must** be installed after applying the 10.1.0.1 or later Service Pack to ensure robust security protection. Reference **PCN2133S** for additional details on the mandatory CM 10.1.0.1 Service Pack and subsequent Service Packs/Feature Packs.
- Installation of CM 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
- Beginning with CM 10.1.3 which launches May 22, 2023, the following methods are supported for installation of CM 10.1 SSPs. Prior to CM 10.1.3, only the CM Command Line Interface (CLI) was supported for installation of CM 10.1 SSPs.
 - xxviii. Solution Deployment Manager (SDM)
 - xxix. CM System Management Interface (SMI)
 - xxx. CM Command Line Interface (CLI)

Additional information can be found in Appendix C of [Upgrading Avaya Aura® Communication Manager](#).

17 April 2023 – Supplement 12 of this PCN introduces **Avaya Aura® Communication Manager (CM) 10.1 Security Service Pack #11**

(AV-CM10.1-RHEL8.4-SSP-011-01.tar.bz2; PLDS ID CM000002021)

- CM 10.1 security updates (both Linux and Kernel) are now provided in a Security Service Pack (SSP). There will no longer be a separate Kernel Service Pack (KSP).
- CM SSP #11 is only applicable to CM 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later Service Pack/Feature Pack or on 10.1.0.1 or later Service Pack/Feature Pack that has an earlier SSP installed.
- **Critical Note:** CM SSP #11 **must** be installed after applying the 10.1.0.1 or later Service Pack to ensure robust security protection. Reference **PCN2133S** for additional details on the mandatory CM 10.1.0.1 Service Pack and subsequent Service Packs/Feature Packs.
- Installation of CM 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

20 March 2023 – Supplement 11 of this PCN introduces **Avaya Aura® Communication Manager (CM) 10.1 Security Service Pack #10**

(AV-CM10.1-RHEL8.4-SSP-010-99.tar.bz2; PLDS ID CM000002020)

- CM 10.1 security updates (both Linux and Kernel) are now provided in a Security Service Pack (SSP). There will no longer be a separate Kernel Service Pack (KSP).
- CM SSP #10 is only applicable to CM 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later Service Pack or on 10.1.0.1 or later Service Pack that has an earlier SSP installed.
- **Critical Note:** CM SSP #10 **must** be installed after applying the 10.1.0.1 or later Service Pack to ensure robust security protection. Reference **PCN2133S** for additional details on the

mandatory CM 10.1.0.1 Service Pack and subsequent Service Packs.

- Installation of CM 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
- 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.

23 January 2023 – Supplement 10 of this PCN announces that the January 2023 release of Avaya Aura® 10.1 Security Service Packs did not require an update for Avaya Aura® Communication Manager (CM). CM 10.1 Security Service Pack #9 should continue to be used.

19 December 2022 – Supplement 9 of this PCN introduces **Avaya Aura® Communication Manager (CM) 10.1 Security Service Pack #9**

(AV-CM10.1-RHEL8.4-SSP-009-03.tar.bz2; PLDS ID CM000002016)

- CM 10.1 security updates (both Linux and Kernel) are now provided in a Security Service Pack (SSP). There will no longer be a separate Kernel Service Pack (KSP).
- CM SSP #9 is only applicable to CM 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later Service Pack or on 10.1.0.1 or later Service Pack that has an earlier SSP installed.
- **Critical Note:** CM SSP #9 **must** be installed after applying the 10.1.0.1 or later Service Pack to ensure robust security protection. Reference **PCN2133S** for additional details on the mandatory CM 10.1.0.1 Service Pack and subsequent Service Packs.
- Installation of CM 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 8 of this PCN introduces **Avaya Aura® Communication Manager (CM) 10.1 Security Service Pack #8**

(AV-CM10.1-RHEL8.4-SSP-008-01.tar.bz2; PLDS ID CM000002015)

- CM 10.1 security updates (both Linux and Kernel) are now provided in a Security Service Pack (SSP). There will no longer be a separate Kernel Service Pack (KSP).
- CM SSP #8 is only applicable to CM 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later Service Pack or on 10.1.0.1 or later Service Pack that has an earlier SSP installed.
- **Critical Note:** CM SSP #8 **must** be installed after applying the 10.1.0.1 or later Service Pack to ensure robust security protection. Reference **PCN2133S** for additional details on the mandatory CM 10.1.0.1 Service Pack and subsequent Service Packs.
- Installation of CM 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.
- Reference the ***"Security Information"*** section of this PCN for updates to the rpm and RHSAs for SSP #8.

17 October 2022 – Supplement 7 of this PCN introduces **Avaya Aura® Communication Manager (CM) 10.1 Security Service Pack #7**

(AV-CM10.1-RHEL8.4-SSP-007-01.tar.bz2; PLDS ID CM000002014)

- CM 10.1 security updates (both Linux and Kernel) are now provided in a Security Service Pack (SSP). There will no longer be a separate Kernel Service Pack (KSP).
- CM SSP #7 is only applicable to CM 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later Service Pack or on 10.1.0.1 or later Service Pack that has an earlier SSP installed.
- **Critical Note:** CM SSP #7 **must** be installed after applying the 10.1.0.1 or later Service Pack to ensure robust security protection. Reference **PCN2133S** for additional details on the mandatory CM 10.1.0.1 Service Pack and subsequent Service Packs.
- Installation of CM 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 6 of this PCN introduces **Avaya Aura® Communication Manager (CM) 10.1 Security Service Pack #6**

(AV-CM10.1-RHEL8.4-SSP-006-01.tar.bz2; PLDS ID CM000002013)

- CM 10.1 security updates (both Linux and Kernel) are now provided in a Security Service Pack (SSP). There will no longer be a separate Kernel Service Pack (KSP).
- CM SSP #6 is only applicable to CM 10.1.0.1 or later. It can be installed directly on 10.1.0.1 or later Service Pack or on 10.1.0.1 or later Service Pack that has an earlier SSP installed.
- **Critical Note:** CM SSP #6 **must** be installed after applying the 10.1.0.1 or later Service Pack to ensure robust security protection. Reference **PCN2133S** for additional details on the mandatory CM 10.1.0.1 Service Pack and subsequent Service Packs.
- Installation of CM 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 5 of this PCN introduces **Avaya Aura® Communication Manager (CM) 10.1 Security Service Pack #5**

(AV-CM10.1-RHEL8.4-SSP-005-02.tar.bz2; PLDS ID CM000002011)

- CM 10.1 security updates (both Linux and Kernel) are now provided in a Security Service Pack (SSP). There will no longer be a separate Kernel Service Pack (KSP).
- CM SSP #5 is only applicable to CM 10.1.0.1. It can be installed directly on 10.1.0.1 or on 10.1.0.1 that has an earlier SSP installed.
- **Critical Note:** CM SSP #5 **must** be installed after applying the 10.1.0.1 Service Pack to ensure robust security protection. Reference **PCN2133S** for additional details on the mandatory CM 10.1.0.1. Service Pack.
- Installation of CM SSP #5 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.

22 July 2022 – Supplement 4 of this PCN introduces **Avaya Aura® Communication Manager (CM)**

10.1 Security Service Pack #4

(AV-CM10.1-RHEL8.4-SSP-004-02.tar.bz2; PLDS ID CM000002010)

- CM 10.1 security updates (both Linux and Kernel) are now provided in a Security Service Pack (SSP). There will no longer be a separate Kernel Service Pack (KSP).
- CM SSP #4 is only applicable to CM 10.1.0.1. It can be installed directly on 10.1.0.1 or on 10.1.0.1 that has an earlier SSP installed.
- **Critical Note:** CM SSP #4 **must** be installed after applying the 10.1.0.1 Service Pack to ensure robust security protection. Reference **PCN2133S** for additional details on the mandatory CM 10.1.0.1. Service Pack.
- Installation of CM 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.

21 June 2022 – Supplement 3 of this PCN introduces **Avaya Aura® Communication Manager (CM)**

10.1 Security Service Pack #3

(AV-CM10.1-RHEL8.4-SSP-003-03.tar.bz2; PLDS ID CM000002009)

- CM 10.1 security updates (both Linux and Kernel) are now provided in a Security Service Pack (SSP). There will no longer be a separate Kernel Service Pack (KSP).
- CM SSP #3 is only applicable to CM 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:** CM SSP #3 **must** be installed after applying the 10.1.0.1 Service Pack to ensure robust security protection. Reference **PCN2133S** for additional details on the mandatory CM 10.1.0.1. Service Pack.
- Installation of CM 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.

16 May 2022 – Supplement 2 of this PCN introduces **Avaya Aura® Communication Manager (CM)**

10.1 Security Service Pack #2

(AV-CM10.1-RHEL8.4-SSP-002-01.tar.bz2; PLDS ID CM000002008)

- CM 10.1 security updates (both Linux and Kernel) are now provided in a Security Service Pack (SSP). There will no longer be a separate Kernel Service Pack (KSP).
- CM SSP #2 is only applicable to CM 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:** CM SSP #2 **must** be installed after applying the 10.1.0.1 Service Pack to ensure robust security protection. Reference **PCN2133S** for additional details on the mandatory CM 10.1.0.1. Service Pack.
- Installation of CM 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.

22 April 2022 – Supplement 1 of this PCN provides updates to *Section 1B - Security Information*. The original list of rpm updates and security vulnerabilities addressed in Security Service Pack #1 was not complete. The tables have been updated to include all security updates delivered into Security

Service Pack #1.

18 April 2022 – This PCN introduces **Avaya Aura® Communication Manager (CM) 10.1 Security Service Pack #1**

(AV-CM10.1-RHEL8.4-SSP-001-01.tar.bz2; PLDS ID CM000002007)

- CM 10.1 security updates (both Linux and Kernel) are now provided in a Security Service Pack (SSP). There will no longer be a separate Kernel Service Pack (KSP).
- CM SSP #1 is only applicable to CM 10.1.0.1.
- **Critical Note:** CM SSP #1 **must** be installed after applying the 10.1.0.1 Service Pack to ensure robust security protection. Reference **PCN2133S** for additional details on the mandatory CM 10.1.0.1. Service Pack.
- Installation of CM 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 Communication Manager 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 during installation?

Activation of the Security Service Pack will disrupt service since it requires a full Linux reboot of the Communication Manager Virtual Machine (VM) to take effect.

Installation of this PCN is required by:

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

**Release notes
and
workarounds
are located:**

The **Security Service Pack** 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® Communication Manager Release 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 **Communication Manager** and when Avaya Aura® Communication Manager 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
implement this
PCN
(If PCN can be
customer
installed):**

This PCN is being issued as a customer installable PCN. The specified Communication Manager files are required. To obtain the update files refer to the **How do I order this PCN** section of this PCN.

If unfamiliar with installing Communication Manager 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 **Communication Manager** and when Avaya Aura® Communication Manager 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® Communication Manager 10.1.x Security Service Pack**.
7. Scroll down the page to find the download link for the required Security Service Pack. This link will take you to the PLDS system with the **Download pub ID** already entered.
8. Select the **Download** link in PLDS to begin the download.

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

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

PLDS Hints:

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

Important Security Service Pack Installation Notes:

2. The SSP update process will utilize the new Common framework that replaces the historic “*update_unpack*”, “*update_activate*” commands with a new “*av-update-os*” command for installation and new “*av-version*” command that will show the SSP version currently running on

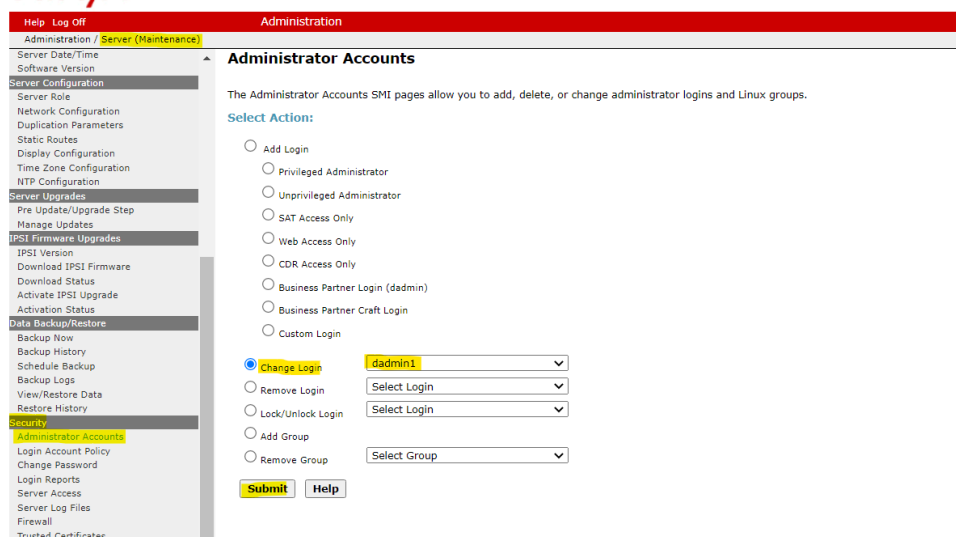
CM.

3. Prior to CM 10.1.3, installing CM 10.1 SSPs through Solution Deployment Manager (SDM) or through the CM SMI was not supported. Only the CLI could be used to install CM SSPs. Beginning with CM 10.1.3, the following methods are supported for installation of CM 10.1 SSPs:
 - a. Solution Deployment Manager (SDM)
 - b. CM System Management Interface (SMI)
 - c. CM Command Line Interface (CLI)

Additional information can be found in Appendix C of [Upgrading Avaya Aura® Communication Manager](#).
4. 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.
5. Security Service Packs are independent of other Communication Manager software updates activated on a server including CM Service Packs, over-writable patches or custom patches. None of these other software updates should be deactivated before installing a Security Service Pack.
6. SSPs should NOT be installed on Communication Manager 10.1.x Software Only deployments.
7. 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.
8. The following have default permission to install a CM SSP: root, sroot and other services logins. These logins are part of the new “avcommonos” group which is a requirement to install a CM SSPs.
9. CM customer logins must be part of the “avcommonos” group in order to install a CM SSP. To add a customer login to the “avcommonos” group, follow these instructions.

Execute the following instructions to add a user to the “avcommonos” group

1. Login to the CM SMI with the customer login, in this example, “dadmin1” which was created during the initial CM OVA deployment.
2. Navigate to **Server (Maintenance)→Security→Administrator Accounts**
3. Select **“Change Login”** and select the customer login you want to modify, in this case “dadmin1”.

4. Select **“Submit”** to advance to the **“Administrator Accounts – Change Login”** page.
5. Select **“Additional groups (profile)”** and add the group **“avcommonos”** (comma

separated from first group).



Help Log Off Administration

Administration / Server (Maintenance)

Server Date/Time
Software Version

Server Configuration

Server Role
Network Configuration
Duplication Parameters
Static Routes
Display Configuration
Time Zone Configuration
NTP Configuration

Server Upgrades

Pre Update/Upgrade Step
Manage Updates

IPSI Firmware Upgrades

IPSI Version
Download IPSI Firmware
Download Status
Activate IPSI Upgrade
Activation Status

Data Backup/Restore

Backup Now
Backup History
Schedule Backup
Backup Logs
View/Restore Data
Restore History

Security

Administrator Accounts
Login Account Policy
Change Password
Login Reports
Server Access
Server Log Files
Firewall
Trusted Certificates
Server/Application Certificates
Certificate Alarms
Certificate Signing Request
SSH Keys

Administrator Accounts -- Change Login

This page allows you to edit an administrator login.

Click to Change

Login name: dadmin1

☐ Primary group: susers

☒ Additional groups (profile): prof18,avcommonos

☐ Linux shell (/sbin/nologin for no shell): /bin/bash

Home directory: /var/home/dadmin1

☐ Lock this account: ☐

☐ SAT Limit: none

☐ Date after which account is disabled-blank to ignore (YYYY-MM-DD):

☐ Enter password:

Re-enter password:

Force password change on next login: ☐ Yes ☒ No

The user will **not** be forced to change the password on next login. To enable this behavior, enter a new password and select the Yes option.

Submit Cancel Help

6. Select "Submit".

7. Ensure that the modification is successful



Help Log Off Administration

Administration / Server (Maintenance)

Server Date/Time
Software Version

Server Configuration

Server Role
Network Configuration
Duplication Parameters
Static Routes
Display Configuration
Time Zone Configuration
NTP Configuration

Server Upgrades

Administrator Accounts -- Change Login

This page allows you to edit an administrator login.

Login dadmin1 was modified successfully.

Continue Help

8. Select "Continue" to return to the **Administrator Accounts** page and then Log Off the system.

Execute the following instructions to apply the CM Security Service Pack

Examples below are for CM 10.1 SSP #1 utilizing the Command Line Interface (CLI). Additional information for all methods of deployment (CLI, SDM, SMI) can be found in Appendix C of [Upgrading](#)

Avaya Aura® Communication Manager.

For a Duplicated CM system, perform the required “Pre update/Upgrade Step” on the ACTIVE server, busy out the standby server, install SSP on standby, then release standby, interchange, perform same steps on new standby.

1. Ensure that a maintenance window has been obtained as application of the SSP will result in a reboot.
2. Ensure that CM Service Pack #1 (10.1.0.1) is installed.
01.0.974.0-27372 **activated** cold 10.1.0.1.0-SP1
3. Download the SSP from PLDS and copy to /var/home/ftp/pub on CM.
4. Perform a backup of the CM application.
5. Perform a snapshot of the CM VM. Follow instructions for performing snapshots as noted in [Deploying Avaya Aura® Communication Manager in Virtualized Environment](#).
6. Login to the CM CLI utilizing customer account (need to ensure customer account has been associated with the “avcommonos” group as noted above), root, sroot, or other services logins credentials.
7. Change directory to /var/home/ftp/pub
8. Ensure the MD5sum matches what is provided in the PLDS Download ID description.

```
dadmin1@cm-cm101adupb> md5sum AV-CM10.1-RHEL8.4-SSP-001-01.tar.bz2
023ea6ae26bea1e2017eb03df269e443 AV-CM10.1-RHEL8.4-SSP-001-01.tar.bz2
```

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-CM10.1-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

Partial sample output below:

```
[root@cm-cm101adupb]# av-update-os AV-CM10.1-RHEL8.4-SSP-001-01.tar.bz2
17-Apr-2022 11:04:32: Log file: /var/log/avaya/SSP001.log-20220417110432
17-Apr-2022 11:04:32: Properties file: /opt/avaya/common-os/etc/os-
patch.properties
17-Apr-2022 11:04:32: Release file: /etc/avaya-release
17-Apr-2022 11:04:40: os-patch.properties file is present in the bundle
17-Apr-2022 11:04:49: Received SSP version: 001, received product name:
CM10.1, received build number: 01
17-Apr-2022 11:04:49: Certificate file: /opt/ws/apr-ca.crt
17-Apr-2022 11:04:49: Base directory: /tmp/CM10.1
17-Apr-2022 11:04:57: Available size before tar bundle in KB: 5162912, bundle
size in KB: 140288
/tmp/CM10.1/rpms/RootSA.txt: OK
Version: 3 (0x2)
Verified OK
```

```

17-Apr-2022 11:05:06: Avaya signing and checksum is correct
17-Apr-2022 11:05:06: Removing older properties file: /opt/avaya/common-
os/etc/os-patch.properties
17-Apr-2022 11:05:06: Property file copied from the bundle
17-Apr-2022 11:05:11: Size of installed RPMs: 169167994, required size of
RPMs: 190576132, required free space in KB: 20907
17-Apr-2022 11:05:11: Available size in KB after tar bundle: 5021796, required
space in KB: 20907
17-Apr-2022 11:05:11: We are updating the RPMs, please wait
Verifying... #####
Preparing... #####
Updating / installing...
  openssl-libs-1:1.1.1k-5.el8_5 #####
  nss-util-3.67.0-7.el8_5 #####
  libgcc-8.5.0-4.el8_5 #####

```

Additional packages will be listed.

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

```

17-Apr-2022 11:06:55: 001 SSP version updated successfully in file /etc/avaya-
release
17-Apr-2022 11:06:55: New SSP version 001 and build number 01 updated
successfully
17-Apr-2022 11:06:55: Reboot flag is set to yes in properties file, rebooting
system
Shutdown scheduled for Sun 2022-04-17 11:07:55 MDT, use 'shutdown -c' to
cancel.

Broadcast message from root@cm-cm101adupb (somewhere) (Sun Apr 17 11:08:08 2
Communication Manager has been shut down on this server.

```

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 CM 10.1 SSP #1.

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

```

[root@cm-cm101adupb]# 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. When using the “swversion” command, the status of the SSP will always be blank.

```

[root@cm-cm101adupb]# swversion
Operating system: Linux 4.18.0-348.20.1.el8_5.x86_64 x86_64
Built: Mar 8 12:56 2022

Contains: 01.0.974.0
CM Reports as: R020x.01.0.974.0

```

```

CM Release String: vcm-020-01.0.974.0
RTS Version: CM 10.1.0.1.0.974.27372
Publication Date: 11 October 2021
VMwaretools version: 11.2.0.23855 (build-16938113)
App Deployment: Virtual Machine
VM Environment: VMware

```

UPDATES:

Update ID	Status	Type	Update description
01.0.974.0-27293	unpacked	cold	CM10.1.0.0.0-SP0.1 Cold Pat
01.0.974.0-27372	activated	cold	10.1.0.1.0-SP1

Platform/Security ID	Status	Type	Update description
AV-CM10.1-RHEL8.4-SSP001			RHEL8.4-SSP001

```

CM Translation Saved: 2022-04-16 09:58:56

```

```

CM License Installed: 2022-04-17 11:09:19

```

```

CM Memory Config: Large

```

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

What you should do if the Service Pack installation fails?

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

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

Security Service Packs cannot be deactivated.

SECTION 1B – SECURITY INFORMATION

Are there any security risks involved?

Issues described by the RHSAs listed in the next section are corrected by the Security Service Pack as noted. Security Service Packs (SSPs) include the fixes from all previous SSPs respectively for a given CM 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.

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

buildah-1.31.3-3.module+el8.9.0+21243+a586538b.x86_64.rpm conmon-2.1.8-1.module+el8.9.0+21243+a586538b.x86_64.rpm containernetworking-plugins-1.3.0-8.module+el8.9.0+21243+a586538b.x86_64.rpm container-selinux-2.221.0-1.module+el8.9.0+21243+a586538b.noarch.rpm criu-3.18-4.module+el8.9.0+21243+a586538b.x86_64.rpm fuse-overlayfs-1.12-1.module+el8.9.0+21243+a586538b.x86_64.rpm gnutls-3.6.16-8.el8_9.i686.rpm gnutls-3.6.16-8.el8_9.x86_64.rpm kernel-4.18.0-513.18.1.el8_9.x86_64.rpm kernel-core-4.18.0-513.18.1.el8_9.x86_64.rpm kernel-devel-4.18.0-513.18.1.el8_9.x86_64.rpm kernel-headers-4.18.0-513.18.1.el8_9.x86_64.rpm kernel-modules-4.18.0-513.18.1.el8_9.x86_64.rpm kernel-tools-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 libmaxminddb-1.2.0-10.el8_9.1.x86_64.rpm libslirp-4.4.0-1.module+el8.9.0+21243+a586538b.x86_64.rpm libssh-0.9.6-13.el8_9.x86_64.rpm libssh-config-0.9.6-13.el8_9.noarch.rpm libxml2-2.9.7-18.el8_9.i686.rpm libxml2-2.9.7-18.el8_9.x86_64.rpm nss-3.90.0-6.el8_9.x86_64.rpm nss-softokn-3.90.0-6.el8_9.i686.rpm nss-softokn-3.90.0-6.el8_9.x86_64.rpm nss-softokn-freebl-3.90.0-6.el8_9.i686.rpm nss-softokn-freebl-3.90.0-6.el8_9.x86_64.rpm nss-sysinit-3.90.0-6.el8_9.x86_64.rpm nss-util-3.90.0-6.el8_9.i686.rpm nss-util-3.90.0-6.el8_9.x86_64.rpm oniguruma-6.8.2-1.el8_9.x86_64.rpm	openssh-8.0p1-19.el8_9.2.x86_64.rpm openssh-clients-8.0p1-19.el8_9.2.x86_64.rpm openssh-server-8.0p1-19.el8_9.2.x86_64.rpm openssl-1.1.1k-12.el8_9.x86_64.rpm openssl-libs-1.1.1k-12.el8_9.i686.rpm openssl-libs-1.1.1k-12.el8_9.x86_64.rpm pixman-0.38.4-3.el8_9.x86_64.rpm platform-python-3.6.8-56.el8_9.3.i686.rpm platform-python-3.6.8-56.el8_9.3.x86_64.rpm podman-4.6.1-8.module+el8.9.0+21243+a586538b.x86_64.rpm podman-catatonit-4.6.1-8.module+el8.9.0+21243+a586538b.x86_64.rpm python3-libs-3.6.8-56.el8_9.3.i686.rpm python3-libs-3.6.8-56.el8_9.3.x86_64.rpm python3-libxml2-2.9.7-18.el8_9.x86_64.rpm python3-perf-4.18.0-513.18.1.el8_9.x86_64.rpm python3-rpm-4.14.3-28.el8_9.x86_64.rpm python3-urllib3-1.24.2-5.el8_9.2.noarch.rpm qemu-guest-agent-6.2.0-40.module+el8.9.0+20867+9a6a0901.2.x86_64.rpm rpm-4.14.3-28.el8_9.x86_64.rpm rpm-build-libs-4.14.3-28.el8_9.x86_64.rpm rpm-libs-4.14.3-28.el8_9.x86_64.rpm rpm-plugin-selinux-4.14.3-28.el8_9.x86_64.rpm rpm-plugin-systemd-inhibit-4.14.3-28.el8_9.x86_64.rpm runc-1.1.12-1.module+el8.9.0+21243+a586538b.x86_64.rpm slirp4netns-1.2.1-1.module+el8.9.0+21243+a586538b.x86_64.rpm sqlite-3.26.0-19.el8_9.x86_64.rpm sqlite-libs-3.26.0-19.el8_9.i686.rpm sqlite-libs-3.26.0-19.el8_9.x86_64.rpm sudo-1.9.5p2-1.el8_9.x86_64.rpm tzdata-2024a-1.el8.noarch
---	--

Security vulnerabilities resolved in CM 10.1 Security Service Pack #21***Delivered under Fix Id CM-55938***

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity
openssl openssl-libs openssl-libs	RHSA-2023:7877	CVE-2023-3446 CVE-2023-3817 CVE-2023-5678	Low
python3-urllib3	RHSA-2024:0116	CVE-2023-43804 CVE-2023-45803	Moderate
libxml2 libxml2 python3-libxml2	RHSA-2024:0119	CVE-2023-39615	Moderate
pixman	RHSA-2024:0131	CVE-2022-44638	Moderate
qemu-guest-agent	RHSA-2024:0135	CVE-2023-3019	Moderate

sqlite sqlite-libs sqlite-libs	RHSA-2024:0253	CVE-2023-7104	Moderate
platform-python platform-python python3-libs python3-libs	RHSA-2024:0256	CVE-2023-27043	Moderate
openssh openssh-clients openssh-server	RHSA-2024:0606	CVE-2023-48795 CVE-2023-51385	Moderate
gnutls gnutls	RHSA-2024:0627	CVE-2024-0553	Moderate
libssh libssh-config	RHSA-2024:0628	CVE-2023-48795	Moderate
python3-rpm rpm rpm-build-libs rpm-libs rpm-plugin-selinux rpm-plugin-systemd-inhibit	RHSA-2024:0647	CVE-2021-35937 CVE-2021-35938 CVE-2021-35939	Moderate
buildah common container-selinux containernetworking-plugins criu fuse-overlayfs libslirp podman podman-catatonit runc slirp4netns	RHSA-2024:0752	CVE-2024-21626	Important
libmaxminddb	RHSA-2024:0768	CVE-2020-28241	Moderate
libmaxminddb	RHSA-2024:0768	CVE-2020-28241	Moderate
nss nss-softokn nss-softokn nss-softokn-freebl nss-softokn-freebl nss-sysinit nss-util nss-util	RHSA-2024:0786	CVE-2023-6135	Moderate
oniguruma	RHSA-2024:0889	CVE-2019-13224 CVE-2019-16163 CVE-2019-19012	Moderate

		CVE-2019-19203 CVE-2019-19204	
oniguruma	RHSA-2024:0889	CVE-2019-13224 CVE-2019-16163 CVE-2019-19012 CVE-2019-19203 CVE-2019-19204	Moderate
kernel kernel-core kernel-devel 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
tzdata	RHBA-2024:0762	NA	bugfix

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

avahi-libs-0.7-21.el8_9.1.x86_64.rpm gstreamer1-plugins-bad-free-1.16.1-2.el8_9.x86_64.rpm kernel-4.18.0-513.9.1.el8_9.x86_64.rpm kernel-core-4.18.0-513.9.1.el8_9.x86_64.rpm kernel-devel-4.18.0-513.9.1.el8_9.x86_64.rpm	kernel-headers-4.18.0-513.9.1.el8_9.x86_64.rpm kernel-modules-4.18.0-513.9.1.el8_9.x86_64.rpm kernel-tools-4.18.0-513.9.1.el8_9.x86_64.rpm kernel-tools-libs-4.18.0-513.9.1.el8_9.x86_64.rpm python3-perf-4.18.0-513.9.1.el8_9.x86_64.rpm
--	---

Security vulnerabilities resolved in CM 10.1 Security Service Pack #20
Delivered under Fix Id CM-55399

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
kernel kernel-core kernel-devel kernel-headers kernel-modules kernel-tools	RHSA-2023:7549	CVE-2022-45884 CVE-2022-45886 CVE-2022-45919 CVE-2023-1192 CVE-2023-2163 CVE-2023-3812	Important	NA	NA

kernel-tools-libs python3-perf		CVE-2023-5178			
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
gststreamer1-plugins-bad-free	RHSA-2023:7841	CVE-2023-44446	Important	NA	NA

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

avahi-libs-0.7-21.el8.x86_64.rpm bind-export-libs-9.11.36-11.el8_9.x86_64.rpm bind-libs-9.11.36-11.el8_9.x86_64.rpm bind-libs-lite-9.11.36-11.el8_9.x86_64.rpm bind-license-9.11.36-11.el8_9.noarch.rpm bind-utils-9.11.36-11.el8_9.x86_64.rpm binutils-2.30-119.el8_8.2.x86_64.rpm buildah-1.31.3-1.module+el8.9.0+19761+326da906.x86_64.rpm c-ares-1.13.0-8.el8.x86_64.rpm c-ares-1.13.0-9.el8_9.1.x86_64.rpm common-2.1.8-1.module+el8.9.0+19761+326da906.x86_64.rpm containernetworking-plugins-1.3.0-4.module+el8.9.0+19649+5879504a.x86_64.rpm container-selinux-2.221.0-1.module+el8.9.0+19685+019f3589.noarch.rpm criu-3.18-4.module+el8.9.0+19090+d2921118.x86_64.rpm cups-libs-2.2.6-54.el8_9.x86_64.rpm emacs-filesystem-26.1-11.el8.noarch.rpm fuse-overlayfs-1.12-1.module+el8.9.0+19090+d2921118.x86_64.rpm fwupd-1.7.8-2.el8.x86_64.rpm kernel-4.18.0-513.5.1.el8_9.x86_64.rpm kernel-core-4.18.0-513.5.1.el8_9.x86_64.rpm kernel-devel-4.18.0-513.5.1.el8_9.x86_64.rpm kernel-headers-4.18.0-513.5.1.el8_9.x86_64.rpm kernel-modules-4.18.0-513.5.1.el8_9.x86_64.rpm	kernel-tools-4.18.0-513.5.1.el8_9.x86_64.rpm kernel-tools-libs-4.18.0-513.5.1.el8_9.x86_64.rpm libfastjson-0.99.9-2.el8.x86_64.rpm libslirp-4.4.0-1.module+el8.9.0+19244+655f84ee.x86_64.rpm libX11-1.6.8-6.el8.x86_64.rpm libX11-common-1.6.8-6.el8.noarch.rpm libX11-xcb-1.6.8-6.el8.x86_64.rpm linux-firmware-20230824-119.git0e048b06.el8_9.noarch.rpm open-vm-tools-12.2.5-3.el8_9.1.x86_64.rpm perl-HTTP-Tiny-0.074-2.el8.noarch.rpm platform-python-3.6.8-51.el8_8.2.i686.rpm platform-python-3.6.8-51.el8_8.2.x86_64.rpm platform-python-3.6.8-56.el8_9.i686.rpm platform-python-3.6.8-56.el8_9.x86_64.rpm platform-python-pip-9.0.3-23.el8.noarch.rpm podman-4.6.1-4.module+el8.9.0+19761+326da906.x86_64.rpm podman-catatonit-4.6.1-4.module+el8.9.0+19761+326da906.x86_64.rpm procps-ng-3.3.15-14.el8.x86_64.rpm protobuf-c-1.3.0-8.el8.x86_64.rpm python2-2.7.18-13.module+el8.8.0+20144+beed974d.2.x86_64.rpm python2-2.7.18-15.module+el8.9.0+20125+68111a8f.x86_64.rpm python2-libs-2.7.18-13.module+el8.8.0+20144+beed974d.2.x86_64.rpm python2-libs-2.7.18-15.module+el8.9.0+20125+68111a8f.x86_64.rpm
--	---

Security vulnerabilities resolved in CM 10.1 Security Service Pack #19
Delivered under Fix Id CM-55303

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
python2 python2-libs python2-pip python2-pip-wheel	RHSA-2023:5994	CVE-2023-40217	Important	NA	NA
platform-python platform-python python3-libs	RHSA-2023:5997	CVE-2023-40217	Important	NA	NA

python3-libs					
binutils	RHSA-2023:6236	CVE-2022-4285	Moderate	NA	NA
buildah common container-selinux containernetworking-plugins criu fuse-overlayfs libslirp podman podman-catatonit runc slirp4netns	RHSA-2023:6939	CVE-2022-3064 CVE-2022-41723 CVE-2022-41724 CVE-2022-41725 CVE-2023-24534 CVE-2023-24536 CVE-2023-24537 CVE-2023-24538 CVE-2023-24539 CVE-2023-24540 CVE-2023-25173 CVE-2023-25809 CVE-2023-27561 CVE-2023-28642 CVE-2023-29400 CVE-2023-29406 CVE-2023-3978	Moderate	NA	NA
protobuf-c	RHSA-2023:6944	CVE-2022-48468	Moderate	NA	NA
qt5-qtbase qt5-qtbase-common qt5-qtbase-gui	RHSA-2023:6967	CVE-2023-33285 CVE-2023-34410 CVE-2023-37369 CVE-2023-38197	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
wireshark wireshark-cli	RHSA-2023:7015	CVE-2023-0666 CVE-2023-2856 CVE-2023-2858 CVE-2023-2952	Moderate	NA	NA
libX11 libX11-common libX11-xcb	RHSA-2023:7029	CVE-2023-3138	Moderate	NA	NA
python2 python2-libs python2-pip python2-pip-wheel python2-setuptools python2-setuptools-wheel	RHSA-2023:7042	CVE-2023-32681	Moderate	NA	NA
kernel kernel-core	RHSA-2023:7077	CVE-2021-43975 CVE-2022-28388	kernel kernel-core	NA	NA

kernel-devel kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf		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	kernel-devel kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf		
emacs-filesystem	RHSA-2023:7083	CVE-2022-48337 CVE-2022-48339	Moderate	NA	NA
python3-cryptography	RHSA-2023:7096	CVE-2023-23931	Moderate	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
platform-python platform-python python3-libs 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
tpm2-tss 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-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

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

bind-export-libs-9.11.36-8.el8_8.2.x86_64.rpm bind-libs-9.11.36-8.el8_8.2.x86_64.rpm bind-libs-lite-9.11.36-8.el8_8.2.x86_64.rpm bind-license-9.11.36-8.el8_8.2.noarch.rpm bind-utils-9.11.36-8.el8_8.2.x86_64.rpm glibc-2.28-225.el8_8.6.i686.rpm glibc-2.28-225.el8_8.6.x86_64.rpm glibc-all-langpacks-2.28-225.el8_8.6.x86_64.rpm glibc-common-2.28-225.el8_8.6.x86_64.rpm glibc-devel-2.28-225.el8_8.6.x86_64.rpm glibc-headers-2.28-225.el8_8.6.x86_64.rpm	glibc-langpack-en-2.28-225.el8_8.6.x86_64.rpm libnghttp2-1.33.0-5.el8_8.x86_64.rpm libnsl-2.28-225.el8_8.6.i686.rpm libnsl-2.28-225.el8_8.6.x86_64.rpm libtiff-4.0.9-29.el8_8.x86_64.rpm libwebp-1.0.0-8.el8_8.1.x86_64.rpm nginxfilesystem-1.20.1-1.module+el8.8.0+20359+9bd89172.1.noarch.rpm nscd-2.28-225.el8_8.6.x86_64.rpm open-vm-tools-12.1.5-2.el8_8.3.x86_64.rpm python3-bind-9.11.36-8.el8_8.2.noarch.rpm
---	---

Security vulnerabilities resolved in CM 10.1 Security Service Pack #18***Delivered under Fix Id CM-55143***

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

libwebp	RHSA-2023-5309	CVE-2023-4863	Important	ASA-2023-134	Critical
open-vm-tools	RHSA-2023-5312	CVE-2023-20900	Important	ASA-2023-122	High
libtiff	RHSA-2023-5353	CVE-2023-0800 CVE-2023-0801 CVE-2023-0802 CVE-2023-0803 CVE-2023-0804	Moderate	ASA-2023-138	Medium
glibc glibc glibc-all-langpacks glibc-common glibc-devel glibc-headers glibc-langpack-en libnsl libnsl 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
ibnhttp2	RHSA-2023-5837	CVE-2023-44487	Important	NA	NA

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

cups-libs-2.2.6-51.el8_8.1.x86_64.rpm dmidecode-3.3-4.el8_8.1.x86_64.rpm flac-libs-1.3.2-9.el8_8.1.x86_64.rpm httpd-2.4.37-56.module+el8.8.0+19808+379766d6.7.x86_64.rpm httpd-filesystem-2.4.37-56.module+el8.8.0+19808+379766d6.7.noarch.rpm httpd-tools-2.4.37-56.module+el8.8.0+19808+379766d6.7.x86_64.rpm kernel-4.18.0-477.27.1.el8_8.x86_64.rpm kernel-core-4.18.0-477.27.1.el8_8.x86_64.rpm kernel-devel-4.18.0-477.27.1.el8_8.x86_64.rpm kernel-headers-4.18.0-477.27.1.el8_8.x86_64.rpm kernel-modules-4.18.0-477.27.1.el8_8.x86_64.rpm kernel-tools-4.18.0-477.27.1.el8_8.x86_64.rpm	kernel-tools-libs-4.18.0-477.27.1.el8_8.x86_64.rpm linux-firmware-20230404-117.git2e92a49f.el8_8.noarch.rpm mod_http2-1.15.7-8.module+el8.8.0+18751+b4557bca.3.x86_64.rpm mod_ssl-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 ncurses-base-6.1-9.20180224.el8_8.1.noarch.rpm ncurses-libs-6.1-9.20180224.el8_8.1.i686.rpm ncurses-libs-6.1-9.20180224.el8_8.1.x86_64.rpm python3-perf-4.18.0-477.27.1.el8_8.x86_64.rpm python3-syspurpose-1.28.36-3.el8_8.x86_64.rpm qemu-guest-agent-6.2.0-33.module+el8.8.0+19768+98f68f21.x86_64.rpm
---	--

Security vulnerabilities resolved in CM 10.1 Security Service Pack #17
Delivered under Fix Id CM-55029

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

python3-syspurpose	RHSA-2023-4706	CVE-2023-3899	Important	ASA-2023-114	High
cups-libs	RHSA-2023-4864	CVE-2023-32360	Important	ASA-2023-116	Medium
flac-libs	RHSA-2023-5046	CVE-2020-22219	Important	ASA-2023-117	High
httpd httpd-filesystem httpd-tools mod_http2 mod_ssl	RHSA-2023-5050	CVE-2023-27522	Moderate	ASA-2023-115	High
kernel kernel-core kernel-devel 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 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

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

bind-export-libs-9.11.36-8.el8_8.1.x86_64.rpm bind-libs-9.11.36-8.el8_8.1.x86_64.rpm bind-libs-lite-9.11.36-8.el8_8.1.x86_64.rpm bind-license-9.11.36-8.el8_8.1.noarch.rpm bind-utils-9.11.36-8.el8_8.1.x86_64.rpm curl-7.61.1-30.el8_8.3.x86_64.rpm dbus-1.12.8-24.el8_8.1.x86_64.rpm dbus-common-1.12.8-24.el8_8.1.noarch.rpm dbus-daemon-1.12.8-24.el8_8.1.x86_64.rpm dbus-libs-1.12.8-24.el8_8.1.x86_64.rpm dbus-tools-1.12.8-24.el8_8.1.x86_64.rpm kernel-4.18.0-477.21.1.el8_8.x86_64.rpm kernel-core-4.18.0-477.21.1.el8_8.x86_64.rpm kernel-devel-4.18.0-477.21.1.el8_8.x86_64.rpm kernel-headers-4.18.0-477.21.1.el8_8.x86_64.rpm	kernel-modules-4.18.0-477.21.1.el8_8.x86_64.rpm kernel-tools-4.18.0-477.21.1.el8_8.x86_64.rpm kernel-tools-libs-4.18.0-477.21.1.el8_8.x86_64.rpm libcap-2.48-5.el8_8.i686.rpm libcap-2.48-5.el8_8.x86_64.rpm libcurl-7.61.1-30.el8_8.3.x86_64.rpm libxml2-2.9.7-16.el8_8.i686.rpm libxml2-2.9.7-16.el8_8.1.x86_64.rpm openssh-8.0p1-19.el8_8.x86_64.rpm openssh-clients-8.0p1-19.el8_8.x86_64.rpm openssh-server-8.0p1-19.el8_8.x86_64.rpm python3-bind-9.11.36-8.el8_8.1.noarch.rpm python3-libxml2-2.9.7-16.el8_8.1.x86_64.rpm python3-perf-4.18.0-477.21.1.el8_8.x86_64.rpm python3-requests-2.20.0-3.el8_8.noarch.rpm
--	---

Security vulnerabilities resolved in CM 10.1 Security Service Pack #16
Delivered under Fix Id CM-54888

Updated Package	RHSA Number	Common	RHSA	ASA Number	ASA
-----------------	-------------	--------	------	------------	-----

		Vulnerability and Exposure (CVE) ID	Severity		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
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-devel 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	TBD
python3-requests	RHSA-2023-4520	CVE-2023-32681	Moderate	NA	NA
curl 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 libxml2 python3-libxml2	RHSA-2023-4529	CVE-2023-28484 CVE-2023-29469	Moderate	ASA-2023-097	Medium

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

c-ares-1.13.0-6.el8_8.2.x86_64.rpm kernel-4.18.0-477.15.1.el8_8.x86_64.rpm kernel-core-4.18.0-477.15.1.el8_8.x86_64.rpm kernel-devel-4.18.0-477.15.1.el8_8.x86_64.rpm kernel-headers-4.18.0-477.15.1.el8_8.x86_64.rpm kernel-modules-4.18.0-477.15.1.el8_8.x86_64.rpm kernel-tools-4.18.0-477.15.1.el8_8.x86_64.rpm kernel-tools-libs-4.18.0-477.15.1.el8_8.x86_64.rpm libssh-0.9.6-10.el8_8.x86_64.rpm libssh-config-0.9.6-10.el8_8.noarch.rpm libtiff-4.0.9-28.el8_8.x86_64.rpm open-vm-tools-12.1.5-2.el8_8.x86_64.rpm platform-python-3.6.8-51.el8_8.i686.rpm platform-python-3.6.8-51.el8_8.1.x86_64.rpm python2-2.7.18-13.module+el8.8.0+19042+06909d2c.1.x86_64.rpm	python2-libs-2.7.18-13.module+el8.8.0+19042+06909d2c.1.x86_64.rpm python2-pip-9.0.3-19.module+el8.6.0+13001+ad200bd9.noarch.rpm python2-pip-wheel-9.0.3-19.module+el8.6.0+13001+ad200bd9.noarch.rpm python3-libs-3.6.8-51.el8_8.i686.rpm python3-libs-3.6.8-51.el8_8.1.x86_64.rpm python3-perf-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 sqlite-3.26.0-18.el8_8.x86_64.rpm sqlite-libs-3.26.0-18.el8_8.i686.rpm sqlite-libs-3.26.0-18.el8_8.x86_64.rpm systemd-239-74.el8_8.2.x86_64.rpm systemd-libs-239-74.el8_8.i686.rpm systemd-libs-239-74.el8_8.2.x86_64.rpm systemd-pam-239-74.el8_8.2.x86_64.rpm systemd-udev-239-74.el8_8.2.x86_64.rpm
--	---

Security vulnerabilities resolved in CM 10.1 Security Service Pack #15
Delivered under Fix Id CM-54427

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 platform-python python3-libs python3-libs	RHSA-2023:3591	CVE-2023-24329	Important	ASA-2023-080	High
python2 python2-libs python2-pip python2-pip-wheel	RHSA-2023:3780	CVE-2023-24329	Important	ASA-2023-072	High
qemu-guest-agent	RHSA-2023:3822	CVE-2023-2700	Moderate	ASA-2023-077	Medium
libtiff	RHSA-2023:3827	CVE-2022-48281	Moderate	ASA-2023-070	Medium
systemd systemd-libs systemd-libs systemd-pam systemd-udev	RHSA-2023:3837	CVE-2023-26604	Moderate	ASA-2023-063	High
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-devel 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

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

apr-util-1.6.1-6.el8.x86_64.rpm apr-util-bdb-1.6.1-6.el8.x86_64.rpm apr-util-openssl-1.6.1-6.el8.x86_64.rpm bind-export-libs-9.11.36-8.el8.x86_64.rpm bind-libs-9.11.36-8.el8.x86_64.rpm bind-libs-lite-9.11.36-8.el8.x86_64.rpm bind-license-9.11.36-8.el8.noarch.rpm bind-utils-9.11.36-8.el8.x86_64.rpm	libarchive-3.3.3-5.el8.x86_64.rpm libcurl-7.61.1-30.el8.x86_64.rpm libcurl-7.61.1-30.el8.x86_64.rpm libslirp-4.4.0-1.module+el8.8.0+18060+3f21f2cc.x86_64.rpm libtiff-4.0.9-27.el8.x86_64.rpm libwayland-client-1.21.0-1.el8.x86_64.rpm libwayland-cursor-1.21.0-1.el8.x86_64.rpm libwayland-egl-1.21.0-1.el8.x86_64.rpm
---	---

buildah-1.29.1-1.module+el8.8.0+18195+471da4bb.x86_64.rpm common-2.1.6-1.module+el8.8.0+18098+9b44df5f.x86_64.rpm containernetworking-plugins-1.2.0-1.module+el8.8.0+18060+3f21f2cc.x86_64.rpm container-selinux-2.205.0-2.module+el8.8.0+18438+15d3aa65.noarch.rpm criu-3.15-3.module+el8.8.0+18060+3f21f2cc.x86_64.rpm curl-7.61.1-30.el8_8.2.x86_64.rpm curl-7.61.1-30.el8.x86_64.rpm dhcp-client-4.3.6-49.el8.x86_64.rpm dhcp-common-4.3.6-49.el8.noarch.rpm dhcp-libs-4.3.6-49.el8.x86_64.rpm emacs-filessystem-26.1-10.el8_8.2.noarch.rpm emacs-filessystem-26.1-9.el8.noarch.rpm fuse-overlayfs-1.10-1.module+el8.8.0+18060+3f21f2cc.x86_64.rpm kernel-4.18.0-477.10.1.el8_8.x86_64.rpm kernel-4.18.0-477.13.1.el8_8.x86_64.rpm kernel-core-4.18.0-477.10.1.el8_8.x86_64.rpm kernel-core-4.18.0-477.13.1.el8_8.x86_64.rpm kernel-devel-4.18.0-477.10.1.el8_8.x86_64.rpm kernel-devel-4.18.0-477.13.1.el8_8.x86_64.rpm kernel-headers-4.18.0-477.10.1.el8_8.x86_64.rpm kernel-headers-4.18.0-477.13.1.el8_8.x86_64.rpm kernel-modules-4.18.0-477.10.1.el8_8.x86_64.rpm kernel-modules-4.18.0-477.13.1.el8_8.x86_64.rpm kernel-tools-4.18.0-477.10.1.el8_8.x86_64.rpm kernel-tools-4.18.0-477.13.1.el8_8.x86_64.rpm kernel-tools-libs-4.18.0-477.10.1.el8_8.x86_64.rpm kernel-tools-libs-4.18.0-477.13.1.el8_8.x86_64.rpm kpartx-0.8.4-37.el8.x86_64.rpm	libwayland-server-1.21.0-1.el8.x86_64.rpm libzip-1.6.1-1.module+el8.3.0+6678+b09f589e.x86_64.rpm net-snmp-5.8-27.el8.x86_64.rpm net-snmp-agent-libs-5.8-27.el8.x86_64.rpm net-snmp-libs-5.8-27.el8.x86_64.rpm net-snmp-perl-5.8-27.el8.x86_64.rpm net-snmp-utils-5.8-27.el8.x86_64.rpm php-7.4.33-1.module+el8.8.0+17865+ef7eddfa.x86_64.rpm php-cli-7.4.33-1.module+el8.8.0+17865+ef7eddfa.x86_64.rpm php-common-7.4.33-1.module+el8.8.0+17865+ef7eddfa.x86_64.rpm php-fpm-7.4.33-1.module+el8.8.0+17865+ef7eddfa.x86_64.rpm php-process-7.4.33-1.module+el8.8.0+17865+ef7eddfa.x86_64.rpm php-xml-7.4.33-1.module+el8.8.0+17865+ef7eddfa.x86_64.rpm podman-4.4.1-8.module+el8.8.0+18438+15d3aa65.x86_64.rpm podman-catatonit-4.4.1-8.module+el8.8.0+18438+15d3aa65.x86_64.rpm python2-2.7.18-12.module+el8.8.0+17629+2cfc9d03.x86_64.rpm python2-libs-2.7.18-12.module+el8.8.0+17629+2cfc9d03.x86_64.rpm python2-pip-9.0.3-19.module+el8.6.0+13001+ad200bd9.noarch.rpm python2-pip-wheel-9.0.3-19.module+el8.6.0+13001+ad200bd9.noarch.rpm python3-bind-9.11.36-8.el8.noarch.rpm python3-perf-4.18.0-477.10.1.el8_8.x86_64.rpm python3-perf-4.18.0-477.13.1.el8_8.x86_64.rpm python3-unbound-1.16.2-5.el8.x86_64.rpm qemu-guest-agent-6.2.0-32.module+el8.8.0+18361+9f407f6e.x86_64.rpm runc-1.1.4-1.module+el8.8.0+18060+3f21f2cc.x86_64.rpm slirp4netns-1.2.0-2.module+el8.8.0+18060+3f21f2cc.x86_64.rpm sysstat-11.7.3-9.el8.x86_64.rpm unbound-libs-1.16.2-5.el8.x86_64.rpm
--	--

Security vulnerabilities resolved in CM 10.1 Security Service Pack #14

Delivered under Fix Id CM-54164

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
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
buildah common container-selinux containernetworking-plugins criu fuse-overlayfs libslirp podman podman-catatonit runc slirp4netns	RHSA-2023:2758	CVE-2022-1705 CVE-2022-1962 CVE-2022-27664 CVE-2022-28131 CVE-2022-30629 CVE-2022-30630 CVE-2022-30631 CVE-2022-30632 CVE-2022-30633 CVE-2022-30635 CVE-2022-32148 CVE-2022-32189 CVE-2022-41717 CVE-2023-0778	Moderate	ASA-2023-042	High

python3-unbound unbound-libs	RHSA-2023:2771	CVE-2022-3204	Moderate	NA	NA
ibwayland-client libwayland-cursor libwayland-egl libwayland-server	RHSA-2023:2786	CVE-2021-3782	Moderate	NA	NA
sysstat	RHSA-2023:2800	CVE-2022-39377	Moderate	ASA-2023-041	High
python2 python2-libs python2-pip python2-pip-wheel	RHSA-2023:2860	CVE-2022-45061	Moderate	NA	NA
libtiff	RHSA-2023:2883	CVE-2022-3627 CVE-2022-3970	Moderate	NA	NA
libzip php php-cli php-common php-fpm php-process 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
kernel kernel-core kernel-devel 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	Important	NA	NA

		CVE-2022-43750 CVE-2022-47929 CVE-2023-0394 CVE-2023-0461 CVE-2023-1195 CVE-2023-1582 CVE-2023-23454			
curl libcurl	RHSA-2023:2963	CVE-2022-35252 CVE-2022-43552	Low	NA	NA
net-snmp net-snmp-agent-libs net-snmp-libs net-snmp-perl net-snmp-utils	RHSA-2023:2969	CVE-2022-44792 CVE-2022-44793	Moderate	NA	NA
dhcp-client dhcp-common dhcp-libs	RHSA-2023:3000	CVE-2022-2928 CVE-2022-2929	Moderate	NA	NA
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	NA
emacsfilesystem	RHSA-2023:3042	CVE-2022-45939	Moderate	ASA-2023-039	High
emacsfilesystem	RHSA-2023:3104	CVE-2023-2491	Important	ASA-2023-045	High
curl 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-devel kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2023:3349	CVE-2023-32233	Important	NA	NA

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

libwebp-1.0.0-8.el8_7.x86_64.rpm

Security vulnerabilities resolved in CM 10.1 Security Service Pack #13***Delivered under Fix Id CM-53872***

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
libwebp	RHSA-2023:2076	CVE-2023-1999	Important	NA	NA

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

emacs-filesystem-26.1-7.el8_7.1.noarch.rpm gnutls-3.6.16-6.el8_7.i686.rpm gnutls-3.6.16-6.el8_7.x86_64.rpm httpd-2.4.37-51.module+el8.7.0+18499+2e106f0b.5.x86_64.rpm httpd-filesystem-2.4.37-51.module+el8.7.0+18499+2e106f0b.5.noarch.rpm httpd-tools-2.4.37-51.module+el8.7.0+18499+2e106f0b.5.x86_64.rpm kernel-4.18.0-425.19.2.el8_7.x86_64.rpm kernel-core-4.18.0-425.19.2.el8_7.x86_64.rpm kernel-devel-4.18.0-425.19.2.el8_7.x86_64.rpm	kernel-headers-4.18.0-425.19.2.el8_7.x86_64.rpm kernel-modules-4.18.0-425.19.2.el8_7.x86_64.rpm kernel-tools-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 mod_http2-1.15.7-5.module+el8.7.0+18499+2e106f0b.4.x86_64.rpm mod_ssl-2.4.37-51.module+el8.7.0+18499+2e106f0b.5.x86_64.rpm python3-perf-4.18.0-425.19.2.el8_7.x86_64.rpm tzdata-2023c-1.el8.noarch.rpm
---	--

Security vulnerabilities resolved in CM 10.1 Security Service Pack #12
Delivered under Fix Id CM-53734

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
kernel kernel-core kernel-devel 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	NA	NA
gnutls gnutls	RHSA-2023:1569	CVE-2023-0361	Moderate	ASA-2023-033	High
httpd httpd-filesystem httpd-tools mod_http2 mod_ssl	RHSA-2023:1673	CVE-2023-25690	Important	NA	NA
emacs-filesystem	RHSA-2023:1930	CVE-2023-28617	Important	ASA-2023-035	High
tzdata	RHBA-2023:1534	NA	Bugfix	NA	NA

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

curl-7.61.1-25.el8_7.3.x86_64.rpm	nss-util-3.79.0-11.el8_7.i686.rpm
-----------------------------------	-----------------------------------

httpd-2.4.37-51.module+el8.7.0+18026+7b169787.1.x86_64.rpm httpd-filesystem-2.4.37-51.module+el8.7.0+18026+7b169787.1.noarch.rpm httpd-tools-2.4.37-51.module+el8.7.0+18026+7b169787.1.x86_64.rpm kernel-4.18.0-425.13.1.el8_7.x86_64.rpm kernel-core-4.18.0-425.13.1.el8_7.x86_64.rpm kernel-devel-4.18.0-425.13.1.el8_7.x86_64.rpm kernel-headers-4.18.0-425.13.1.el8_7.x86_64.rpm kernel-modules-4.18.0-425.13.1.el8_7.x86_64.rpm kernel-tools-4.18.0-425.13.1.el8_7.x86_64.rpm kernel-tools-libs-4.18.0-425.13.1.el8_7.x86_64.rpm libcurl-7.61.1-25.el8_7.3.x86_64.rpm mod_http2-1.15.7-5.module+el8.6.0+13996+01710940.x86_64.rpm mod_ssl-2.4.37-51.module+el8.7.0+18026+7b169787.1.x86_64.rpm nss-3.79.0-11.el8_7.x86_64.rpm nss-softokn-3.79.0-11.el8_7.i686.rpm nss-softokn-3.79.0-11.el8_7.x86_64.rpm nss-softokn-freebl-3.79.0-11.el8_7.i686.rpm nss-softokn-freebl-3.79.0-11.el8_7.x86_64.rpm nss-sysinit-3.79.0-11.el8_7.x86_64.rpm	nss-util-3.79.0-11.el8_7.x86_64.rpm openssl-1.1.1k-9.el8_7.x86_64.rpm openssl-libs-1.1.1k-9.el8_7.i686.rpm openssl-libs-1.1.1k-9.el8_7.x86_64.rpm platform-python-3.6.8-48.el8_7.1.i686.rpm platform-python-3.6.8-48.el8_7.1.x86_64.rpm platform-python-setuptools-39.2.0-6.el8_7.1.noarch.rpm python3-libs-3.6.8-48.el8_7.1.i686.rpm python3-libs-3.6.8-48.el8_7.1.x86_64.rpm python3-perf-4.18.0-425.13.1.el8_7.x86_64.rpm python3-setuptools-39.2.0-6.el8_7.1.noarch.rpm python3-setuptools-wheel-39.2.0-6.el8_7.1.noarch.rpm systemd-239-68.el8_7.4.x86_64.rpm systemd-libs-239-68.el8_7.4.i686.rpm systemd-libs-239-68.el8_7.4.x86_64.rpm systemd-pam-239-68.el8_7.4.x86_64.rpm systemd-udev-239-68.el8_7.4.x86_64.rpm tar-1.30-6.el8_7.1.x86_64.rpm tzdata-2023b-1.el8.noarch
---	---

Security vulnerabilities resolved in CM 10.1 Security Service Pack #11

Delivered under Fix Id CM-53352

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
kernel kernel-core kernel-devel kernel-headers kernel-modules kernel-tools kernel-tools-libs python3-perf	RHSA-2023:0832	CVE-2022-2873 CVE-2022-41222 CVE-2022-43945	Important	NA	NA
platform-python platform-python python3-libs python3-libs	RHSA-2023:0833	CVE-2020-10735 CVE-2021-28861 CVE-2022-45061	Moderate	NA	NA
platform-python-setuptools python3-setuptools python3-setuptools-wheel	RHSA-2023:0835	CVE-2022-40897	Moderate	ASA-2023-023	Medium
systemd systemd-libs systemd-libs systemd-pam systemd-udev	RHSA-2023:0837	CVE-2022-4415	Moderate	NA	NA
tar	RHSA-2023:0842	CVE-2022-48303	Moderate	ASA-2023-024	High
httpd httpd-filesystem httpd-tools	RHSA-2023:0852	CVE-2006-20001 CVE-2022-36760 CVE-2022-37436	Moderate	ASA-2023-022	Low

mod_http2 mod_ssl					
curl libcurl	RHSA-2023:1140	CVE-2023-23916	Moderate	NA	NA
nss nss-softokn nss-softokn nss-softokn-freebl nss-softokn-freebl nss-sysinit nss-util nss-util	RHSA-2023:1252	CVE-2023-0767	Important	ASA-2023-028	High
openssl openssl-lib openssl-lib	RHSA-2023:1405	CVE-2022-4304 CVE-2022-4450 CVE-2023-0215 CVE-2023-0286	Important	ASA-2023-031	High
tzdata	RHBA-2023:1491	BZ - 2178569	Bugfix	NA	NA

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

dbus-1:1.12.8-23.el8_7.1.x86_64 dbus-common-1:1.12.8-23.el8_7.1.noarch dbus-daemon-1:1.12.8-23.el8_7.1.x86_64 dbus-lib-1:1.12.8-23.el8_7.1.x86_64 dbus-tools-1:1.12.8-23.el8_7.1.x86_64 expat-2.2.5-10.el8_7.1.i686 expat-2.2.5-10.el8_7.1.x86_64 grub2-common-1:2.02-142.el8_7.1.noarch grub2-efi-x64-1:2.02-142.el8_7.1.x86_64 grub2-pc-1:2.02-142.el8_7.1.x86_64 grub2-pc-modules-1:2.02-142.el8_7.1.noarch grub2-tools-1:2.02-142.el8_7.1.x86_64 grub2-tools-extra-1:2.02-142.el8_7.1.x86_64 grub2-tools-minimal-1:2.02-142.el8_7.1.x86_64 kernel-4.18.0-425.10.1.el8_7.x86_64 kernel-core-4.18.0-425.10.1.el8_7.x86_64 kernel-devel-4.18.0-425.10.1.el8_7.x86_64 kernel-headers-4.18.0-425.10.1.el8_7.x86_64 kernel-modules-4.18.0-425.10.1.el8_7.x86_64 kernel-tools-4.18.0-425.10.1.el8_7.x86_64 kernel-tools-lib-4.18.0-425.10.1.el8_7.x86_64	libXpm-3.5.12-9.el8_7.x86_64 libksba-1.3.5-9.el8_7.x86_64 libtasn1-4.13-4.el8_7.i686 libtasn1-4.13-4.el8_7.x86_64 libtiff-4.0.9-26.el8_7.x86_64 libxml2-2.9.7-15.el8_7.1.i686 libxml2-2.9.7-15.el8_7.1.x86_64 python3-libxml2-2.9.7-15.el8_7.1.x86_64 python3-perf-4.18.0-425.10.1.el8_7.x86_64 qemu-guest-agent-15:6.2.0-21.module+el8.7.0+17573+effbd7e8.2.x86_64 sqlite-3.26.0-17.el8_7.x86_64 sqlite-lib-3.26.0-17.el8_7.i686 sqlite-lib-3.26.0-17.el8_7.x86_64 sudo-1.8.29-8.el8_7.1.x86_64 systemd-239-68.el8_7.1.x86_64 systemd-lib-239-68.el8_7.1.i686 systemd-lib-239-68.el8_7.1.x86_64 systemd-pam-239-68.el8_7.1.x86_64 systemd-udev-239-68.el8_7.1.x86_64
---	---

Security vulnerabilities resolved in CM 10.1 Security Service Pack #10***Delivered under Fix Id CM-53210***

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
grub2-common grub2-efi-x64	RHSA-2023:0049	CVE-2022-2601 CVE-2022-3775	Moderate	ASA-2023-002	Medium

grub2-pc grub2-pc-modules grub2-tools grub2-tools-extra grub2-tools-minimal					
libtiff	RHSA-2023:0095	CVE-2022-2056 CVE-2022-2057 CVE-2022-2058 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-libs systemd-pam systemd-udev	RHSA-2023:0100	CVE-2022-3821	Moderate	ASA-2023-006	Medium
kernel kernel-core kernel-devel 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 libxml2 python3-libxml2	RHSA-2023:0173	CVE-2022-40303 CVE-2022-40304	Moderate	ASA-2023-007	High
sudo	RHSA-2023:0284	CVE-2023-22809	Important	ASA-2023-010	High
libXpm	RHSA-2023:0379	CVE-2022-44617	Important	ASA-2023-020	High

		CVE-2022-46285 CVE-2022-4883			
libksba	RHSA-2023:0625	CVE-2022-47629	Important/Sec.	ASA-2023-017	High

- There was no Communication Manager February 2023 Security Service Pack update required.
- January 2023 release of Avaya Aura® 10.1 Security Service Packs did not require an update for Avaya Aura® Communication Manager (CM). CM 10.1 Security Service Pack #9 should continue to be used.

CM 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 bind-license-9.11.36-5.el8.noarch.rpm bind-utils-9.11.36-5.el8.x86_64.rpm buildah-1.27.0-2.module+el8.7.0+16772+33343656.x86_64.rpm buildah-1.27.2-2.module+el8.7.0+17064+3b31f55c.x86_64.rpm common-2.1.4-1.module+el8.7.0+16772+33343656.x86_64.rpm common-2.1.4-1.module+el8.7.0+17064+3b31f55c.x86_64.rpm containernetworking-plugins-1.1.1-3.module+el8.7.0+16772+33343656.x86_64.rpm containernetworking-plugins-1.1.1-3.module+el8.7.0+17064+3b31f55c.x86_64.rpm container-selinux-2.189.0-1.module+el8.7.0+16772+33343656.noarch.rpm container-selinux-2.189.0-1.module+el8.7.0+17064+3b31f55c.noarch.rpm criu-3.15-3.module+el8.7.0+16772+33343656.x86_64.rpm criu-3.15-3.module+el8.7.0+17064+3b31f55c.x86_64.rpm e2fsprogs-1.45.6-5.el8.x86_64.rpm e2fsprogs-libs-1.45.6-5.el8.x86_64.rpm freetype-2.9.1-9.el8.x86_64.rpm fribidi-1.0.4-9.el8.x86_64.rpm fuse-overlayfs-1.9-1.module+el8.7.0+16772+33343656.x86_64.rpm fuse-overlayfs-1.9-1.module+el8.7.0+17064+3b31f55c.x86_64.rpm gdisk-1.0.3-11.el8.x86_64.rpm glib2-2.56.4-159.el8.i686.rpm glib2-2.56.4-159.el8.x86_64.rpm httpd-2.4.37-51.module+el8.7.0+16050+02173b8e.x86_64.rpm httpd-filesystem-2.4.37-51.module+el8.7.0+16050+02173b8e.noarch.rpm httpd-tools-2.4.37-51.module+el8.7.0+16050+02173b8e.x86_64.rpm kernel-4.18.0-425.3.1.el8.x86_64.rpm kernel-core-4.18.0-425.3.1.el8.x86_64.rpm kernel-devel-4.18.0-425.3.1.el8.x86_64.rpm kernel-headers-4.18.0-425.3.1.el8.x86_64.rpm krb5-libs-1.18.2-22.el8_7.i686.rpm krb5-libs-1.18.2-22.el8_7.x86_64.rpm libcom_err-1.45.6-5.el8.i686.rpm libcom_err-1.45.6-5.el8.x86_64.rpm libslirp-4.4.0-1.module+el8.7.0+16772+33343656.x86_64.rpm libslirp-4.4.0-1.module+el8.7.0+17064+3b31f55c.x86_64.rpm	kernel-modules-4.18.0-425.3.1.el8.x86_64.rpm kernel-tools-4.18.0-425.3.1.el8.x86_64.rpm kernel-tools-libs-4.18.0-425.3.1.el8.x86_64.rpm kpartx-0.8.4-28.el8_7.1.x86_64.rpm libss-1.45.6-5.el8.x86_64.rpm libtiff-4.0.9-23.el8.x86_64.rpm libxml2-2.9.7-15.el8.i686.rpm libxml2-2.9.7-15.el8.x86_64.rpm libzip-1.6.1-1.module+el8.3.0+6678+b09f589e.x86_64.rpm mod_http2-1.15.7-5.module+el8.6.0+13996+01710940.x86_64.rpm mod_ssl-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 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 php-fpm-7.4.30-1.module+el8.7.0+15886+8e29b882.x86_64.rpm php-process-7.4.30-1.module+el8.7.0+15886+8e29b882.x86_64.rpm php-xml-7.4.30-1.module+el8.7.0+15886+8e29b882.x86_64.rpm podman-4.2.0-1.module+el8.7.0+16772+33343656.x86_64.rpm podman-4.2.0-4.module+el8.7.0+17064+3b31f55c.x86_64.rpm podman-catatonit-4.2.0-1.module+el8.7.0+16772+33343656.x86_64.rpm podman-catatonit-4.2.0-4.module+el8.7.0+17064+3b31f55c.x86_64.rpm python2-2.7.18-11.module+el8.7.0+15681+7a92afba.x86_64.rpm python2-libs-2.7.18-11.module+el8.7.0+15681+7a92afba.x86_64.rpm python2-pip-9.0.3-19.module+el8.6.0+13001+ad200bd9.noarch.rpm python2-pip-wheel-9.0.3-19.module+el8.6.0+13001+ad200bd9.noarch.rpm python3-bind-9.11.36-5.el8.noarch.rpm python3-libxml2-2.9.7-15.el8.x86_64.rpm python3-perf-4.18.0-425.3.1.el8.x86_64.rpm python3-unbound-1.16.2-2.el8.x86_64.rpm qemu-guest-agent-6.2.0-20.module+el8.7.0+16689+53d59bc2.1.x86_64.rpm qt5-srpm-macros-5.15.3-1.el8.noarch.rpm rsync-3.1.3-19.el8.x86_64.rpm runc-1.1.4-1.module+el8.7.0+16772+33343656.x86_64.rpm runc-1.1.4-1.module+el8.7.0+17064+3b31f55c.x86_64.rpm slirp4netns-1.2.0-2.module+el8.7.0+16772+33343656.x86_64.rpm slirp4netns-1.2.0-2.module+el8.7.0+17064+3b31f55c.x86_64.rpm unbound-libs-1.16.2-2.el8.x86_64.rpm
---	---

Security vulnerabilities resolved in CM 10.1 Security Service Pack #9

Delivered under Fix Id CM-52811

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
uildah; common; container-selinux; containernetworking-plugins; criu; fuse-overlayfs; libslirp; podman; podman-catatonit; runc; slirp4netns	RHSA-2022:7457	CVE-2021-36221 CVE-2021-41190 CVE-2022-1708 CVE-2022-27191 CVE-2022-29162 CVE-2022-2990	Moderate	ASA-2022-139	High
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	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
python2; python2-libs; python2-pip; python2-pip-wheel	RHSA-2022:7593	CVE-2015-20107	Moderate	ASA-2022-156	High
python3-unbound; unbound-libs	RHSA-2022:7622	CVE-2022-30698 CVE-2022-30699	Moderate	ASA-2022-150	Medium
ibzip; php; php-cli; php-common; php-fpm; php-process; php-xml	RHSA-2022:7628	CVE-2021-21707 CVE-2021-21708 CVE-2021-32610	Moderate	ASA-2022-143	Critical
httpd; httpd-filesystem; httpd-tools; mod_http2;	RHSA-2022:7647	CVE-2022-22719 CVE-2022-22721 CVE-2022-23943 CVE-2022-26377	Moderate	ASA-2022-145	High

mod_ssl		CVE-2022-28614 CVE-2022-28615 CVE-2022-29404 CVE-2022-30522 CVE-2022-30556 CVE-2022-31813			
kernel; kernel-core; kernel-devel; 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
ibxml2; libxml2; python3-libxml2	RHSA-2022:7715	CVE-2016-3709	Moderate	ASA-2022-138	Medium
e2fsprogs; e2fsprogs-libs; libcom_err; libcom_err;libss	RHSA-2022:7720	CVE-2022-1304	Moderate	ASA-2022-141	High

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	None	None
buildah; common; container-selinux; containernetworking-plugins; criu; fuse-overlayfs; libslirp; podman; podman-catatonit; runc; slirp4netns	RHSA-2022:7822	CVE-2022-2989 CVE-2022-2990	Low	ASA-2022-148	High
kpartx	RHSA-2022:7928	CVE-2022-3787	Important	ASA-2022-149	High
krb5-libs; krb5-libs	RHSA-2022:8638	CVE-2022-42898	Important	None	None

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

bind-export-libs-9.11.36-3.el8_6.1.x86_64.rpm bind-libs-9.11.36-3.el8_6.1.x86_64.rpm bind-libs-lite-9.11.36-3.el8_6.1.x86_64.rpm bind-license-9.11.36-3.el8_6.1.noarch.rpm bind-utils-9.11.36-3.el8_6.1.x86_64.rpm expat-2.2.5-8.el8_6.3.i686.rpm expat-2.2.5-8.el8_6.3.x86_64.rpm gnutls-3.6.16-5.el8_6.i686.rpm gnutls-3.6.16-5.el8_6.x86_64.rpm kernel-4.18.0-372.32.1.el8_6.x86_64.rpm kernel-core-4.18.0-372.32.1.el8_6.x86_64.rpm kernel-devel-4.18.0-372.32.1.el8_6.x86_64.rpm kernel-headers-4.18.0-372.32.1.el8_6.x86_64.rpm	kernel-modules-4.18.0-372.32.1.el8_6.x86_64.rpm kernel-tools-4.18.0-372.32.1.el8_6.x86_64.rpm kernel-tools-libs-4.18.0-372.32.1.el8_6.x86_64.rpm kpartx-0.8.4-22.el8_6.2.x86_64.rpm libksba-1.3.5-8.el8_6.x86_64.rpm python3-bind-9.11.36-3.el8_6.1.noarch.rpm python3-perf-4.18.0-372.32.1.el8_6.x86_64.rpm sqlite-3.26.0-16.el8_6.x86_64.rpm sqlite-libs-3.26.0-16.el8_6.i686.rpm sqlite-libs-3.26.0-16.el8_6.x86_64.rpm zlib-1.2.11-19.el8_6.i686.rpm zlib-1.2.11-19.el8_6.x86_64.rpm tzdata-2022e-1.el8.noarch.rpm
---	--

Security vulnerabilities resolved in CM 10.1 Security Service Pack #8

Delivered under Fix Id CM-52370

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;	RHSA-2022:6778	CVE-2022-38177 CVE-2022-38178	Important	None	None

bind-utils; python3-bind					
expat; expat	RHSA-2022:6878	CVE-2022-40674	Important	None	None
libksba	RHSA-2022:7089	CVE-2022-3515	Important	None	None
gnutls; gnutls	RHSA-2022:7105	CVE-2022-2509	Moderate	None	None
zlib; zlib	RHSA-2022:7106	CVE-2022-37434	Moderate	ASA-2022-129	Critical
sqlite; sqlite-libs; sqlite-libs	RHSA-2022:7108	CVE-2020-35525 CVE-2020-35527	Moderate	ASA-2022-130	High
kernel; kernel-core; kernel-devel; 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
kpartx	RHSA-2022:7192	CVE-2022-41974	Important	ASA-2022-128	High
tzdata	RHBA-2021:3790	BZ-2007732	bugfix	None	None
tzdata	RHBA-2021:4003	BZ-2015242 BZ-2015246 BZ-2016369	bugfix	None	None
tzdata	RHBA-2021:4543	BZ-2016370	bugfix	None	None
tzdata	RHBA-2022:1032	None	bugfix	None	None
tzdata	RHBA-2022:6138	BZ-2117170 BZ-2117323 BZ-2117737 BZ-2117739 BZ-2117740 BZ-2117741	bugfix	None	None
tzdata	RHBA-2022:6827	None	bugfix	None	None
tzdata	RHBA-2022:7067	BZ-2134107 BZ-2134108 BZ-2134190 BZ-2134191 BZ-2134192 BZ-2134193 BZ-2134194	bugfix	None	None

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

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

Security vulnerabilities resolved in CM 10.1 Security Service Pack #7**Delivered under Fix Id CM-52129**

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-process; php-xml	RHSA-2022:6158	CVE-2022-31625	Moderate	ASA-2022-117	High
curl; libcurl	RHSA-2022:6159	CVE-2022-32206 CVE-2022-32208	Moderate	None	None
rsync	RHSA-2022:6180	CVE-2022-29154	Important	ASA-2022-116	High
systemd; systemd-libs; 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; platform-python; python3-libs; python3-libs	RHSA-2022:6457	CVE-2015-20107 CVE-2022-0391	Moderate	None	None
kernel; kernel-core; kernel-devel; kernel-headers;	RHSA-2022:6460	CVE-2022-21123 CVE-2022-21125 CVE-2022-21166	Moderate	None	None

kernel-modules; kernel-tools; kernel-tools-libs; python3-perf					
gnupg2; gnupg2-smime	RHSA-2022:6463	CVE-2022-34903	Moderate	ASA-2022-121	Medium
libzip; php; php-cli; php-common; php-fpm; php-process; 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

.....

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

kernel-4.18.0-372.19.1.el8_6.x86_64.rpm kernel-core-4.18.0-372.19.1.el8_6.x86_64.rpm kernel-devel-4.18.0-372.19.1.el8_6.x86_64.rpm kernel-headers-4.18.0-372.19.1.el8_6.x86_64.rpm kernel-modules-4.18.0-372.19.1.el8_6.x86_64.rpm kernel-tools-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 nginx-filestream-1.20.1-1.module+el8.5.0+13723+ab304644.noarch.rpm openssl-1.1.1k-7.el8_6.x86_64.rpm	openssl-libs-1.1.1k-7.el8_6.i686.rpm openssl-libs-1.1.1k-7.el8_6.x86_64.rpm pcre2-10.32-3.el8_6.i686.rpm pcre2-10.32-3.el8_6.x86_64.rpm pcre2-utf16-10.32-3.el8_6.x86_64.rpm python3-perf-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 vim-minimal-8.0.1763-19.el8_6.4.x86_64.rpm
--	---

Security vulnerabilities resolved in CM 10.1 Security Service Pack #6

Delivered under Fix Id CM-51856

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
nginx-filestream	RHSA-2022:0323	CVE-2021-23017	Important	ASA-2022-013	High
pcre2; pcre2; pcre2-utf16	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;	RHSA-2022:5818	CVE-2022-1292	Moderate	ASA-2022-111	Medium

openssl-lib;		CVE-2022-2068			
openssl-lib		CVE-2022-2097			
kernel; kernel-core; kernel-devel; kernel-headers; kernel-modules; kernel-tools; kernel-tools-lib; 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

.....

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

compat-openssl10-1.0.2o-4.el8_6.i686.rpm curl-7.61.1-22.el8_6.x86_64.rpm expat-2.2.5-8.el8_6.2.i686.rpm expat-2.2.5-8.el8_6.x86_64.rpm kernel-4.18.0-372.13.1.el8_6.x86_64.rpm kernel-4.18.0-372.16.1.el8_6.x86_64.rpm kernel-core-4.18.0-372.13.1.el8_6.x86_64.rpm kernel-core-4.18.0-372.16.1.el8_6.x86_64.rpm kernel-devel-4.18.0-372.13.1.el8_6.x86_64.rpm kernel-devel-4.18.0-372.16.1.el8_6.x86_64.rpm kernel-headers-4.18.0-372.13.1.el8_6.x86_64.rpm kernel-headers-4.18.0-372.16.1.el8_6.x86_64.rpm kernel-modules-4.18.0-372.13.1.el8_6.x86_64.rpm kernel-modules-4.18.0-372.16.1.el8_6.x86_64.rpm kernel-tools-4.18.0-372.13.1.el8_6.x86_64.rpm kernel-tools-4.18.0-372.16.1.el8_6.x86_64.rpm kernel-tools-lib-4.18.0-372.13.1.el8_6.x86_64.rpm kernel-tools-lib-4.18.0-372.16.1.el8_6.x86_64.rpm	libcurl-7.61.1-22.el8_6.x86_64.rpm libgcrypt-1.8.5-7.el8_6.i686.rpm libgcrypt-1.8.5-7.el8_6.x86_64.rpm libinput-1.16.3-3.el8_6.x86_64.rpm libxml2-2.9.7-13.el8_6.1.i686.rpm libxml2-2.9.7-13.el8_6.1.x86_64.rpm libzip-1.6.1-1.module+el8.3.0+6678+b09f589e.x86_64.rpm php-7.4.19-3.module+el8.6.0+15726+994cde98.x86_64.rpm php-cli-7.4.19-3.module+el8.6.0+15726+994cde98.x86_64.rpm php-common-7.4.19-3.module+el8.6.0+15726+994cde98.x86_64.rpm php-fpm-7.4.19-3.module+el8.6.0+15726+994cde98.x86_64.rpm php-process-7.4.19-3.module+el8.6.0+15726+994cde98.x86_64.rpm php-xml-7.4.19-3.module+el8.6.0+15726+994cde98.x86_64.rpm python3-libxml2-2.9.7-13.el8_6.1.x86_64.rpm python3-perf-4.18.0-372.13.1.el8_6.x86_64.rpm python3-perf-4.18.0-372.16.1.el8_6.x86_64.rpm vim-minimal-8.0.1763-19.el8_6.2.x86_64.rpm
---	--

Security vulnerabilities resolved in CM 10.1 Security Service Pack #5

Delivered under Fix Id CM-51689

Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
grypt;libgrypt	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-devel;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;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
libinput	RHSA-2022:5331	CVE-2022-1215	Moderate	ASA-2022-105	High
libzip;php;php-cli;php-common;php-fpm;php-process;php-xml	RHSA-2022:5467	CVE-2022-31626	Important	None	None
kernel;kernel-core;kernel-devel;kernel-headers;kernel-modules;kernel-tools;kernel-tools-libs;python3-perf	RHSA-2022:5564	CVE-2022-1729	Important	ASA-2022-109	Medium

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

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-pc-2.02-123.el8_6.8.x86_64.rpm grub2-pc-modules-2.02-123.el8_6.8.noarch.rpm grub2-tools-2.02-123.el8_6.8.x86_64.rpm grub2-tools-extra-2.02-123.el8_6.8.x86_64.rpm grub2-tools-minimal-2.02-123.el8_6.8.x86_64.rpm httpd-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 httpd-tools-2.4.37-47.module+el8.6.0+15654+427eba2e.2.x86_64.rpm libzip-1.6.1-1.module+el8.3.0+6678+b09f589e.x86_64.rpm mod_http2-1.15.7-5.module+el8.6.0+13996+01710940.x86_64.rpm mod_ssl-2.4.37-47.module+el8.6.0+15654+427eba2e.2.x86_64.rpm mokutil-0.3.0-11.el8_6.1.x86_64.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-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-process-7.4.19-1.module+el8.5.0+11143+cc873159.x86_64.rpm php-process-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 CM 10.1 Security Service Pack #4

Beginning with CM 10.1 SSP #4, all updates are delivered under one Fix ID. Therefore, the Fix ID column is removed from the table.

Delivered under Fix Id CM-50816

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-process;php-xml	RHSA-2021:4213	CVE-2020-7068 CVE-2020-7069 CVE-2020-7070 CVE-2020-7071 CVE-2021-21702	Moderate	None	None
libzip;php;php-cli;php-common;php-fpm;php-process;php-xml	RHSA-2022:1935	CVE-2021-21703 CVE-2021-21705	Moderate	ASA-2022-047	High
rsyslog;rsyslog-gnutls	RHSA-2022:4799	CVE-2022-24903	Important	ASA-2022-078	High
xz;xz-libs;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-pc;grub2-pc-modules;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
httpd;httpd-filesystem;httpd-tools;mod_http2;mod_ssl	RHSA-2022:5163	CVE-2020-13950	Low	ASA-2022-083	High

.....

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

bind-export-libs-9.11.36-3.el8.x86_64.rpm bind-libs-9.11.36-3.el8.x86_64.rpm bind-libs-lite-9.11.36-3.el8.x86_64.rpm bind-license-9.11.36-3.el8.noarch.rpm bind-utils-9.11.36-3.el8.x86_64.rpm buildah-1.24.2-4.module+el8.6.0+14673+621cb8be.x86_64.rpm cairo-1.15.12-6.el8.x86_64.rpm c-ares-1.13.0-6.el8.x86_64.rpm	libslirp-4.4.0-1.module+el8.6.0+14673+621cb8be.x86_64.rpm libsndfile-1.0.28-12.el8.x86_64.rpm libssh-0.9.6-3.el8.x86_64.rpm libssh-config-0.9.6-3.el8.noarch.rpm libtiff-4.0.9-21.el8.x86_64.rpm libudisks2-2.9.0-9.el8.x86_64.rpm mod_http2-1.15.7-5.module+el8.6.0+13996+01710940.x86_64.rpm mod_ssl-2.4.37-47.module+el8.6.0+14529+083145da.1.x86_64.rpm
---	--

common-2.1.0-1.module+el8.6.0+14673+621cb8be.x86_64.rpm containernetworking-plugins-1.0.1-2.module+el8.6.0+14673+621cb8be.x86_64.rpm container-selinux-2.179.1-1.module+el8.6.0+14673+621cb8be.noarch.rpm cpio-2.12-11.el8.x86_64.rpm criu-3.15-3.module+el8.6.0+14673+621cb8be.x86_64.rpm fuse-overlayfs-1.8.2-1.module+el8.6.0+14673+621cb8be.x86_64.rpm grub2-common-2.02-123.el8.noarch.rpm grub2-efi-x64-2.02-123.el8.x86_64.rpm grub2-pc-2.02-123.el8.x86_64.rpm grub2-pc-modules-2.02-123.el8.noarch.rpm grub2-tools-2.02-123.el8.x86_64.rpm grub2-tools-extra-2.02-123.el8.x86_64.rpm grub2-tools-minimal-2.02-123.el8.x86_64.rpm gzip-1.9-13.el8_5.x86_64.rpm httpd-2.4.37-47.module+el8.6.0+14529+083145da.1.x86_64.rpm httpd-filesystem-2.4.37-47.module+el8.6.0+14529+083145da.1.noarch.rpm httpd-tools-2.4.37-47.module+el8.6.0+14529+083145da.1.x86_64.rpm kernel-4.18.0-348.23.1.el8_5.x86_64.rpm kernel-4.18.0-372.9.1.el8.x86_64.rpm kernel-core-4.18.0-348.23.1.el8_5.x86_64.rpm kernel-core-4.18.0-372.9.1.el8.x86_64.rpm kernel-devel-4.18.0-348.23.1.el8_5.x86_64.rpm kernel-devel-4.18.0-372.9.1.el8.x86_64.rpm kernel-headers-4.18.0-348.23.1.el8_5.x86_64.rpm kernel-headers-4.18.0-372.9.1.el8.x86_64.rpm kernel-modules-4.18.0-348.23.1.el8_5.x86_64.rpm kernel-modules-4.18.0-372.9.1.el8.x86_64.rpm kernel-tools-4.18.0-348.23.1.el8_5.x86_64.rpm kernel-tools-4.18.0-372.9.1.el8.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	openssh-8.0p1-13.el8.x86_64.rpm openssh-clients-8.0p1-13.el8.x86_64.rpm openssh-server-8.0p1-13.el8.x86_64.rpm pixman-0.38.4-2.el8.x86_64.rpm platform-python-3.6.8-45.el8.i686.rpm platform-python-3.6.8-45.el8.x86_64.rpm podman-4.0.2-6.module+el8.6.0+14673+621cb8be.x86_64.rpm podman-catatonit-4.0.2-6.module+el8.6.0+14673+621cb8be.x86_64.rpm polkit-0.115-13.el8_5.2.x86_64.rpm polkit-libs-0.115-13.el8_5.2.x86_64.rpm python2-2.7.18-10.module+el8.6.0+14191+7fdd52cd.x86_64.rpm python2-libs-2.7.18-10.module+el8.6.0+14191+7fdd52cd.x86_64.rpm python2-pip-9.0.3-19.module+el8.6.0+13001+ad200bd9.noarch.rpm python2-pip-wheel-9.0.3-19.module+el8.6.0+13001+ad200bd9.noarch.rpm python3-bind-9.11.36-3.el8.noarch.rpm python3-libs-3.6.8-45.el8.i686.rpm python3-libs-3.6.8-45.el8.x86_64.rpm python3-perf-4.18.0-348.23.1.el8_5.x86_64.rpm python3-perf-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 qt5-qtbase-5.15.2-4.el8.x86_64.rpm qt5-qtbase-common-5.15.2-4.el8.noarch.rpm qt5-qtbase-gui-5.15.2-4.el8.x86_64.rpm rsync-3.1.3-14.el8_6.2.x86_64.rpm runc-1.0.3-2.module+el8.6.0+14673+621cb8be.x86_64.rpm slirp4netns-1.1.8-2.module+el8.6.0+14673+621cb8be.x86_64.rpm udisks2-2.9.0-9.el8.x86_64.rpm vim-minimal-8.0.1763-16.el8_5.13.x86_64.rpm zlib-1.2.11-18.el8_5.i686.rpm zlib-1.2.11-18.el8_5.x86_64.rpm
---	--

Security vulnerabilities resolved in CM 10.1 Security Service Pack #3

Fix ID	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-50140	gzip	RHSA-2022:1537	CVE-2022-1271	Important	ASA-2022-041	High
CM-50139	polkit;polkit-libs	RHSA-2022:1546	CVE-2021-4115	Moderate	ASA-2022-040	Medium
CM-50508	kernel;kernel-core;kernel-devel;kernel-headers;kernel-modules;kernel-tools;kernel-tools-libs;python3-perf	RHSA-2022:1550	CVE-2021-4028 CVE-2022-25636	Important	None	None
CM-50141	vim-minimal	RHSA-2022:1552	CVE-2022-1154	Moderate	ASA-2022-042	Critical
CM-50142	zlib;zlib	RHSA-2022:1642	CVE-2018-25032	Important	ASA-2022-044	High
CM-	qemu-guest-agent	RHSA-2022:1759	CVE-2021-20196	Moderate	ASA-2022-062	High

50245			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			
50244	buildah;common;container-selinux;containernetworking-plugins;criu;fuse-overlayfs;libslirp;podman;podman-catatonit;runc;slirp4netns	RHSA-2022:1762	CVE-2022-1227 CVE-2022-21698 CVE-2022-27649 CVE-2022-27650 CVE-2022-27651	Important	ASA-2022-061	High
CM-50231	qt5-qtbase;qt5-qtbase-common;qt5-qtbase-gui	RHSA-2022:1796	CVE-2021-38593	Moderate	ASA-2022-045	High
CM-50234	libtiff	RHSA-2022:1810	CVE-2020-19131	Moderate	ASA-2022-050	High
CM-50232	libudisks2;udisks2	RHSA-2022:1820	CVE-2021-3802	Low	ASA-2022-048	Low
CM-50243	python2;python2-libs;python2-pip;python2-pip-wheel	RHSA-2022:1821	CVE-2021-3733 CVE-2021-3737 CVE-2021-4189 CVE-2021-43818 CVE-2022-0391	Moderate	ASA-2022-059	High
CM-50237	httpd;httpd-filesystem;httpd-tools;mod_http2;mod_ssl	RHSA-2022:1915	CVE-2020-35452 CVE-2021-33193 CVE-2021-36160 CVE-2021-44224	Moderate	ASA-2022-053	High
CM-50236	cairo;pixman	RHSA-2022:1961	CVE-2020-35492	Moderate	ASA-2022-052	High
	libsndfile	RHSA-2022:1968	CVE-2021-4156	Moderate		
50239	kernel;kernel-core;kernel-devel;kernel-headers;kernel-modules;kernel-tools;kernel-tools-	RHSA-2022:1988	CVE-2020-0404 CVE-2020-13974 CVE-2020-27820	Important	ASA-2022-055	Critical

	libs;python3-perf		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			
CM-50238	cpio	RHSA-2022:1991	CVE-2021-38185	Moderate	ASA-2022-054	High
CM-50240	openssh;openssh-clients;openssh-server	RHSA-2022:2013	CVE-2021-41617	Moderate	ASA-2022-056	High
CM-50241	libssh;libssh-config	RHSA-2022:2031	CVE-2021-3634	Low	ASA-2022-057	Medium
CM-50509	c-ares	RHSA-2022:2043	CVE-2021-3672	Moderate	None	None
CM-50250	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
CM-50235	grub2-common;grub2-efi-x64;grub2-pc;grub2-pc-modules;grub2-tools;grub2-tools-extra;grub2-tools-minimal	RHSA-2022:2110	CVE-2021-3981	Low	ASA-2022-051	Low
CM-50246	rsync	RHSA-2022:2201	CVE-2018-25032	Important	ASA-2022-063	High

.....

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

expat-2.2.5-4.el8_5.3.i686 expat-2.2.5-4.el8_5.3.x86_64 glibc-2.28-164.el8_5.3.i686 glibc-2.28-164.el8_5.3.x86_64 glibc-all-langpacks-2.28-164.el8_5.3.x86_64 glibc-common-2.28-164.el8_5.3.x86_64 glibc-devel-2.28-164.el8_5.3.x86_64 glibc-headers-2.28-164.el8_5.3.x86_64 glibc-langpack-en-2.28-164.el8_5.3.x86_64 httpd-2.4.37-43.module+el8.5.0+14370+51c6d843.2.x86_64 httpd-2.4.37-43.module+el8.5.0+14530+6f259f31.3.x86_64 httpd-filesystem-2.4.37-43.module+el8.5.0+14370+51c6d843.2.noarch httpd-filesystem-2.4.37-43.module+el8.5.0+14530+6f259f31.3.noarch httpd-tools-2.4.37-43.module+el8.5.0+14370+51c6d843.2.x86_64 httpd-tools-2.4.37-43.module+el8.5.0+14530+6f259f31.3.x86_64	libarchive-3.3.3-3.el8_5.x86_64 libnsl-2.28-164.el8_5.3.i686 libnsl-2.28-164.el8_5.3.x86_64 libxml2-2.9.7-12.el8_5.i686 libxml2-2.9.7-12.el8_5.x86_64 mod_ssl-1:2.4.37-43.module+el8.5.0+14370+51c6d843.2.x86_64 mod_ssl-1:2.4.37-43.module+el8.5.0+14530+6f259f31.3.x86_64 nscd-2.28-164.el8_5.3.x86_64 openssl-1:1.1.1k-6.el8_5.x86_64 openssl-libs-1:1.1.1k-6.el8_5.i686 openssl-libs-1:1.1.1k-6.el8_5.x86_64 python3-libxml2-2.9.7-12.el8_5.x86_64 qemu-guest-agent-15.4.2.0-59.module+el8.5.0+14169+68d2f392.2.x86_64 vim-minimal-2:8.0.1763-16.el8_5.12.x86_64
--	---

Security vulnerabilities resolved in CM 10.1 Security Service Pack #2

Fix ID	Updated Package	RHSA Number	Common Vulnerability and Exposure (CVE) ID	RHSA Severity	ASA Number	ASA Overall Severity
CM-49265	expat security update	RHSA-2022:0951	CVE-2021-45960 CVE-2021-46143 CVE-2022-22822 CVE-2022-22823 CVE-2022-22824 CVE-2022-22825 CVE-2022-22826 CVE-2022-22827 CVE-2022-23852 CVE-2022-25235 CVE-2022-25236 CVE-2022-25315	Important	ASA-2022-031	Critical
CM-49432	openssl security update	RHSA-2022:1065	CVE-2022-0778	Important	ASA-2022-036	High
CM-49264	virt:rhel and virt-devel:rhel security update	RHSA-2022:0886	CVE-2022-0358	Moderate	ASA-2022-032	High
CM-49262	httpd:2.4 security update	RHSA-2022:1049	CVE-2022-22720	Important	ASA-2022-034	Critical
CM-49266	vim security update	RHSA-2022:0894	CVE-2022-0261 CVE-2022-0318 CVE-2022-0359 CVE-2022-0361 CVE-2022-0392 CVE-2022-0413	Moderate	ASA-2022-030	High

CM-49263	libxml2 security update	RHSA-2022:0899	CVE-2022-23308	Moderate	ASA-2022-033	High
CM-49267	httpd:2.4 security update	RHSA-2022:0891	CVE-2021-34798 CVE-2021-39275	Moderate	ASA-2022-029	High
CM-50023	glibc security update	RHSA-2022:0896	CVE-2021-3999 CVE-2022-23218 CVE-2022-23219	Moderate	None	NA
CM-50024	libarchive security update	RHSA-2022:0892	CVE-2021-23177 CVE-2021-31566	Moderate	None	NA

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

aide-0.16-14.el8_5.1.x86_64 cryptsetup-2.3.3-4.el8_5.1.x86_64 cryptsetup-libs-2.3.3-4.el8_5.1.x86_64 cyrus-sasl-lib-2.1.27-6.el8_5.i686 cyrus-sasl-lib-2.1.27-6.el8_5.x86_64 httpd-2.4.37-43.module+el8.5.0+13806+b30d9eec.1.x86_64 httpd-filesystem-2.4.37-43.module+el8.5.0+13806+b30d9eec.1.noarch httpd-tools-2.4.37-43.module+el8.5.0+13806+b30d9eec.1.x86_64 kernel-4.18.0-348.12.2.el8_5.x86_64 kernel-4.18.0-348.20.1.el8_5.x86_64 kernel-4.18.0-348.7.1.el8_5.x86_64 kernel-core-4.18.0-348.12.2.el8_5.x86_64 kernel-core-4.18.0-348.20.1.el8_5.x86_64 kernel-core-4.18.0-348.7.1.el8_5.x86_64 kernel-devel-4.18.0-348.12.2.el8_5.x86_64 kernel-devel-4.18.0-348.20.1.el8_5.x86_64 kernel-devel-4.18.0-348.7.1.el8_5.x86_64 kernel-headers-4.18.0-348.12.2.el8_5.x86_64 kernel-headers-4.18.0-348.20.1.el8_5.x86_64 kernel-headers-4.18.0-348.7.1.el8_5.x86_64 kernel-modules-4.18.0-348.12.2.el8_5.x86_64 kernel-modules-4.18.0-348.20.1.el8_5.x86_64 kernel-modules-4.18.0-348.7.1.el8_5.x86_64 kernel-tools-4.18.0-348.12.2.el8_5.x86_64 kernel-tools-4.18.0-348.20.1.el8_5.x86_64 kernel-tools-4.18.0-348.7.1.el8_5.x86_64 kernel-tools-libs-4.18.0-348.12.2.el8_5.x86_64 kernel-tools-libs-4.18.0-348.20.1.el8_5.x86_64 kernel-tools-libs-4.18.0-348.7.1.el8_5.x86_64 libgcc-8.5.0-3.el8.i686 libgcc-8.5.0-3.el8.x86_64 libgcc-8.5.0-4.el8_5.i686	libgcc-8.5.0-4.el8_5.x86_64 libgomp-8.5.0-3.el8.x86_64 libgomp-8.5.0-4.el8_5.x86_64 libstdc++-8.5.0-3.el8.i686 libstdc++-8.5.0-3.el8.x86_64 libstdc++-8.5.0-4.el8_5.i686 libstdc++-8.5.0-4.el8_5.x86_64 mod_ssl-1:2.4.37-43.module+el8.5.0+13806+b30d9eec.1.x86_64 nss-3.67.0-7.el8_5.x86_64 nss-softokn-3.67.0-7.el8_5.i686 nss-softokn-3.67.0-7.el8_5.x86_64 nss-softokn-freebl-3.67.0-7.el8_5.i686 nss-softokn-freebl-3.67.0-7.el8_5.x86_64 nss-sysinit-3.67.0-7.el8_5.x86_64 nss-util-3.67.0-7.el8_5.i686 nss-util-3.67.0-7.el8_5.x86_64 openssl-1:1.1.1k-5.el8_5.x86_64 openssl-libs-1:1.1.1k-5.el8_5.i686 openssl-libs-1:1.1.1k-5.el8_5.x86_64 polkit-0.115-13.el8_5.1.x86_64 polkit-libs-0.115-13.el8_5.1.x86_64 python3-perf-4.18.0-348.12.2.el8_5.x86_64 python3-perf-4.18.0-348.20.1.el8_5.x86_64 python3-perf-4.18.0-348.7.1.el8_5.x86_64 python3-rpm-4.14.3-19.el8_5.2.x86_64 qemu-guest-agent-15:4.2.0-59.module+el8.5.0+13495+8166cdf8.1.x86_64 rpm-4.14.3-19.el8_5.2.x86_64 rpm-build-libs-4.14.3-19.el8_5.2.x86_64 rpm-libs-4.14.3-19.el8_5.2.x86_64 rpm-plugin-selinux-4.14.3-19.el8_5.2.x86_64 rpm-plugin-systemd-inhibit-4.14.3-19.el8_5.2.x86_64 vim-minimal-2:8.0.1763-16.el8_5.4.x86_64
--	--

Security vulnerabilities resolved in CM 10.1 Security Service Pack #1

Fix ID	Updated Package	RHSA Number	Common Vulnerability and	RHSA Severity	ASA Number	ASA Overall
--------	-----------------	-------------	--------------------------	---------------	------------	-------------

			Exposure (CVE) ID			Severity
CM-48786	aide security update	RHSA-2022:0441	CVE-2021-45417	Important	ASA-2022-021	High
CM-48502	httpd:2.4 security update	RHSA-2022:0258	CVE-2021-44790	Important	ASA-2022-020	Critical
CM-48501	cryptsetup security update	RHSA-2022:0370	CVE-2021-4122	Moderate	ASA-2022-019	Medium
CM-48470	rpm security update	RHSA-2022:0368	CVE-2021-3521	Moderate	ASA-2022-016	Medium
CM-48469	vim security update	RHSA-2022:0366	CVE-2021-3872 CVE-2021-3984 CVE-2021-4019 CVE-2021-4192 CVE-2021-4193	Moderate	ASA-2022-015	High
CM-48465	polkit security update	RHSA-2022:0267	CVE-2021-4034	Important	ASA-2022-007	High
CM-48464	kernel security and bug fix update	RHSA-2022:0188	CVE-2021-4155 CVE-2022-0185	Important	ASA-2022-006	High
CM-48463	openssh security update	RHSA-2021:4368	CVE-2020-14145	Moderate	ASA-2021-140	Medium
CM-48462	python3 security update	RHSA-2021:4057	CVE-2021-3733	Moderate	ASA-2021-133	Medium
CM-48461	python-pip security update	RHSA-2021:4455	CVE-2021-3572	Low	ASA-2021-139	Medium
CM-48460	lua security update	RHSA-2021:4510	CVE-2020-24370	Low	ASA-2021-137	Medium
CM-48459	rpm security, bug fix, and enhancement update	RHSA-2021:4489	CVE-2021-20266	Low	ASA-2021-136	Medium
CM-48458	libwebp security update	RHSA-2021:4231	CVE-2018-25009 CVE-2018-25010 CVE-2018-25012 CVE-2018-25013 CVE-2018-25014 CVE-2020-36330 CVE-2020-36331 CVE-2020-36332	Moderate	ASA-2021-143	Critical
CM-48457	python36:3.6 security and bug fix update	RHSA-2021:4150	CVE-2021-20270 CVE-2021-27291	Moderate	ASA-2021-142	High
CM-48456	sqlite security update	RHSA-2021:4396	CVE-2019-5827 CVE-2019-13750 CVE-2019-13751 CVE-2019-19603 CVE-2020-13435	Moderate	ASA-2021-141	High
CM-48455	kernel security update	RHSA-2021:4647	CVE-2021-20317 CVE-2021-43267	Important	ASA-2021-178	High

CM-48454	virt:rhel and virt-devel:rhel security update	RHSA-2021:5238	CVE-2021-3930 CVE-2021-20257	Low	ASA-2021-189	Low
CM-48453	httpd:2.4 security update	RHSA-2021:3816	CVE-2021-26691 CVE-2021-40438	Important	ASA-2021-126	Critical
CM-47480	container-tools 3.0	RHSA-2021:4222	CVE-2021-3602	Moderate	None	None
CM-47479	container-tools	RHSA-2021:1796	CVE-2020-29652 CVE-2021-20199	Moderate	None	None
CM-47478	container-tools	RHSA-2021:0531	CVE-2020-14370	Moderate	None	None
CM-47477	container-tools	RHSA-2020:4694	CVE-2020-10749 CVE-2020-10756 CVE-2020-14040	Moderate	None	None
CM-47476	container-tools	RHSA-2020:3053	CVE-2020-1983 CVE-2021-20188	Moderate	None	None
CM-47969	libjpeg-turbo	RHSA-2021:4288	CVE-2020-17541	Moderate	ASA-2021-148	High
CM-47970	Moderate: openssl	RHSA-2021:4424	CVE-2021-23840 CVE-2021-23841	Moderate	ASA-2021-134	High
CM-47971	kernel security	RHSA-2021:4356	CVE-2019-14615 CVE-2020-0427 CVE-2020-24502 CVE-2020-24503 CVE-2020-24504 CVE-2020-24586 CVE-2020-24587 CVE-2020-24588 CVE-2020-26139 CVE-2020-26140 CVE-2020-26141 CVE-2020-26143 CVE-2020-26144 CVE-2020-26145 CVE-2020-26146 CVE-2020-26147 CVE-2020-27777 CVE-2020-29368 CVE-2020-29660 CVE-2020-36158 CVE-2020-36312 CVE-2020-36386 CVE-2021-0129 CVE-2021-3348 CVE-2021-3489 CVE-2021-3564 CVE-2021-3573 CVE-2021-3600 CVE-2021-3635 CVE-2021-3659 CVE-2021-3679 CVE-2021-3732 CVE-2021-20194 CVE-2021-20239 CVE-2021-23133 CVE-2021-28950 CVE-2021-28971	Moderate	ASA-2021-147	High

			CVE-2021-29155 CVE-2021-29646 CVE-2021-29650 CVE-2021-31440 CVE-2021-31829 CVE-2021-31916 CVE-2021-33033 CVE-2021-33200			
CM-47972	ncurses	RHSA-2021:4426	CVE-2019-17594 CVE-2019-17595	Moderate	ASA-2021-146	Medium
CM-47973	binutils	RHSA-2021:4364	CVE-2021-3487 CVE-2021-20197 CVE-2020-35448 CVE-2021-20284	Moderate	ASA-2021-145	Medium
CM-48000	kexec-tools	RHSA-2021:4404	CVE-2021-20269	Low	ASA-2021-151	Medium
CM-47965	vim	RHSA-2021:4517	CVE-2021-3778 CVE-2021-3796	Moderate	ASA-2021-150	High
CM-47966	binutils	RHSA-2021:4595	CVE-2021-42574	Moderate	ASA-2021-152	High
CM-47967	gnutls and nettle security	RHSA-2021:4451	CVE-2021-3580 CVE-2021-20231 CVE-2021-20232	Moderate	ASA-2021-149	High
CM-47968	kernel	RHSA-2021:5227	CVE-2021-20321	Moderate	ASA-2021-187	Medium
CM-49900	cyrus-sasl	RHSA-2022:0658	CVE-2022-24407	Important	None	None
CM-49268	kernel security, bug fix, and enhancement update	RHSA-2022:0825	CVE-2021-0920 CVE-2021-4154 CVE-2022-0330 CVE-2022-0435 CVE-2022-0492 CVE-2022-0516 CVE-2022-0847 CVE-2022-22942	Important	ASA-2022-028	High
CM-49901	gcc security and bug fix update	RHSA-2021:4386	CVE-2018-20673	Low	None	None
CM-49902	gcc security and bug fix update	RHSA-2021:4587	CVE-2021-42574	Moderate	None	None
CM-49903	nss security update	RHSA-2021:4903	CVE-2021-43527	Critical	None	None
CM-49904	openssl security update	RHSA-2021:5226	CVE-2021-3712	Moderate	ASA-2022-002	High

Mitigation: N/A

SECTION 1C – ENTITLEMENTS AND CONTACTS

Material There is no incremental charge for the material in this PCN. The software updates are available on

**Coverage
Entitlements:**

support.avaya.com and from plds.avaya.com.

**Avaya Customer
Service
Coverage
Entitlements:**

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

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

Customers under the following Avaya coverage:

- Full Coverage Service Contract*
- On-site Hardware Maintenance Contract*

Remote Installation	Current Per Incident Rates Apply
Remote or On-site Services Labor	Current Per Incident Rates Apply

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

Customers under the following Avaya coverage:

- Warranty
- Software Support
- Software Support Plus Upgrades
- Remote Only
- Parts Plus Remote
- Remote Hardware Support
- Remote Hardware Support w/ Advance Parts Replacement

Help-Line Assistance	Per Terms of Services Contract or coverage
Remote or On-site Services Labor	Per Terms of Services Contract or coverage

Avaya Product Correction Notice Support Offer

The Avaya Product Correction Support Offer provides out-of-hours support for remote and on-site technician installable PCNs, and Avaya installation for all Avaya issued PCNs that are classified as “Customer-Installable”. Refer to the PCN Offer or contact your Avaya Account Representative for complete details.

**Avaya
Authorized
Partner
Service
Coverage
Entitlements:**
Avaya Authorized Partner

Avaya Authorized Partners are responsible for the implementation of this PCN on behalf of their customers.

**Who to contact
for more
information:**

If you require further information or assistance please contact your Authorized Service Provider, or visit support.avaya.com. There you can access more product information, chat with an Agent, or open an online Service Request. Support is provided per your warranty or service contract terms unless otherwise specified in the Avaya support [Terms of Use](#).