Avaya Aura® Media Server (AAMS) Release Notes

Release 10.1.x.x

Issue 1.11

April 15, 2024

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“**Hosted Service**” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If you purchase a Hosted Service subscription, the foregoing limited warranty may not apply but you may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, https://support.avaya.com/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR

SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA LLC, ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA LLCOR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “**Software**” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “**Designated Processor**” means a single stand-alone computing device. “**Server**” means a Designated Processor that hosts a software application to be accessed by multiple users. “**Instance**” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“**VM**”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “**Unit**” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya’s prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. “Named User,” means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo/ under the link "Heritage Nortel Products," or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"**Third Party Components**" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting you, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components, to the extent that these Software License Terms impose greater restrictions on you than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE

AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya LLC.

All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com/ (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Change history

Issue	Date	Description
1.0	April 18, 2022	Release of AAMS 10.1.0
1.1	June 6, 2022	Added note about FIPS upgrade issue (AMS-12047)
1.2	September 19, 2022	Release of AAMS 10.1.0 Service Pack 1
1.3	October 25, 2022	Added additional information about SRTP upgrade changes and SSRC reuse support.
1.4	October 31, 2022	Added upgrade note about internal communications.
1.5	February 13, 2023	Release of AAMS 10.1.0 Service Pack 2
1.6	March 17, 2023	Clarification about UEFI support.
1.7	June 19, 2023	Release of AAMS 10.1.0 Service Pack 3
1.8	August 14, 2023	Release of AAMS 10.1.0 Service Pack 4
1.9	September 11, 2023	Release of September 2023 Security Service Pack
1.10	December 18, 2023	Release of AAMS 10.1.0 Service Pack 5
1.11	April 15, 2024	Release of AAMS 10.1.0 Service Pack 6

Introduction

This document provides late-breaking information to supplement Avaya Aura® Media Server software and documentation. For updated documentation, product support notices, and service pack information, go to the Avaya Support site at https://support.avaya.com.

The Avaya Aura® Media Server delivers advanced multimedia processing features to a broad range of products and applications. Utilizing the latest open standards for media control and media processing, the highly scalable software-based solution deploys on standard server hardware. It is comprised of the following components:

- Media Server Software
- System Layer (appliance only).

What's new

What's new in 10.1.0

The following table lists enhancements in this release.

Enhancement	Description
AMS-9517	Red Hat 8.x support
AMS-10719	Updated Element Manager to assign the new System Manager-signed certificate to all service profiles in System Manager enrollment
AMS-10108	Generate alarm if no scheduled backup task is defined for all backup types
AMS-10559	All deployments enable multi-SSRC tracking for SRTP and HA.

What's new in 10.1.0 SP 1

The following table lists enhancements in this release.

Enhancement	Description
AMS-11446	Update logcapture to include cpuinfo, meminfo and SELinux status in its log archive
AMS-11682	Added support for ABCD DTMF tones generation

What's new in 10.1.0 SP 2

The following table lists enhancements in this release.

Enhancement	Description
AMS-12479	Default staging certificates replaced by self-signed certificates generated during installation. Note this applies to new deployments only and customer must replace these certificates with an unique identify certificate signed by a trusted CA.
AMS-11752	Update to RHEL 8.6 in virtual and physical appliance.
AMS-10150	Introduce UEFI support for physical and virtual appliances appliance. Note this applies to new deployments only.

What's new in 10.1.0 SP 3

The following table lists enhancements in this release.

Enhancement	Description
N/A	

What’s new in 10.1.0 SP 4

The following table lists enhancements in this release.

Enhancement	Description
N/A	

What’s new in 10.1.0 SP 5

The following table lists enhancements in this release.

Enhancement	Description
	ESXi 8.0

What’s new in 10.1.0 SP 6

The following table lists enhancements in this release.

Enhancement	Description
N/A	

Contacting support

Contact support checklist

If you are having trouble with *Avaya Aura® Media Server*, you should:

1. Retry the action. Carefully follow the instructions in written or online documentation.
2. Check the documentation that came with your software for maintenance or software-related problems.
3. Note the sequence of events that led to the problem and the exact messages displayed.

If you continue to have a problem, contact Avaya Technical Support:

1. Log in to the Avaya Technical Support Web site https://support.avaya.com.
2. Contact Avaya Technical Support at one of the telephone numbers in the Support Directory listings on the Avaya support Web site.

Avaya Global Services Escalation Management provides the means to escalate urgent service issues. For more information, see the Escalation Contacts listings on the Avaya Support site.

Contact support tasks

You may be asked to email one or more files to Technical Support for analysis of your application and its environment.

- Media Server log capture with trace logs included
- Network packet capture on the Media Server

- Screen shots for Element Manager issues
- Debug log (ams_debug.log) for System Manager Media Server element issues

Avaya Aura® Media Server

Software Compatibility

Prior to upgrading AAMS software you must review the Avaya compatibility matrix of the controlling application (i.e. CM) to ensure that the controlling application has been tested and is compatible with AAMS.

Supported Upgrade Paths

Prior to upgrading to AAMS 10.1.0 your prior installation must meet the following minimum software revisions for the Media Server software:

Release	***Minimum Supported***
8.0.2	8.0.2.56 or higher

8.0.2 to 10.1 Appliance Upgrade Considerations

Before upgrading the 8.0.2 AAMS appliance (virtual or physical) to 10.1 consider the following:

- Rollback from 10.1 SP 3 or higher to an prior 10.1 release is not supported due to an DB upgrade. Prior to doing upgrade please ensure you take a backup and transfer the backup off the server.   Installation media (ISO/OVA plus updates) of the previous 10.1.0 release should be on-hand in case you need to revert back to it.   For virtual appliances it is recommend you take a snapshot prior to doing the upgrade.
- Rollbacks from 10.1 to 8.0.2 is not supported.   Prior to doing upgrade please ensure you take a backup and transfer the backup off the server.   Installation media (ISO/OVA plus updates) of the previous 8.0.2 release should be on-hand in case you need to revert back to 8.0.2.   For virtual appliances it is recommend you take a snapshot prior to doing the upgrade.
- Ensure that one of these partitions have approximately 2 GB of free space.   If it doesn't customer should cleanup files in /root, /var, pub (/opt/ayaya/pub) and/or local media directory (/opt/avaya/app) to free up disk space.

  /opt/avaya/app

  /var

  /
- 8.0.2 doesn't backup authenticated NTP configuration. After upgrading authenticated NTP configuration is not preserved and manual authenticated NTP configuration is required. Configuration setting ***Reject SRTP Audio On SSRC Reuse*** has been removed and SSRC reuse is enabled by default.   There are no configuration settings to disable.
- Internal media communication uses G.711 ulaw or G.722.   Need to ensure these codecs are enabled within audio codec configuration or there will be errors when allocating IVR resources.Disable the use of TLS ciphers with a key size less than 2048.

10.1.0.x to 10.1.0.y Appliance Upgrade Considerations

Before upgrading the 10.1.0.x AAMS appliance (virtual or physical) to 10.1.0.y consider the following:

- If upgrading from 10.1.0.77, 10.1.0.101, 10.1.0.125, or 10.1.0.147 you must stage both updates (media server and system layer) before attempting the upgrade.

Installation

10.1.0 New Installation File List (Virtual Appliance Only)

Download ID	Filename	Notes
MSR000000175	MediaServer_10.1.0.121_A5_2022.12.20_OVF10.ova	AAMS virtual appliance (OVA) for new deployments. Appliance contains Media Server 10.1.0.121 and System Layer 10.0.0.11. ***NOTE after deploying the OVA you MUST install the mandatory updates listed in the section titled "10.1.010.1.0 Required Updates and Hotfixes (Appliance Only)". If the updates are the same version as what is installed on the appliance then no action is required.***

10.1.0 New Installation File List (Physical Appliance Only)

Download ID	Filename	Notes
MSR000000176	MediaServer_10.1.0.121_A5_2022.12.20.iso	AAMS physical appliance installer and recovery disk for new appliance deployments. Appliance contains Media Server 10.1.0.121 and System Layer 10.0.0.11. ***NOTE after installing the appliance you MUST install the mandatory updates listed in the section titled "10.1.010.1.0 Required Updates and Hotfixes (Appliance Only)". If the updates are the same version as what is installed on the appliance then no action is required.***

10.1.0 New Installation File List (Customer Supplied Hardware and OS Only)

Download ID	Filename	Notes
MSR000000199	MediaServer_10.1.0.195_2024.03.06.bin	AAMS software only installer (PVI) for new deployments where customer is supplying the hardware and Linux OS.

10.1.0 Required Updates and Hotfixes (Appliance Only)

Find patch information at https://support.avaya.com.

Download ID	Patch	Notes
MSR000000200	10.1.0.195	AAMS update for Media Server software that needs to be applied to all 10.1..x appliance deployments.
MSR000000201	10.0.0.17	AAMS update for System Layer software that needs to be applied to all 10..x appliance deployments.

10.1.0 Required Updates and Hotfixes (Customer Supplied Hardware and OS Only)

Find patch information at https://support.avaya.com.

Download ID	Patch	Notes
MSR000000199	10.1.0.195	AAMS software only installer (PVI) for new deployments where customer is supplying the hardware and Linux OS.

10.1.0 Patch File list (Appliance Only)

Filename	File size	Version
MediaServer_System_Update_10.0.0.17_2024.03.08.iso	2,039,793,664	10.1.0.17
MediaServer_Update_10.1.0.195_2024.03.06.iso	886,472,704	10.1.0.195

10.1.0 Patch File list (Customer Supplied Hardware and OS Only)

Filename	File size	Version
MediaServer_10.1.0.195_2024.03.06.bin	886,081,675	10.1.0.195

Installing the release

For appliance installations, see procedures documented in *Deploying and Updating Avaya Aura® Media Server Appliance* on the Avaya Support website at: https://downloads.avaya.com/css/P8/documents/101079837.

For Customer Supplied Hardware and OS installations, refer to procedures documented in *Installing and Updating Avaya Aura® Media Server Application on Customer Supplied Hardware and OS* on the Avaya Support at: https://downloads.avaya.com/css/P8/documents/101080249.

When upgrading an appliance, use the following procedure:

1. Backup the system.
2. Upload both system layer and media sever updates.
3. Place system in pending lock (one node at a time).
4. Click “Install Updates” in Element Manager to initiate update install.
5. Once installation complete place system in an unlocked state.

Backing up the software

For appliance installations, see procedures documented in *Deploying and Updating Avaya Aura® Media Server Appliance* on the Avaya Support website at: https://downloads.avaya.com/css/P8/documents/101079837.

For Customer Supplied Hardware and OS installations, see procedures documented in *Implementing and Administering Avaya Aura® Media Server* on the Avaya Support website at: https://downloads.avaya.com/css/P8/documents/101080151.

Troubleshooting the installation

For appliance installations, see procedures documented in *Deploying and Updating Avaya Aura® Media Server Appliance* on the Avaya Support website at: https://downloads.avaya.com/css/P8/documents/101079837.

For non-appliance installations, see procedures documented in *Installing and Updating Avaya Aura® Media Server Application on Customer Supplied Hardware and OS* on the Avaya Support website at: https://downloads.avaya.com/css/P8/documents/101080249.

Restoring software to previous version

For appliance installations refer to procedures documented in *Deploying and Updating Avaya Aura® Media Server Appliance* on the Avaya Support site at: https://downloads.avaya.com/css/P8/documents/101079837.

For non-appliance installs refer to procedures documented in Implementing and Administering Avaya Aura® Media Server on the Avaya Support site: https://downloads.avaya.com/css/P8/documents/101080151.

Enhanced Access Security Gateway (EASG)

EASG provides a secure method for Avaya services personnel to access the Avaya Aura® MS remotely and onsite. Access is under the control of the customer and can be enabled or disabled at any time. EASG must be enabled for Avaya Services to perform tasks necessary for the ongoing support, management and optimization of the solution. EASG is also required to enable remote proactive support tools such as Avaya Expert Systems® and Avaya Healthcheck.

On the AAMS appliance EASG is disabled by default so customers that are deploying a new appliance for the first time are encouraged to enable EASG, which can be done by issuing the following command after upgrading.

```
        EASGManage –enableEASG
```

SELinux and su operations

When SELinux is enabled su operations will prompt first for the current users credentials followed by the target users credentials.

Session Detail Record Archiving

As of AAMS 8.0.2 SP2 Session Detail Record (SDR) archiving is disabled by default. SDR archiving can be enabled with AAMS Element Manager by navigating to *Home » System Configuration » Logging Settings* and clicking the *Session Logging*.   To enable SDR archiving ensure the *Session Detail Record Archiving* is check and click save.

Debug Log Retention

As of AAMS 8.0.2 SP2 debug log rotation will be enabled by default when debug logging is enabled. Debug logs will rotate every hour and will only be retained for 1 day. Log retention settings can be disabled, or retention time can be modified using AAMS Element Manager. To modify log retention settings, navigate to *Home » System Configuration » Debug Tracing » General Settings* and update *Trace File Retention Limit setting* accordingly.

Functionality not supported

N/A

Fixes

Fixes in System Layer for 10.1.0 GA (10.0.0.6)

The following table lists the fixes in this release.

ID	Minimum conditions	Description
AMS-10539	All appliance deployments.	Apply and verify rp_filter settings
AMS-11507	All appliance deployments.	Clean up PVI checker artifacts after upgrade
	All appliance deployments	RHSA-2022:0188 – https://access.redhat.com/errata/RHSA-2022:0188 kernel-modules-4.18.0-348.12.2.el8_5.x86_64 kernel-core-4.18.0-348.12.2.el8_5.x86_64 kernel-4.18.0-348.12.2.el8_5.x86_64 python3-perf-4.18.0-348.12.2.el8_5.x86_64 https://access.redhat.com/security/cve/CVE-2021-4155 https://access.redhat.com/security/cve/CVE-2022-0185 RHSA-2022:0267 – https://access.redhat.com/errata/RHSA-2022:0267 polkit-0.115-13.el8_5.1.x86_64 polkit-libs-0.115-13.el8_5.1.x86_64 https://access.redhat.com/security/cve/CVE-2021-4034 RHSA-2022:0366 – https://access.redhat.com/errata/RHSA-2022:0366 vim-minimal-2:8.0.1763-16.el8_5.4.x86_64 https://access.redhat.com/security/cve/CVE-2021-3872 https://access.redhat.com/security/cve/CVE-2021-3984 https://access.redhat.com/security/cve/CVE-2021-4019 https://access.redhat.com/security/cve/CVE-2021-4192 https://access.redhat.com/security/cve/CVE-2021-4193 RHSA-2022:0368 – https://access.redhat.com/errata/RHSA-2022:0368 rpm-build-libs-4.14.3-19.el8_5.2.x86_64 python3-rpm-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 rpm-4.14.3-19.el8_5.2.x86_64 https://access.redhat.com/security/cve/CVE-2021-3521 RHSA-2022:0370 – https://access.redhat.com/errata/RHSA-2022:0370

ID	Minimum conditions	Description
		cryptsetup-libs-2.3.3-4.el8_5.1.x86_64 https://access.redhat.com/security/cve/CVE-2021-4122 RHSA-2022:0441 – https://access.redhat.com/errata/RHSA-2022:0441 aide-0.16-14.el8_5.1.x86_64 https://access.redhat.com/security/cve/CVE-2021-45417 RHSA-2022:0658 – https://access.redhat.com/errata/RHSA-2022:0658 cyrus-sasl-lib-2.1.27-6.el8_5.x86_64 cyrus-sasl-lib-2.1.27-6.el8_5.i686 cyrus-sasl-2.1.27-6.el8_5.x86_64 https://access.redhat.com/security/cve/CVE-2022-24407 RHSA-2022:0825 – https://access.redhat.com/errata/RHSA-2022:0825 kernel-4.18.0-348.20.1.el8_5.x86_64 python3-perf-4.18.0-348.20.1.el8_5.x86_64 kernel-core-4.18.0-348.20.1.el8_5.x86_64 kernel-modules-4.18.0-348.20.1.el8_5.x86_64 https://access.redhat.com/security/cve/CVE-2021-0920 https://access.redhat.com/security/cve/CVE-2021-4154 https://access.redhat.com/security/cve/CVE-2022-0330 https://access.redhat.com/security/cve/CVE-2022-0435 https://access.redhat.com/security/cve/CVE-2022-0492 https://access.redhat.com/security/cve/CVE-2022-0516 https://access.redhat.com/security/cve/CVE-2022-0847 https://access.redhat.com/security/cve/CVE-2022-22942 RHSA-2022:0892 – https://access.redhat.com/errata/RHSA-2022:0892 libarchive-3.3.3-3.el8_5.x86_64 https://access.redhat.com/security/cve/CVE-2021-23177 https://access.redhat.com/security/cve/CVE-2021-31566 RHSA-2022:0894 – https://access.redhat.com/errata/RHSA-2022:0894 vim-minimal-2:8.0.1763-16.el8_5.12.x86_64 https://access.redhat.com/security/cve/CVE-2022-0261 https://access.redhat.com/security/cve/CVE-2022-0318 https://access.redhat.com/security/cve/CVE-2022-0359 https://access.redhat.com/security/cve/CVE-2022-0361 https://access.redhat.com/security/cve/CVE-2022-0392

ID	Minimum conditions	Description
		https://access.redhat.com/security/cve/CVE-2022-0413 RHSA-2022:0896 – https://access.redhat.com/errata/RHSA-2022:0896 glibc-2.28-164.el8_5.3.x86_64 glibc-common-2.28-164.el8_5.3.x86_64 libnsl-2.28-164.el8_5.3.x86_64 glibc-minimal-langpack-2.28-164.el8_5.3.x86_64 glibc-2.28-164.el8_5.3.i686 libnsl-2.28-164.el8_5.3.i686 glibc-locale-source-2.28-164.el8_5.3.x86_64 glibc-langpack-en-2.28-164.el8_5.3.x86_64 https://access.redhat.com/security/cve/CVE-2021-3999 https://access.redhat.com/security/cve/CVE-2022-23218 https://access.redhat.com/security/cve/CVE-2022-23219 RHSA-2022:0899 – https://access.redhat.com/errata/RHSA-2022:0899 python3-libxml2-2.9.7-12.el8_5.x86_64 libxml2-2.9.7-12.el8_5.x86_64 https://access.redhat.com/security/cve/CVE-2022-23308
AMS-11201	All appliance deployments	Backup/restore NTP Entries
AMS-11507	All appliance deployments	Skip PVI check for upgrades/re-installs
AMS-10937	All appliance deployments	Add alias and wrapper for emtool on appliances.
AMS-10164	All appliance deployments	Enable major release upgrades for 8.0 to 10.x
	All appliance deployments	Security updates: RHSA-2021:1206 – https://access.redhat.com/errata/RHSA-2021:1206 nettle-3.4.1-4.el8_3.x86_64 gnutls-3.6.14-8.el8_3.x86_64 https://access.redhat.com/security/cve/CVE-2021-20305 RHSA-2021:2168 – https://access.redhat.com/errata/RHSA-2021:2168 kernel-modules-4.18.0-305.3.1.el8_4.x86_64 kernel-core-4.18.0-305.3.1.el8_4.x86_64 kernel-4.18.0-305.3.1.el8_4.x86_64 python3-perf-4.18.0-305.3.1.el8_4.x86_64 https://access.redhat.com/security/cve/CVE-2021-3501 https://access.redhat.com/security/cve/CVE-2021-3543

ID	Minimum conditions	Description
		RHSA-2021:2170 – https://access.redhat.com/errata/RHSA-2021:2170 glib2-2.56.4-10.el8_4.x86_64 https://access.redhat.com/security/cve/CVE-2021-27219 RHSA-2021:2238 – https://access.redhat.com/errata/RHSA-2021:2238 polkit-0.115-11.el8_4.1.x86_64 polkit-libs-0.115-11.el8_4.1.x86_64 https://access.redhat.com/security/cve/CVE-2021-3560 RHSA-2021:2308 – https://access.redhat.com/errata/RHSA-2021:2308 microcode_ctl-4:20210216-1.20210525.1.el8_4.x86_64 https://access.redhat.com/security/cve/CVE-2020-24489 https://access.redhat.com/security/cve/CVE-2020-24511 https://access.redhat.com/security/cve/CVE-2020-24512 https://access.redhat.com/security/cve/CVE-2020-24513 RHSA-2021:2569 – https://access.redhat.com/errata/RHSA-2021:2569 libxml2-2.9.7-9.el8_4.2.x86_64 python3-libxml2-2.9.7-9.el8_4.2.x86_64 https://access.redhat.com/security/cve/CVE-2021-3516 https://access.redhat.com/security/cve/CVE-2021-3517 https://access.redhat.com/security/cve/CVE-2021-3518 https://access.redhat.com/security/cve/CVE-2021-3537 https://access.redhat.com/security/cve/CVE-2021-3541 RHSA-2021:2570 – https://access.redhat.com/errata/RHSA-2021:2570 kernel-4.18.0-305.7.1.el8_4.x86_64 python3-perf-4.18.0-305.7.1.el8_4.x86_64 kernel-modules-4.18.0-305.7.1.el8_4.x86_64 kernel-core-4.18.0-305.7.1.el8_4.x86_64 https://access.redhat.com/security/cve/CVE-2020-26541 https://access.redhat.com/security/cve/CVE-2021-33034 RHSA-2021:2574 – https://access.redhat.com/errata/RHSA-2021:2574 rpm-build-libs-4.14.3-14.el8_4.x86_64 rpm-4.14.3-14.el8_4.x86_64 rpm-plugin-selinux-4.14.3-14.el8_4.x86_64 rpm-libs-4.14.3-14.el8_4.x86_64

ID	Minimum conditions	Description
		rpm-plugin-systemd-inhibit-4.14.3-14.el8_4.x86_64 python3-rpm-4.14.3-14.el8_4.x86_64 https://access.redhat.com/security/cve/CVE-2021-20271 https://access.redhat.com/security/cve/CVE-2021-3421 RHSA-2021:2575 – https://access.redhat.com/errata/RHSA-2021:2575 lz4-libs-1.8.3-3.el8_4.x86_64 lz4-1.8.3-3.el8_4.x86_64 https://access.redhat.com/security/cve/CVE-2021-3520 RHSA-2021:2714 – https://access.redhat.com/errata/RHSA-2021:2714 kernel-4.18.0-305.10.2.el8_4.x86_64 python3-perf-4.18.0-305.10.2.el8_4.x86_64 kernel-core-4.18.0-305.10.2.el8_4.x86_64 kernel-modules-4.18.0-305.10.2.el8_4.x86_64 https://access.redhat.com/security/cve/CVE-2021-32399 https://access.redhat.com/security/cve/CVE-2021-33909 RHSA-2021:2717 – https://access.redhat.com/errata/RHSA-2021:2717 systemd-udev-239-45.el8_4.2.x86_64 systemd-libs-239-45.el8_4.2.x86_64 systemd-239-45.el8_4.2.x86_64 systemd-pam-239-45.el8_4.2.x86_64 https://access.redhat.com/security/cve/CVE-2021-33910 RHSA-2021:3027 – https://access.redhat.com/errata/RHSA-2021:3027 microcode_ctl-4:20210216-1.20210608.1.el8_4.x86_64 https://access.redhat.com/security/cve/CVE-2020-0543 https://access.redhat.com/security/cve/CVE-2020-0548 https://access.redhat.com/security/cve/CVE-2020-0549 https://access.redhat.com/security/cve/CVE-2020-24489 https://access.redhat.com/security/cve/CVE-2020-24511 https://access.redhat.com/security/cve/CVE-2020-24512 https://access.redhat.com/security/cve/CVE-2020-8695 https://access.redhat.com/security/cve/CVE-2020-8696 https://access.redhat.com/security/cve/CVE-2020-8698 RHSA-2021:3057 – https://access.redhat.com/errata/RHSA-2021:3057 kernel-modules-4.18.0-305.12.1.el8_4.x86_64

ID	Minimum conditions	Description
		python3-perf-4.18.0-305.12.1.el8_4.x86_64 kernel-4.18.0-305.12.1.el8_4.x86_64 kernel-core-4.18.0-305.12.1.el8_4.x86_64 https://access.redhat.com/security/cve/CVE-2021-22543 https://access.redhat.com/security/cve/CVE-2021-22555 https://access.redhat.com/security/cve/CVE-2021-3609 RHSA-2021:3058 – https://access.redhat.com/errata/RHSA-2021:3058 glib2-2.56.4-10.el8_4.1.x86_64 https://access.redhat.com/security/cve/CVE-2021-27218 RHSA-2021:3447 – https://access.redhat.com/errata/RHSA-2021:3447 kernel-4.18.0-305.17.1.el8_4.x86_64 python3-perf-4.18.0-305.17.1.el8_4.x86_64 kernel-core-4.18.0-305.17.1.el8_4.x86_64 kernel-modules-4.18.0-305.17.1.el8_4.x86_64 https://access.redhat.com/security/cve/CVE-2021-37576 https://access.redhat.com/security/cve/CVE-2021-38201 RHSA-2021:3548 – https://access.redhat.com/errata/RHSA-2021:3548 python3-perf-4.18.0-305.19.1.el8_4.x86_64 kernel-4.18.0-305.19.1.el8_4.x86_64 kernel-core-4.18.0-305.19.1.el8_4.x86_64 kernel-modules-4.18.0-305.19.1.el8_4.x86_64 https://access.redhat.com/security/cve/CVE-2021-3653 RHSA-2021:3576 – https://access.redhat.com/errata/RHSA-2021:3576 krb5-libs-1.18.2-8.3.el8_4.i686 krb5-libs-1.18.2-8.3.el8_4.x86_64 https://access.redhat.com/security/cve/CVE-2021-36222 https://access.redhat.com/security/cve/CVE-2021-37750 RHSA-2021:3582 – https://access.redhat.com/errata/RHSA-2021:3582 curl-7.61.1-18.el8_4.1.x86_64 libcurl-7.61.1-18.el8_4.1.i686 libcurl-7.61.1-18.el8_4.1.x86_64 https://access.redhat.com/security/cve/CVE-2021-22922 https://access.redhat.com/security/cve/CVE-2021-22923 https://access.redhat.com/security/cve/CVE-2021-22924

ID	Minimum conditions	Description
		RHSA-2021:4056 – https://access.redhat.com/errata/RHSA-2021:4056 kernel-modules-4.18.0-305.25.1.el8_4.x86_64 kernel-core-4.18.0-305.25.1.el8_4.x86_64 kernel-4.18.0-305.25.1.el8_4.x86_64 python3-perf-4.18.0-305.25.1.el8_4.x86_64 https://access.redhat.com/security/cve/CVE-2020-36385 https://access.redhat.com/security/cve/CVE-2021-0512 https://access.redhat.com/security/cve/CVE-2021-3656 RHSA-2021:4057 – https://access.redhat.com/errata/RHSA-2021:4057 python3-libs-3.6.8-39.el8_4.x86_64 platform-python-3.6.8-39.el8_4.x86_64 https://access.redhat.com/security/cve/CVE-2021-3733 RHSA-2021:4059 – https://access.redhat.com/errata/RHSA-2021:4059 curl-7.61.1-18.el8_4.2.x86_64 libcurl-7.61.1-18.el8_4.2.x86_64 libcurl-7.61.1-18.el8_4.2.i686 https://access.redhat.com/security/cve/CVE-2021-22946 https://access.redhat.com/security/cve/CVE-2021-22947 RHSA-2021:4060 – https://access.redhat.com/errata/RHSA-2021:4060 libsolv-0.7.16-3.el8_4.x86_64 https://access.redhat.com/security/cve/CVE-2021-33928 https://access.redhat.com/security/cve/CVE-2021-33929 https://access.redhat.com/security/cve/CVE-2021-33930 https://access.redhat.com/security/cve/CVE-2021-33938 RHSA-2021:4151 – https://access.redhat.com/errata/RHSA-2021:4151 python2-libs-2.7.18-7.module+el8.5.0+12203+77770ab7.x86_64 python2-2.7.18-7.module+el8.5.0+12203+77770ab7.x86_64 https://access.redhat.com/security/cve/CVE-2020-27619 https://access.redhat.com/security/cve/CVE-2020-28493 https://access.redhat.com/security/cve/CVE-2021-20095 https://access.redhat.com/security/cve/CVE-2021-20270 https://access.redhat.com/security/cve/CVE-2021-23336 https://access.redhat.com/security/cve/CVE-2021-27291 https://access.redhat.com/security/cve/CVE-2021-28957

ID	Minimum conditions	Description
		https://access.redhat.com/security/cve/CVE-2021-42771 RHSA-2021:4172 – https://access.redhat.com/errata/RHSA-2021:4172 qt5-srpm-macros-5.15.2-1.el8.noarch https://access.redhat.com/security/cve/CVE-2021-3481 RHSA-2021:4326 – https://access.redhat.com/errata/RHSA-2021:4326 libX11-1.6.8-5.el8.x86_64 libX11-common-1.6.8-5.el8.noarch https://access.redhat.com/security/cve/CVE-2021-31535 RHSA-2021:4356 – https://access.redhat.com/errata/RHSA-2021:4356 kernel-4.18.0-348.el8.x86_64 kernel-core-4.18.0-348.el8.x86_64 kernel-modules-4.18.0-348.el8.x86_64 python3-perf-4.18.0-348.el8.x86_64 https://access.redhat.com/security/cve/CVE-2019-14615 https://access.redhat.com/security/cve/CVE-2020-0427 https://access.redhat.com/security/cve/CVE-2020-24502 https://access.redhat.com/security/cve/CVE-2020-24503 https://access.redhat.com/security/cve/CVE-2020-24504 https://access.redhat.com/security/cve/CVE-2020-24586 https://access.redhat.com/security/cve/CVE-2020-24587 https://access.redhat.com/security/cve/CVE-2020-24588 https://access.redhat.com/security/cve/CVE-2020-26139 https://access.redhat.com/security/cve/CVE-2020-26140 https://access.redhat.com/security/cve/CVE-2020-26141 https://access.redhat.com/security/cve/CVE-2020-26143 https://access.redhat.com/security/cve/CVE-2020-26144 https://access.redhat.com/security/cve/CVE-2020-26145 https://access.redhat.com/security/cve/CVE-2020-26146 https://access.redhat.com/security/cve/CVE-2020-26147 https://access.redhat.com/security/cve/CVE-2020-27777 https://access.redhat.com/security/cve/CVE-2020-29368 https://access.redhat.com/security/cve/CVE-2020-29660 https://access.redhat.com/security/cve/CVE-2020-36158 https://access.redhat.com/security/cve/CVE-2020-36312 https://access.redhat.com/security/cve/CVE-2020-36386 https://access.redhat.com/security/cve/CVE-2021-0129

ID	Minimum conditions	Description
		https://access.redhat.com/security/cve/CVE-2021-20194 https://access.redhat.com/security/cve/CVE-2021-20239 https://access.redhat.com/security/cve/CVE-2021-23133 https://access.redhat.com/security/cve/CVE-2021-28950 https://access.redhat.com/security/cve/CVE-2021-28971 https://access.redhat.com/security/cve/CVE-2021-29155 https://access.redhat.com/security/cve/CVE-2021-29646 https://access.redhat.com/security/cve/CVE-2021-29650 https://access.redhat.com/security/cve/CVE-2021-31440 https://access.redhat.com/security/cve/CVE-2021-31829 https://access.redhat.com/security/cve/CVE-2021-31916 https://access.redhat.com/security/cve/CVE-2021-33033 https://access.redhat.com/security/cve/CVE-2021-33200 https://access.redhat.com/security/cve/CVE-2021-3348 https://access.redhat.com/security/cve/CVE-2021-3489 https://access.redhat.com/security/cve/CVE-2021-3564 https://access.redhat.com/security/cve/CVE-2021-3573 https://access.redhat.com/security/cve/CVE-2021-3600 https://access.redhat.com/security/cve/CVE-2021-3635 https://access.redhat.com/security/cve/CVE-2021-3659 https://access.redhat.com/security/cve/CVE-2021-3679 https://access.redhat.com/security/cve/CVE-2021-3732 RHSA-2021:4358 – https://access.redhat.com/errata/RHSA-2021:4358 libnsl-2.28-164.el8.i686 glibc-2.28-164.el8.x86_64 glibc-locale-source-2.28-164.el8.x86_64 glibc-langpack-en-2.28-164.el8.x86_64 glibc-common-2.28-164.el8.x86_64 glibc-minimal-langpack-2.28-164.el8.x86_64 glibc-2.28-164.el8.i686 https://access.redhat.com/security/cve/CVE-2021-27645 https://access.redhat.com/security/cve/CVE-2021-33574 https://access.redhat.com/security/cve/CVE-2021-35942 RHSA-2021:4361 – https://access.redhat.com/errata/RHSA-2021:4361 NetworkManager-1:1.32.10-4.el8.x86_64 NetworkManager-libnm-1:1.32.10-4.el8.x86_64 https://access.redhat.com/security/cve/CVE-2020-13529

ID	Minimum conditions	Description
		RHSA-2021:4364 – https://access.redhat.com/errata/RHSA-2021:4364 binutils-2.30-108.el8.x86_64 https://access.redhat.com/security/cve/CVE-2020-35448 https://access.redhat.com/security/cve/CVE-2021-20197 https://access.redhat.com/security/cve/CVE-2021-20284 https://access.redhat.com/security/cve/CVE-2021-3487 RHSA-2021:4368 – https://access.redhat.com/errata/RHSA-2021:4368 openssh-server-8.0p1-10.el8.x86_64 openssh-8.0p1-10.el8.x86_64 openssh-clients-8.0p1-10.el8.x86_64 https://access.redhat.com/security/cve/CVE-2020-14145 RHSA-2021:4373 – https://access.redhat.com/errata/RHSA-2021:4373 pcre-8.42-6.el8.x86_64 https://access.redhat.com/security/cve/CVE-2019-20838 https://access.redhat.com/security/cve/CVE-2020-14155 RHSA-2021:4374 – https://access.redhat.com/errata/RHSA-2021:4374 file-5.33-20.el8.x86_64 file-libs-5.33-20.el8.x86_64 https://access.redhat.com/security/cve/CVE-2019-18218 RHSA-2021:4382 – https://access.redhat.com/errata/RHSA-2021:4382 json-c-0.13.1-2.el8.x86_64 https://access.redhat.com/security/cve/CVE-2020-12762 RHSA-2021:4384 – https://access.redhat.com/errata/RHSA-2021:4384 bind-utils-32:9.11.26-6.el8.x86_64 bind-32:9.11.26-6.el8.x86_64 bind-libs-32:9.11.26-6.el8.x86_64 python3-bind-32:9.11.26-6.el8.noarch bind-license-32:9.11.26-6.el8.noarch bind-libs-lite-32:9.11.26-6.el8.x86_64 https://access.redhat.com/security/cve/CVE-2021-25214 RHSA-2021:4385 – https://access.redhat.com/errata/RHSA-2021:4385 glib2-2.56.4-156.el8.x86_64

ID	Minimum conditions	Description
		https://access.redhat.com/security/cve/CVE-2021-28153 https://access.redhat.com/security/cve/CVE-2021-3800 RHSA-2021:4386 – https://access.redhat.com/errata/RHSA-2021:4386 libstdc++-8.5.0-3.el8.x86_64 libstdc++-8.5.0-3.el8.i686 libgomp-8.5.0-3.el8.x86_64 libgcc-8.5.0-3.el8.x86_64 libgcc-8.5.0-3.el8.i686 https://access.redhat.com/security/cve/CVE-2018-20673 RHSA-2021:4387 – https://access.redhat.com/errata/RHSA-2021:4387 libssh-config-0.9.4-3.el8.noarch libssh-0.9.4-3.el8.i686 libssh-0.9.4-3.el8.x86_64 https://access.redhat.com/security/cve/CVE-2020-16135 RHSA-2021:4396 – https://access.redhat.com/errata/RHSA-2021:4396 sqlite-libs-3.26.0-15.el8.x86_64 sqlite-3.26.0-15.el8.x86_64 https://access.redhat.com/security/cve/CVE-2019-13750 https://access.redhat.com/security/cve/CVE-2019-13751 https://access.redhat.com/security/cve/CVE-2019-19603 https://access.redhat.com/security/cve/CVE-2019-5827 https://access.redhat.com/security/cve/CVE-2020-13435 RHSA-2021:4399 – https://access.redhat.com/errata/RHSA-2021:4399 platform-python-3.6.8-41.el8.x86_64 python3-libs-3.6.8-41.el8.x86_64 https://access.redhat.com/security/cve/CVE-2021-3426 RHSA-2021:4408 – https://access.redhat.com/errata/RHSA-2021:4408 libsolv-0.7.19-1.el8.x86_64 https://access.redhat.com/security/cve/CVE-2021-3200 RHSA-2021:4409 – https://access.redhat.com/errata/RHSA-2021:4409 libgcrypt-1.8.5-6.el8.x86_64 https://access.redhat.com/security/cve/CVE-2021-33560

ID	Minimum conditions	Description
		RHSA-2021:4424 – https://access.redhat.com/errata/RHSA-2021:4424 openssl-libs-1:1.1.1k-4.el8.x86_64 openssl-1:1.1.1k-4.el8.x86_64 openssl-libs-1:1.1.1k-4.el8.i686 https://access.redhat.com/security/cve/CVE-2021-23840 https://access.redhat.com/security/cve/CVE-2021-23841 RHSA-2021:4426 – https://access.redhat.com/errata/RHSA-2021:4426 ncurses-libs-6.1-9.20180224.el8.x86_64 ncurses-libs-6.1-9.20180224.el8.i686 ncurses-base-6.1-9.20180224.el8.noarch ncurses-6.1-9.20180224.el8.x86_64 https://access.redhat.com/security/cve/CVE-2019-17594 https://access.redhat.com/security/cve/CVE-2019-17595 RHSA-2021:4451 – https://access.redhat.com/errata/RHSA-2021:4451 nettle-3.4.1-7.el8.x86_64 gnutls-3.6.16-4.el8.x86_64 https://access.redhat.com/security/cve/CVE-2021-20231 https://access.redhat.com/security/cve/CVE-2021-20232 https://access.redhat.com/security/cve/CVE-2021-3580 RHSA-2021:4455 – https://access.redhat.com/errata/RHSA-2021:4455 python3-pip-wheel-9.0.3-20.el8.noarch platform-python-pip-9.0.3-20.el8.noarch https://access.redhat.com/security/cve/CVE-2021-3572 RHSA-2021:4464 – https://access.redhat.com/errata/RHSA-2021:4464 python3-libdnf-0.63.0-3.el8.x86_64 dnf-4.7.0-4.el8.noarch dnf-plugins-core-4.0.21-3.el8.noarch yum-4.7.0-4.el8.noarch python3-hawkey-0.63.0-3.el8.x86_64 python3-dnf-4.7.0-4.el8.noarch python3-dnf-plugins-core-4.0.21-3.el8.noarch dnf-data-4.7.0-4.el8.noarch libdnf-0.63.0-3.el8.x86_64 https://access.redhat.com/security/cve/CVE-2021-3445

ID	Minimum conditions	Description
		RHSA-2021:4489 – https://access.redhat.com/errata/RHSA-2021:4489 rpm-plugin-systemd-inhibit-4.14.3-19.el8.x86_64 rpm-plugin-selinux-4.14.3-19.el8.x86_64 rpm-build-libs-4.14.3-19.el8.x86_64 rpm-4.14.3-19.el8.x86_64 python3-rpm-4.14.3-19.el8.x86_64 rpm-libs-4.14.3-19.el8.x86_64 https://access.redhat.com/security/cve/CVE-2021-20266 RHSA-2021:4510 – https://access.redhat.com/errata/RHSA-2021:4510 lua-libs-5.3.4-12.el8.x86_64 https://access.redhat.com/security/cve/CVE-2020-24370 RHSA-2021:4511 – https://access.redhat.com/errata/RHSA-2021:4511 libcurl-7.61.1-22.el8.x86_64 curl-7.61.1-22.el8.x86_64 libcurl-7.61.1-22.el8.i686 https://access.redhat.com/security/cve/CVE-2021-22876 https://access.redhat.com/security/cve/CVE-2021-22898 https://access.redhat.com/security/cve/CVE-2021-22925 RHSA-2021:4513 – https://access.redhat.com/errata/RHSA-2021:4513 libsepol-2.9-3.el8.x86_64 libsepol-2.9-3.el8.i686 https://access.redhat.com/security/cve/CVE-2021-36084 https://access.redhat.com/security/cve/CVE-2021-36085 https://access.redhat.com/security/cve/CVE-2021-36086 https://access.redhat.com/security/cve/CVE-2021-36087 RHSA-2021:4517 – https://access.redhat.com/errata/RHSA-2021:4517 vim-minimal-2:8.0.1763-16.el8.x86_64 https://access.redhat.com/security/cve/CVE-2021-3778 https://access.redhat.com/security/cve/CVE-2021-3796 RHSA-2021:4587 – https://access.redhat.com/errata/RHSA-2021:4587 libstdc++-8.5.0-4.el8_5.i686 libstdc++-8.5.0-4.el8_5.x86_64 libgomp-8.5.0-4.el8_5.x86_64 libgcc-8.5.0-4.el8_5.i686

ID	Minimum conditions	Description
		libgcc-8.5.0-4.el8_5.x86_64 https://access.redhat.com/security/cve/CVE-2021-42574 RHSA-2021:4595 – https://access.redhat.com/errata/RHSA-2021:4595 binutils-2.30-108.el8_5.1.x86_64 https://access.redhat.com/security/cve/CVE-2021-42574 RHSA-2021:4647 – https://access.redhat.com/errata/RHSA-2021:4647 kernel-modules-4.18.0-348.2.1.el8_5.x86_64 python3-perf-4.18.0-348.2.1.el8_5.x86_64 kernel-core-4.18.0-348.2.1.el8_5.x86_64 kernel-4.18.0-348.2.1.el8_5.x86_64 https://access.redhat.com/security/cve/CVE-2021-20317 https://access.redhat.com/security/cve/CVE-2021-43267 RHSA-2021:5226 – https://access.redhat.com/errata/RHSA-2021:5226 openssl-libs-1:1.1.1k-5.el8_5.x86_64 openssl-libs-1:1.1.1k-5.el8_5.i686 openssl-1:1.1.1k-5.el8_5.x86_64 https://access.redhat.com/security/cve/CVE-2021-3712 RHSA-2021:5227 – https://access.redhat.com/errata/RHSA-2021:5227 kernel-modules-4.18.0-348.7.1.el8_5.x86_64 kernel-core-4.18.0-348.7.1.el8_5.x86_64 kernel-4.18.0-348.7.1.el8_5.x86_64 python3-perf-4.18.0-348.7.1.el8_5.x86_64 https://access.redhat.com/security/cve/CVE-2021-20321

Fixes in Media Server for 10.1.0 GA (10.1.0.77)

The following table lists the fixes in this release.

ID	Minimum conditions	Description
AMS-11595	SIP deployments	SIP Unable to trust Ipv6 address
AMS-11519	All deployments	Fixed Platform Locked setting after a major upgrade
AMS-11402	All deployments	Removed the Open WebLM Server button from Element Manager Licensing General Settings

ID	Minimum conditions	Description
AMS-11470	All deployments	Removed server info from Element Manager responses
AMS-11628	All deployments	Updated the restart messages on Element Manager IP Interface Assignment confirmation page
AMS-10719	All deployments	Updated Element Manager to assign the new System Manager-signed certificate to all service profiles in System Manager enrollment
AMS-11551	All deployments	Enable restore of 8.0.2 NTP data
AMS-11640	WebRTC deployment	FNTMP lockup generating ICE credentials
AMS-11625	SIP deployments	SIP outgoing connection audit
AMS-11510	All deployments	Fixed Element Manager access issue after major upgrade from 8.0.2
AMS-11493	All deployments	Fixed major upgrade failure related to NTP configuration
AMS-11588	FIPS deployments	Fixed FIPS mode query
AMS-11599	FIPS deployments	Fixed audit log for FIPS mode change via Element Manager
AMS-11422	All deployments	Fixed hidden texts styling in Element Manager Software Update task
AMS-11050	FIPS deployments	Updated Element Manager UI upon FIPS configuration change
AMS-11563	All deployments	Add log capture trigger mechanism
AMS-11055	JITC deployments	Update Tomcat server.xml for JTIC security enhancements
AMS-11048	JITC deployments	Update Tomcat web.xml for JTIC security enhancements
AMS-11517	Deployments with SNMP traps configured.	Fix SNMP crash when trap destinations are configured
AMS-11425	All deployments	Update RTCP handling
AMS-11201	All deployments	Fixed NTP Backup/Restore via Element Manager

ID	Minimum conditions	Description
AMS-7372	FIPS deployments	Fixed issue with Element Manager not starting after upgrade or downgrade with FIPS enabled.
AMS-10204	SIP deployments	Fixed the port value on protocol selection for SIP route configuration
AMS-10832	All deployments	Fixed Element Manager login redirect after session termination/expiration
AMS-11411	All deployments	Update config constraint for Element Manager security warning message
AMS-11412	WebRTC deployments	FNTMP keepalive STUN processing
AMS-11193	Cluster deployments	Fixed status info from other servers in Element Manager Cluster Status
AMS-11196	All deployments	Radiobutton selection in DTMF codec config not working
AMS-11079	All deployments	Fixed multiple content uploading in Element Manager Media Management Provisioning
AMS-10660	All deployments	Fixed alarm info update in Element Manager Element Status for Chrome browsers
AMS-10634	Deployments with SNMP traps configured.	Fixed lock/unlock trap for SNMP route configuration in Element Manager
AMS-11065	All deployments	Fixed Element Manager console Page Not Found error
AMS-10741	Cluster deployments	Fixed incorrect URL for remote AAMS in Cluster Status
AMS-11038	All deployments	Update log4j2 to 2.17.1 for security vulnerability (CVE-2021-44832)
AMS-9422	FIPS deployments	Changes to simplify FIPS configuration by using the OS settings
AMS-10968	All deployments	Workers stalled during IvrMP post operations
AMS-10986	All deployments	Update log4j2 to 2.17.0 for security vulnerability (CVE-2021-45105)
AMS-10433	SNMP	SNMP queries do not work after config change
AMS-10950	All deployments	Update log4j2 to 2.16.0 for security vulnerability (CVE-2021-44228)

ID	Minimum conditions	Description
AMS-10825	All deployments	Fixed content deletion from a multi-level content group in Element Manager media management
AMS-10772	All deployments	Added Content-Security-Policy HTTP header
AMS-10851	All deployments	Removing incorrect audio path for monitor session
AMS-10242	Deployments using MRCP	Correction of major upgrade and information display in Element Manager for MRCP configuration
AMS-10280	Deployments using SELinux.	Set SELinux timer driver file context before loading
AMS-10579	All deployments	Fix Media Processing General Settings and Advanced Settings in Element Manager
AMS-10556	SIP deployments	Fix the deletion of SIP trusted nodes in Element Manager
AMS-10441	All deployments	Fix the help link on Element Manager welcome page and header
AMS-10746	All deployments	Mask SFTP password in debug logs
AMS-10742	All deployments	Update to prevent SQL injection through Element Manager
AMS-10482	All deployments	Address incorrect server.xml after major upgrade from 8.0.2 to 10.1
AMS-10714	All deployments	Remove incorrect hostname check against FQDN
AMS-10108	All deployments	Generate alarm if no scheduled backup task is defined for all backup types
AMS-10684	All deployments	Changes to default Diffie Hellman keylength to 2048
AMS-10636	All deployments	WebUa logs contain pwd info
AMS-10599	SNMP	Fix SNMP agent so it returns information from the interface MIB
AMS-10444	SNMP	Fixing action string of alarm 18982 for correct display in MIB browser
AMS-10509	Contact Center deployments	Prompts sound muffled after resampling
AMS-10276	All deployments	Log capture active session report doesn’t include GSLID.
AMS-9978	All deployments	DSCP is 0 in RTCP but RTP is 46 as expected on AMS 8.0.2 SP6

ID	Minimum conditions	Description
AMS-9937	All deployments	Avaya Media server is sending malformed headers on RTCP data

Fixes in System Layer for 10.1.0 SP 1 (10.0.0.8)

The following table lists the fixes in this release.

ID	Minimum conditions	Description
AMS-12313	All appliance deployments	Update RPMs to address security advisories RHSA-2022:5564 https://access.redhat.com/errata/RHSA-2022:5564 kernel-4.18.0-372.16.1.el8_6.x86_64 kernel-core-4.18.0-372.16.1.el8_6.x86_64 kernel-modules-4.18.0-372.16.1.el8_6.x86_64 python3-perf-4.18.0-372.16.1.el8_6.x86_64 https://access.redhat.com/security/cve/CVE-2022-1729 RHSA-2022:5813 https://access.redhat.com/errata/RHSA-2022:5813 vim-minimal-2:8.0.1763-19.el8_6.4.x86_64 https://access.redhat.com/security/cve/CVE-2022-1785 https://access.redhat.com/security/cve/CVE-2022-1897 https://access.redhat.com/security/cve/CVE-2022-1927 RHSA-2022:5819 https://access.redhat.com/errata/RHSA-2022:5819 kernel-4.18.0-372.19.1.el8_6.x86_64 kernel-core-4.18.0-372.19.1.el8_6.x86_64 kernel-modules-4.18.0-372.19.1.el8_6.x86_64 python3-perf-4.18.0-372.19.1.el8_6.x86_64 https://access.redhat.com/security/cve/CVE-2022-1012 https://access.redhat.com/security/cve/CVE-2022-32250 RHSA-2022:5818 https://access.redhat.com/errata/RHSA-2022:5818 openssl-1:1.1.1k-7.el8_6.x86_64 openssl-libs-1:1.1.1k-7.el8_6.i686 openssl-libs-1:1.1.1k-7.el8_6.x86_64 https://access.redhat.com/security/cve/CVE-2022-1292 https://access.redhat.com/security/cve/CVE-2022-2068 https://access.redhat.com/security/cve/CVE-2022-2097

ID	Minimum conditions	Description
		RHSA-2022:5809 https://access.redhat.com/errata/RHSA-2022:5809 pcre2-10.32-3.el8_6.i686 pcre2-10.32-3.el8_6.x86_64 https://access.redhat.com/security/cve/CVE-2022-1586 FEDORA-EPEL-2022-858300d946 – https://bodhi.fedoraproject.org/updates/FEDORA-EPEL-2022-858300d946 clamav-0.103.7-1.el8.x86_64.rpm clamav-lib-0.103.7-1.el8.x86_64.rpm clamav-data-0.103.7-1.el8.noarch.rpm clamav-filesystem-0.103.7-1.el8.noarch.rpm clamav-update-0.103.7-1.el8.x86_64.rpm
AMS-10867	JITC and FedRAMP deployments	STIG compliance – Investigate, install and configure usbguard.
AMS-10787	JITC and FedRAMP deployments	STIG compliance – SSH config updates V-230251, V-230252, V-230253
AMS-12236	All appliance deployments	RPM security updates RHSA-2022:0951 – https://access.redhat.com/errata/RHSA-2022:0951 expat-2.2.5-4.el8_5.3.x86_64 https://access.redhat.com/security/cve/CVE-2021-45960 https://access.redhat.com/security/cve/CVE-2021-46143 https://access.redhat.com/security/cve/CVE-2022-22822 https://access.redhat.com/security/cve/CVE-2022-22823 https://access.redhat.com/security/cve/CVE-2022-22824 https://access.redhat.com/security/cve/CVE-2022-22825 https://access.redhat.com/security/cve/CVE-2022-22826 https://access.redhat.com/security/cve/CVE-2022-22827 https://access.redhat.com/security/cve/CVE-2022-23852 https://access.redhat.com/security/cve/CVE-2022-25235 https://access.redhat.com/security/cve/CVE-2022-25236 https://access.redhat.com/security/cve/CVE-2022-25315 RHSA-2022:1065 – https://access.redhat.com/errata/RHSA-2022:1065 openssl-libs-1:1.1.1k-6.el8_5.x86_64 openssl-libs-1:1.1.1k-6.el8_5.i686 openssl-1:1.1.1k-6.el8_5.x86_64 https://access.redhat.com/security/cve/CVE-2022-0778

ID	Minimum conditions	Description
		RHSA-2022:1537 – https://access.redhat.com/errata/RHSA-2022:1537 gzip-1.9-13.el8_5.x86_64 https://access.redhat.com/security/cve/CVE-2022-1271 RHSA-2022:1546 – https://access.redhat.com/errata/RHSA-2022:1546 polkit-0.115-13.el8_5.2.x86_64 polkit-libs-0.115-13.el8_5.2.x86_64 https://access.redhat.com/security/cve/CVE-2021-4115 RHSA-2022:1550 – https://access.redhat.com/errata/RHSA-2022:1550 kernel-4.18.0-348.23.1.el8_5.x86_64 kernel-core-4.18.0-348.23.1.el8_5.x86_64 python3-perf-4.18.0-348.23.1.el8_5.x86_64 kernel-modules-4.18.0-348.23.1.el8_5.x86_64 https://access.redhat.com/security/cve/CVE-2021-4028 https://access.redhat.com/security/cve/CVE-2022-25636 RHSA-2022:1552 – https://access.redhat.com/errata/RHSA-2022:1552 vim-minimal-2:8.0.1763-16.el8_5.13.x86_64 https://access.redhat.com/security/cve/CVE-2022-1154 RHSA-2022:1642 – https://access.redhat.com/errata/RHSA-2022:1642 zlib-1.2.11-18.el8_5.i686 zlib-1.2.11-18.el8_5.x86_64 https://access.redhat.com/security/cve/CVE-2018-25032 RHSA-2022:1821 – https://access.redhat.com/errata/RHSA-2022:1821 python2-pip-wheel-9.0.3-19.module+el8.6.0+13001+ad200bd9.noarch python2-libs-2.7.18-10.module+el8.6.0+14191+7fdd52cd.x86_64 python2-pip-9.0.3-19.module+el8.6.0+13001+ad200bd9.noarch python2-2.7.18-10.module+el8.6.0+14191+7fdd52cd.x86_64 https://access.redhat.com/security/cve/CVE-2021-3733 https://access.redhat.com/security/cve/CVE-2021-3737 https://access.redhat.com/security/cve/CVE-2021-4189 https://access.redhat.com/security/cve/CVE-2021-43818 https://access.redhat.com/security/cve/CVE-2022-0391 RHSA-2022:1961 – https://access.redhat.com/errata/RHSA-2022:1961 cairo-1.15.12-6.el8.x86_64

ID	Minimum conditions	Description
		pixman-0.38.4-2.el8.x86_64 https://access.redhat.com/security/cve/CVE-2020-35492 RHSA-2022:1986 – https://access.redhat.com/errata/RHSA-2022:1986 python3-libs-3.6.8-45.el8.x86_64 platform-python-3.6.8-45.el8.x86_64 https://access.redhat.com/security/cve/CVE-2021-3737 https://access.redhat.com/security/cve/CVE-2021-4189 RHSA-2022:1988 – https://access.redhat.com/errata/RHSA-2022:1988 kernel-4.18.0-372.9.1.el8.x86_64 kernel-core-4.18.0-372.9.1.el8.x86_64 kernel-modules-4.18.0-372.9.1.el8.x86_64 python3-perf-4.18.0-372.9.1.el8.x86_64 https://access.redhat.com/security/cve/CVE-2020-0404 https://access.redhat.com/security/cve/CVE-2020-13974 https://access.redhat.com/security/cve/CVE-2020-27820 https://access.redhat.com/security/cve/CVE-2020-4788 https://access.redhat.com/security/cve/CVE-2021-0941 https://access.redhat.com/security/cve/CVE-2021-20322 https://access.redhat.com/security/cve/CVE-2021-21781 https://access.redhat.com/security/cve/CVE-2021-26401 https://access.redhat.com/security/cve/CVE-2021-29154 https://access.redhat.com/security/cve/CVE-2021-3612 https://access.redhat.com/security/cve/CVE-2021-3669 https://access.redhat.com/security/cve/CVE-2021-37159 https://access.redhat.com/security/cve/CVE-2021-3743 https://access.redhat.com/security/cve/CVE-2021-3744 https://access.redhat.com/security/cve/CVE-2021-3752 https://access.redhat.com/security/cve/CVE-2021-3759 https://access.redhat.com/security/cve/CVE-2021-3764 https://access.redhat.com/security/cve/CVE-2021-3772 https://access.redhat.com/security/cve/CVE-2021-3773 https://access.redhat.com/security/cve/CVE-2021-4002 https://access.redhat.com/security/cve/CVE-2021-4037 https://access.redhat.com/security/cve/CVE-2021-4083 https://access.redhat.com/security/cve/CVE-2021-4157 https://access.redhat.com/security/cve/CVE-2021-41864 https://access.redhat.com/security/cve/CVE-2021-4197

ID	Minimum conditions	Description
		https://access.redhat.com/security/cve/CVE-2021-4203 https://access.redhat.com/security/cve/CVE-2021-42739 https://access.redhat.com/security/cve/CVE-2021-43056 https://access.redhat.com/security/cve/CVE-2021-43389 https://access.redhat.com/security/cve/CVE-2021-43976 https://access.redhat.com/security/cve/CVE-2021-44733 https://access.redhat.com/security/cve/CVE-2021-45485 https://access.redhat.com/security/cve/CVE-2021-45486 https://access.redhat.com/security/cve/CVE-2022-0001 https://access.redhat.com/security/cve/CVE-2022-0002 https://access.redhat.com/security/cve/CVE-2022-0286 https://access.redhat.com/security/cve/CVE-2022-0322 https://access.redhat.com/security/cve/CVE-2022-1011 RHSA-2022:1991 – https://access.redhat.com/errata/RHSA-2022:1991 cpio-2.12-11.el8.x86_64 https://access.redhat.com/security/cve/CVE-2021-38185 RHSA-2022:2013 – https://access.redhat.com/errata/RHSA-2022:2013 openssh-clients-8.0p1-13.el8.x86_64 openssh-8.0p1-13.el8.x86_64 openssh-server-8.0p1-13.el8.x86_64 https://access.redhat.com/security/cve/CVE-2021-41617 RHSA-2022:2031 – https://access.redhat.com/errata/RHSA-2022:2031 libssh-0.9.6-3.el8.i686 libssh-config-0.9.6-3.el8.noarch libssh-0.9.6-3.el8.x86_64 https://access.redhat.com/security/cve/CVE-2021-3634 RHSA-2022:2043 – https://access.redhat.com/errata/RHSA-2022:2043 c-ares-1.13.0-6.el8.x86_64 https://access.redhat.com/security/cve/CVE-2021-3672 RHSA-2022:2092 – https://access.redhat.com/errata/RHSA-2022:2092 bind-license-32:9.11.36-3.el8.noarch bind-32:9.11.36-3.el8.x86_64 bind-libs-32:9.11.36-3.el8.x86_64 python3-bind-32:9.11.36-3.el8.noarch

ID	Minimum conditions	Description
		bind-libs-lite-32:9.11.36-3.el8.x86_64 bind-utils-32:9.11.36-3.el8.x86_64 https://access.redhat.com/security/cve/CVE-2021-25219 RHSA-2022:2110 – https://access.redhat.com/errata/RHSA-2022:2110 grub2-pc-1:2.02-123.el8.x86_64 grub2-pc-modules-1:2.02-123.el8.noarch grub2-tools-minimal-1:2.02-123.el8.x86_64 grub2-tools-1:2.02-123.el8.x86_64 grub2-common-1:2.02-123.el8.noarch grub2-tools-extra-1:2.02-123.el8.x86_64 grub2-tools-efi-1:2.02-123.el8.x86_64 https://access.redhat.com/security/cve/CVE-2021-3981 RHSA-2022:4799 – https://access.redhat.com/errata/RHSA-2022:4799 rsyslog-8.2102.0-7.el8_6.1.x86_64 rsyslog-gnutls-8.2102.0-7.el8_6.1.x86_64 https://access.redhat.com/security/cve/CVE-2022-24903 RHSA-2022:4991 – https://access.redhat.com/errata/RHSA-2022:4991 xz-5.2.4-4.el8_6.x86_64 xz-libs-5.2.4-4.el8_6.x86_64 https://access.redhat.com/security/cve/CVE-2022-1271 RHSA-2022:5095 – https://access.redhat.com/errata/RHSA-2022:5095 grub2-pc-1:2.02-123.el8_6.8.x86_64 grub2-tools-1:2.02-123.el8_6.8.x86_64 grub2-common-1:2.02-123.el8_6.8.noarch grub2-tools-efi-1:2.02-123.el8_6.8.x86_64 grub2-tools-extra-1:2.02-123.el8_6.8.x86_64 grub2-pc-modules-1:2.02-123.el8_6.8.noarch grub2-tools-minimal-1:2.02-123.el8_6.8.x86_64 https://access.redhat.com/security/cve/CVE-2021-3695 https://access.redhat.com/security/cve/CVE-2021-3696 https://access.redhat.com/security/cve/CVE-2021-3697 https://access.redhat.com/security/cve/CVE-2022-28733 https://access.redhat.com/security/cve/CVE-2022-28734 https://access.redhat.com/security/cve/CVE-2022-28735 https://access.redhat.com/security/cve/CVE-2022-28736

ID	Minimum conditions	Description
		https://access.redhat.com/security/cve/CVE-2022-28737 RHSA-2022:5311 – https://access.redhat.com/errata/RHSA-2022:5311 libgcrypt-1.8.5-7.el8_6.x86_64 https://access.redhat.com/security/cve/CVE-2021-40528 RHSA-2022:5313 – https://access.redhat.com/errata/RHSA-2022:5313 curl-7.61.1-22.el8_6.3.x86_64 libcurl-7.61.1-22.el8_6.3.x86_64 libcurl-7.61.1-22.el8_6.3.i686 https://access.redhat.com/security/cve/CVE-2022-22576 https://access.redhat.com/security/cve/CVE-2022-27774 https://access.redhat.com/security/cve/CVE-2022-27776 https://access.redhat.com/security/cve/CVE-2022-27782 RHSA-2022:5314 – https://access.redhat.com/errata/RHSA-2022:5314 expat-2.2.5-8.el8_6.2.x86_64 https://access.redhat.com/security/cve/CVE-2022-25313 https://access.redhat.com/security/cve/CVE-2022-25314 RHSA-2022:5316 – https://access.redhat.com/errata/RHSA-2022:5316 kernel-modules-4.18.0-372.13.1.el8_6.x86_64 kernel-core-4.18.0-372.13.1.el8_6.x86_64 kernel-4.18.0-372.13.1.el8_6.x86_64 python3-perf-4.18.0-372.13.1.el8_6.x86_64 https://access.redhat.com/security/cve/CVE-2020-28915 https://access.redhat.com/security/cve/CVE-2022-27666 RHSA-2022:5317 – https://access.redhat.com/errata/RHSA-2022:5317 libxml2-2.9.7-13.el8_6.1.x86_64 python3-libxml2-2.9.7-13.el8_6.1.x86_64 https://access.redhat.com/security/cve/CVE-2022-29824 RHSA-2022:5319 – https://access.redhat.com/errata/RHSA-2022:5319 vim-minimal-2:8.0.1763-19.el8_6.2.x86_64 https://access.redhat.com/security/cve/CVE-2022-1621 https://access.redhat.com/security/cve/CVE-2022-1629 FEDORA-EPEL-2022-334a36ba83 –

ID	Minimum conditions	Description
		https://bodhi.fedoraproject.org/updates/FEDORA-EPEL-2022-334a36ba83 clamav-0.103.6-1.el8.x86_64.rpm clamav-data-0.103.6-1.el8.noarch.rpm clamav-filesystem-0.103.6-1.el8.noarch.rpm clamav-lib-0.103.6-1.el8.x86_64.rpm clamav-update-0.103.6-1.el8.x86_64.rpm https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20785 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20771 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20796 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20770

Fixes in Media Server for 10.1.0 SP 1 (10.1.0.101)

The following table lists the fixes in this release.

ID	Minimum conditions	Description
AMS-12157	WebRTC deployments	FNTMP crashed on turn allocation timer.
AMS-12192	All deployments	Disallow HTTP Options method in Element Manager.
AMS-12134	All deployments	Fixed applying destination config change to existing scheduled backup tasks.
AMS-12136	All deployments	MSML failed to stop tonegen in individual tone mode.
AMS-11939	JITC and FedRAMP deployments	Added proxy handling in Tomcat server.xml as needed..
AMS-11083	Appliance deployments.	Audit logging for changes to specific Tomcat folders
AMS-12101	JITC and FedRAMP deployments	Fixed a typo in the confirmation message for enabling FIPS mode in Element Manager
AMS-12073	WebRTC deployments	Fixed the missing Element Manager task Web Collaboration
AMS-12026	All deployments	OpenJDK security update
AMS-4893	All deployments	Use log4j2 for Tomcat system out/error log for rollover handling
AMS-12019	All deployments	MSML tonegen aborting play request

ID	Minimum conditions	Description
AMS-12008	Deployments using CRL	Fixed the CRL import for a CA certificate in Element Manager
AMS-10766	All deployments	Update 3rd party license file and generate report from BD hub
AMS-11456	All deployments	Tomcat security update
AMS-11934	Deployments using Element Manager media management. Provisioning	Fix sequential file upload in Element Manager Media Management Provisioning
AMS-11897	All deployments	Update System Manager tmclient libraries for the use of log4j2
AMS-11063	All deployments	Enable Java Security Manager for AMS Tomcat by default
AMS-11755	All deployments	Removed MS Silverlight plugins from Avaya Aura Media Server
AMS-11750	All deployments	Removed weak ciphers and fixed HTTP headers for Element Manager
AMS-11695	All deployments	Fixed Element Manager Monitoring Operational Measurements refresh issue
AMS-11633	All deployments	Correctly manage msml <createconference> command in lock state
AMS-11656	All deployments	Fixed Element Manager database updates for app trace config and backup/restore logs
AMS-11507	Appliance deployments	Cleanup pvichecker artifacts after upgrade

Fixes in System Layer for 10.1.0 SP 2 (10.0.0.11)

The following table lists the fixes in this release.

ID	Minimum conditions	Description
AMS-12718	Appliance deployments	Disable SHA1 KEX crypto for SSH
AMS-12781	Appliance deployments with static routes upgrading from 8.0.x.	Restore static routes on major release upgrade
AMS-12003	New virtual appliance deployments.	Update OVA hashes to use sha256
N/A	Appliance deployments	Other security updates:

ID	Minimum conditions	Description
		RHSA-2022:7622 https://access.redhat.com/errata/RHSA-2022:7622 python3-unbound-1.16.2-2.el8.x86_64 unbound-libs-1.16.2-2.el8.x86_64 https://access.redhat.com/security/cve/CVE-2022-30698 https://access.redhat.com/security/cve/CVE-2022-30699 RHSA-2022:8638 https://access.redhat.com/errata/RHSA-2022:8638 krb5-libs-1.18.2-22.el8_7.i686 krb5-libs-1.18.2-22.el8_7.x86_64 https://access.redhat.com/security/cve/CVE-2022-42898
AMS-11705	Physical Appliance deployments	Add SSH enable script for ASP
N/A	Appliance Deployments	Other security updates: RHSA-2022:5095 https://access.redhat.com/errata/RHSA-2022:5095 mokutil-1:0.3.0-11.el8_6.1.x86_64 shim-x64-15.6-1.el8.x86_64 https://access.redhat.com/security/cve/CVE-2021-3695 https://access.redhat.com/security/cve/CVE-2021-3696 https://access.redhat.com/security/cve/CVE-2021-3697 https://access.redhat.com/security/cve/CVE-2022-28733 https://access.redhat.com/security/cve/CVE-2022-28734 https://access.redhat.com/security/cve/CVE-2022-28735 https://access.redhat.com/security/cve/CVE-2022-28736 https://access.redhat.com/security/cve/CVE-2022-28737 RHSA-2022:7482 https://access.redhat.com/errata/RHSA-2022:7482 qt5-srpm-macros-5.15.3-1.el8.noarch https://access.redhat.com/security/cve/CVE-2022-25255 RHSA-2022:7700 https://access.redhat.com/errata/RHSA-2022:7700 gdisk-1.0.3-11.el8.x86_64 https://access.redhat.com/security/cve/CVE-2020-0256 https://access.redhat.com/security/cve/CVE-2021-0308 RHSA-2022:7704 https://access.redhat.com/errata/RHSA-2022:7704 glib2-2.56.4-159.el8.x86_64 https://access.redhat.com/security/cve/CVE-2022-22624 https://access.redhat.com/security/cve/CVE-2022-22628

ID	Minimum conditions	Description
		https://access.redhat.com/security/cve/CVE-2022-22629 https://access.redhat.com/security/cve/CVE-2022-22662 https://access.redhat.com/security/cve/CVE-2022-26700 https://access.redhat.com/security/cve/CVE-2022-26709 https://access.redhat.com/security/cve/CVE-2022-26710 https://access.redhat.com/security/cve/CVE-2022-26716 https://access.redhat.com/security/cve/CVE-2022-26717 https://access.redhat.com/security/cve/CVE-2022-26719 https://access.redhat.com/security/cve/CVE-2022-30293 RHSA-2022:1820 https://access.redhat.com/errata/RHSA-2022:1820 libudisks2-2.9.0-9.el8.x86_64 udisks2-2.9.0-9.el8.x86_64 https://access.redhat.com/security/cve/CVE-2021-3802 RHSA-2022:7928 https://access.redhat.com/errata/RHSA-2022:7928 kpartx-0.8.4-28.el8_7.1.x86_64 https://access.redhat.com/security/cve/CVE-2022-3787 RHSA-2022:7593 https://access.redhat.com/errata/RHSA-2022:7593 python2-2.7.18-11.module+el8.7.0+15681+7a92afba.x86_64 python2-libs-2.7.18-11.module+el8.7.0+15681+7a92afba.x86_64 https://access.redhat.com/security/cve/CVE-2015-20107 RHSA-2022:7715 https://access.redhat.com/errata/RHSA-2022:7715 libxml2-2.9.7-15.el8.x86_64 python3-libxml2-2.9.7-15.el8.x86_64 https://access.redhat.com/security/cve/CVE-2016-3709 RHSA-2022:7790 https://access.redhat.com/errata/RHSA-2022:7790 bind-32:9.11.36-5.el8.x86_64 bind-libs-32:9.11.36-5.el8.x86_64 bind-libs-lite-32:9.11.36-5.el8.x86_64 bind-license-32:9.11.36-5.el8.noarch bind-utils-32:9.11.36-5.el8.x86_64 python3-bind-32:9.11.36-5.el8.noarch https://access.redhat.com/security/cve/CVE-2021-25220 RHSA-2022:7514 https://access.redhat.com/errata/RHSA-2022:7514

ID	Minimum conditions	Description
		fribidi-1.0.4-9.el8.x86_64 https://access.redhat.com/security/cve/CVE-2022-25308 https://access.redhat.com/security/cve/CVE-2022-25309 https://access.redhat.com/security/cve/CVE-2022-25310 RHSA-2022:7464 https://access.redhat.com/errata/RHSA-2022:7464 protobuf-3.5.0-15.el8.x86_64 https://access.redhat.com/security/cve/CVE-2021-22570 RHSA-2022:7745 https://access.redhat.com/errata/RHSA-2022:7745 freetype-2.9.1-9.el8.x86_64 https://access.redhat.com/security/cve/CVE-2022-27404 https://access.redhat.com/security/cve/CVE-2022-27405 https://access.redhat.com/security/cve/CVE-2022-27406 RHSA-2022:7720 https://access.redhat.com/errata/RHSA-2022:7720 e2fsprogs-1.45.6-5.el8.x86_64 e2fsprogs-libs-1.45.6-5.el8.i686 e2fsprogs-libs-1.45.6-5.el8.x86_64 libcom_err-1.45.6-5.el8.i686 libcom_err-1.45.6-5.el8.x86_64 libss-1.45.6-5.el8.x86_64 https://access.redhat.com/security/cve/CVE-2022-1304 RHSA-2022:7683 https://access.redhat.com/errata/RHSA-2022:7683 kernel-4.18.0-425.3.1.el8.x86_64 kernel-core-4.18.0-425.3.1.el8.x86_64 kernel-modules-4.18.0-425.3.1.el8.x86_64 python3-perf-4.18.0-425.3.1.el8.x86_64 https://access.redhat.com/security/cve/CVE-2020-36516 https://access.redhat.com/security/cve/CVE-2020-36558 https://access.redhat.com/security/cve/CVE-2021-30002 https://access.redhat.com/security/cve/CVE-2021-3640 https://access.redhat.com/security/cve/CVE-2022-0168 https://access.redhat.com/security/cve/CVE-2022-0617 https://access.redhat.com/security/cve/CVE-2022-0854 https://access.redhat.com/security/cve/CVE-2022-1016 https://access.redhat.com/security/cve/CVE-2022-1048 https://access.redhat.com/security/cve/CVE-2022-1055

ID	Minimum conditions	Description
		https://access.redhat.com/security/cve/CVE-2022-1184 https://access.redhat.com/security/cve/CVE-2022-1852 https://access.redhat.com/security/cve/CVE-2022-20368 https://access.redhat.com/security/cve/CVE-2022-2078 https://access.redhat.com/security/cve/CVE-2022-21499 https://access.redhat.com/security/cve/CVE-2022-23960 https://access.redhat.com/security/cve/CVE-2022-24448 https://access.redhat.com/security/cve/CVE-2022-2586 https://access.redhat.com/security/cve/CVE-2022-26373 https://access.redhat.com/security/cve/CVE-2022-2639 https://access.redhat.com/security/cve/CVE-2022-27950 https://access.redhat.com/security/cve/CVE-2022-28390 https://access.redhat.com/security/cve/CVE-2022-28893 https://access.redhat.com/security/cve/CVE-2022-2938 https://access.redhat.com/security/cve/CVE-2022-29581 https://access.redhat.com/security/cve/CVE-2022-36946
AMS-10786	Appliance deployments	STIG compliance – module blacklisting
AMS-10788	Appliance deployments	STIG compliance – systemd and core dump config updates
AMS-10789	Appliance deployments	STIG compliance – Various config file updates (rsyslog, chrony,...)
AMS-10790	Appliance deployments	STIG compliance – Partition permission configuration
AMS-12596	Appliance deployments	Update RPMs to address security advisories RHSA-2022:6878 https://access.redhat.com/errata/RHSA-2022:6878 expat-2.2.5-8.el8_6.3.x86_64 https://access.redhat.com/security/cve/CVE-2022-40674 RHSA-2022:7110 https://access.redhat.com/errata/RHSA-2022:7110 kernel-4.18.0-372.32.1.el8_6.x86_64 kernel-core-4.18.0-372.32.1.el8_6.x86_64 kernel-modules-4.18.0-372.32.1.el8_6.x86_64 python3-perf-4.18.0-372.32.1.el8_6.x86_64 https://access.redhat.com/security/cve/CVE-2022-0494 https://access.redhat.com/security/cve/CVE-2022-1353 https://access.redhat.com/security/cve/CVE-2022-23816 https://access.redhat.com/security/cve/CVE-2022-23825 https://access.redhat.com/security/cve/CVE-2022-2588

ID	Minimum conditions	Description
		https://access.redhat.com/security/cve/CVE-2022-29900 https://access.redhat.com/security/cve/CVE-2022-29901 RHSA-2022:6460 https://access.redhat.com/errata/RHSA-2022:6460 kernel-4.18.0-372.26.1.el8_6.x86_64 kernel-core-4.18.0-372.26.1.el8_6.x86_64 kernel-modules-4.18.0-372.26.1.el8_6.x86_64 python3-perf-4.18.0-372.26.1.el8_6.x86_64 https://access.redhat.com/security/cve/CVE-2022-21123 https://access.redhat.com/security/cve/CVE-2022-21125 https://access.redhat.com/security/cve/CVE-2022-21166 RHSA-2022:6778 https://access.redhat.com/errata/RHSA-2022:6778 bind-32:9.11.36-3.el8_6.1.x86_64 bind-libs-32:9.11.36-3.el8_6.1.x86_64 bind-libs-lite-32:9.11.36-3.el8_6.1.x86_64 bind-license-32:9.11.36-3.el8_6.1.noarch bind-utils-32:9.11.36-3.el8_6.1.x86_64 python3-bind-32:9.11.36-3.el8_6.1.noarch https://access.redhat.com/security/cve/CVE-2022-38177 https://access.redhat.com/security/cve/CVE-2022-38178 RHSA-2022:6463 https://access.redhat.com/errata/RHSA-2022:6463 gnupg2-2.2.20-3.el8_6.x86_64 gnupg2-smime-2.2.20-3.el8_6.x86_64 https://access.redhat.com/security/cve/CVE-2022-34903 RHSA-2022:7192 https://access.redhat.com/errata/RHSA-2022:7192 kpartx-0.8.4-22.el8_6.2.x86_64 https://access.redhat.com/security/cve/CVE-2022-41974 RHSA-2022:7089 https://access.redhat.com/errata/RHSA-2022:7089 libksba-1.3.5-8.el8_6.x86_64 https://access.redhat.com/security/cve/CVE-2022-3515 RHSA-2022:6357 https://access.redhat.com/errata/RHSA-2022:6357 open-vm-tools-11.3.5-1.el8_6.1.x86_64 https://access.redhat.com/security/cve/CVE-2022-31676

ID	Minimum conditions	Description
		RHSA-2022:6457 https://access.redhat.com/errata/RHSA-2022:6457 platform-python-3.6.8-47.el8_6.x86_64 python3-libs-3.6.8-47.el8_6.x86_64 https://access.redhat.com/security/cve/CVE-2015-20107 https://access.redhat.com/security/cve/CVE-2022-0391 RHSA-2022:6159 https://access.redhat.com/errata/RHSA-2022:6159 curl-7.61.1-22.el8_6.4.x86_64 libcurl-7.61.1-22.el8_6.4.i686 libcurl-7.61.1-22.el8_6.4.x86_64 https://access.redhat.com/security/cve/CVE-2022-32206 https://access.redhat.com/security/cve/CVE-2022-32208 RHSA-2022:6206 https://access.redhat.com/errata/RHSA-2022:6206 systemd-239-58.el8_6.4.x86_64 systemd-libs-239-58.el8_6.4.x86_64 systemd-pam-239-58.el8_6.4.x86_64 systemd-udev-239-58.el8_6.4.x86_64 https://access.redhat.com/security/cve/CVE-2022-2526 RHSA-2022:7108 https://access.redhat.com/errata/RHSA-2022:7108 sqlite-3.26.0-16.el8_6.x86_64 sqlite-libs-3.26.0-16.el8_6.x86_64 https://access.redhat.com/security/cve/CVE-2020-35525 https://access.redhat.com/security/cve/CVE-2020-35527 RHSA-2022:7105 https://access.redhat.com/errata/RHSA-2022:7105 gnutls-3.6.16-5.el8_6.x86_64 https://access.redhat.com/security/cve/CVE-2022-2509 RHSA-2022:7106 https://access.redhat.com/errata/RHSA-2022:7106 zlib-1.2.11-19.el8_6.i686 zlib-1.2.11-19.el8_6.x86_64 https://access.redhat.com/security/cve/CVE-2022-37434

Fixes in Media Server for 10.1.0 SP 2 (10.1.0.125)

The following table lists the fixes in this release.

ID	Minimum conditions	Description
AMS-13035	All deployments	Fix destination configuration for Element Manager backup tasks
AMS-12995	All deployments	Party IVR call failure when PCMU/G.722 is disabled in media configuration
AMS-12906	Deployments using Element Manger media management	Fix Element Manager media management batch file provisioning issue
AMS-12793	All deployments	Fix CA certificate import with non-UTC date type in certificate
AMS-12699	All deployments	Fix Tomcat SSL cipher update in major upgrade
AMS-12526	All deployments	Disable TLSv1.0 and insecure TLSv1.2 DHE ciphers
AMS-12655	All deployments	Security update with Spring Frameworks for CVE-22950 and CVE-22971
AMS-10288	All deployments	‘License Expired’ alarm not cleared after refreshing license
AMS-12047	Deploments upgrading from 8.0.x with FIPS enabled.	Manage correctly FIPS in amsupgrade tool
AMS-12435	Deployments using WebRTC	Increase number of media formats supported for WebRTC calls
AMS-12460	All deployments	Restore config parameters in Element Manager UI that are missing in Element Manager migration
AMS-12518	IVR deployments	Duplicate digit detection caused by out of order RFC 2833 packet
AMS-12507	Breeze deployments	MSML interpreter crashed by play request with an invalid cstore url
AMS-12494	All deployments	Element Manager SDR monitoring incomplete data
AMS-12449	All deployments	Prevent WebUA crash when a session is deleted using Element Manager.
AMS-11621	Appliance deployments	Add Element Manager audit logs for appliance software update stage and install.
AMS-12378	All deployments	Restore table data sorting and fix radiobutton size in Element Manager tasks
AMS-12413	AACC Agent Greeting deployments.	Agent Greeting prompt recording failed after upgrade to AMS 10.1.077

ID	Minimum conditions	Description
AMS-12409	1+1 HA deployments	SIP slow-start re-INVITE failed after HA failover
AMS-12275	Deployments requiring SFTP rsa-sha2-256/rsa-sha2-512 algorithm.	Add rsa-sha2-256/rsa-sha2-512 algorithm support for remote backup SFTP
AMS-12252 AMS-12290	All deployments	Addresses Element Manager Look-and-Feel styling
AMS-12425	Deployments using WebRTC	WebRTC media session and MPU resource leak.

Fixes in System Layer for 10.1.0 SP 3 (10.0.0.12)

The following table lists the fixes in this release.

ID	Minimum conditions	Description
AMS-13321	Appliance deployments	Include sysstat package
AMS-13164	Appliance deployments	Update system layer to address various vulnerabilities RHSA-2023:0087 https://access.redhat.com/errata/RHSA-2023:0087 usbguard-1.0.0-8.el8_7.2.x86_64 usbguard-selinux-1.0.0-8.el8_7.2.noarch https://access.redhat.com/security/cve/CVE-2019-25058 RHSA-2023:0116 https://access.redhat.com/errata/RHSA-2023:0116 libtasn1-4.13-4.el8_7.x86_64 https://access.redhat.com/security/cve/CVE-2021-46848 RHSA-2023:0049 https://access.redhat.com/errata/RHSA-2023:0049 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-efi-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 https://access.redhat.com/security/cve/CVE-2022-2601 https://access.redhat.com/security/cve/CVE-2022-3775

ID	Minimum conditions	Description
		RHSA-2023:0101 https://access.redhat.com/errata/RHSA-2023:0101 kernel-4.18.0-425.10.1.el8_7.x86_64 kernel-core-4.18.0-425.10.1.el8_7.x86_64 kernel-modules-4.18.0-425.10.1.el8_7.x86_64 python3-perf-4.18.0-425.10.1.el8_7.x86_64 https://access.redhat.com/security/cve/CVE-2022-2964 https://access.redhat.com/security/cve/CVE-2022-4139 RHSA-2023:0100 https://access.redhat.com/errata/RHSA-2023:0100 systemd-239-68.el8_7.1.x86_64 systemd-libs-239-68.el8_7.1.x86_64 systemd-pam-239-68.el8_7.1.x86_64 systemd-udev-239-68.el8_7.1.x86_64 https://access.redhat.com/security/cve/CVE-2022-3821 RHSA-2023:0110 https://access.redhat.com/errata/RHSA-2023:0110 sqlite-3.26.0-17.el8_7.x86_64 sqlite-libs-3.26.0-17.el8_7.x86_64 https://access.redhat.com/security/cve/CVE-2022-35737 RHSA-2023:0173 https://access.redhat.com/errata/RHSA-2023:0173 libxml2-2.9.7-15.el8_7.1.x86_64 python3-libxml2-2.9.7-15.el8_7.1.x86_64 https://access.redhat.com/security/cve/CVE-2022-40303 https://access.redhat.com/security/cve/CVE-2022-40304 RHSA-2023:0096 https://access.redhat.com/errata/RHSA-2023:0096 dbus-1:1.12.8-23.el8_7.1.x86_64 dbus-common-1:1.12.8-23.el8_7.1.noarch dbus-daemon-1:1.12.8-23.el8_7.1.x86_64 dbus-libs-1:1.12.8-23.el8_7.1.x86_64 dbus-tools-1:1.12.8-23.el8_7.1.x86_64 https://access.redhat.com/security/cve/CVE-2022-42010 https://access.redhat.com/security/cve/CVE-2022-42011 https://access.redhat.com/security/cve/CVE-2022-42012 RHSA-2023:0103 https://access.redhat.com/errata/RHSA-2023:0103 expat-2.2.5-10.el8_7.1.x86_64

ID	Minimum conditions	Description
		https://access.redhat.com/security/cve/CVE-2022-43680 RHSA-2023:0284 https://access.redhat.com/errata/RHSA-2023:0284 sudo-1.8.29-8.el8_7.1.x86_64 https://access.redhat.com/security/cve/CVE-2023-22809 FEDORA-EPEL-2023-5cb6798308 https://bodhi.fedoraproject.org/updates/FEDORA-EPEL-2023-5cb6798308 clamav-0.103.8-3.el8.x86_64.rpm clamav-data-0.103.8-3.el8.noarch.rpm clamav-filesystem-0.103.8-3.el8.noarch.rpm clamav-lib-0.103.8-3.el8.x86_64.rpm clamav-update-0.103.8-3.el8.x86_64.rpm Other security updates: RHSA-2023:1405 https://access.redhat.com/errata/RHSA-2023:1405 openssl-1:1.1.1k-9.el8_7.x86_64 openssl-libs-1:1.1.1k-9.el8_7.i686 openssl-libs-1:1.1.1k-9.el8_7.x86_64 https://access.redhat.com/security/cve/CVE-2022-4304 https://access.redhat.com/security/cve/CVE-2022-4450 https://access.redhat.com/security/cve/CVE-2023-0215 https://access.redhat.com/security/cve/CVE-2023-0286 RHSA-2023:1140 https://access.redhat.com/errata/RHSA-2023:1140 curl-7.61.1-25.el8_7.3.x86_64 libcurl-7.61.1-25.el8_7.3.i686 libcurl-7.61.1-25.el8_7.3.x86_64 https://access.redhat.com/security/cve/CVE-2023-23916 RHSA-2023:0837 https://access.redhat.com/errata/RHSA-2023:0837 systemd-239-68.el8_7.4.x86_64 systemd-libs-239-68.el8_7.4.x86_64 systemd-pam-239-68.el8_7.4.x86_64 systemd-udev-239-68.el8_7.4.x86_64 https://access.redhat.com/security/cve/CVE-2022-4415

ID	Minimum conditions	Description
		RHSA-2023:0835 https://access.redhat.com/errata/RHSA-2023:0835 platform-python-setuptools-39.2.0-6.el8_7.1.noarch python3-setuptools-wheel-39.2.0-6.el8_7.1.noarch https://access.redhat.com/security/cve/CVE-2022-40897 RHSA-2023:1252 https://access.redhat.com/errata/RHSA-2023:1252 nss-3.79.0-11.el8_7.x86_64 nss-softokn-3.79.0-11.el8_7.x86_64 nss-softokn-freebl-3.79.0-11.el8_7.x86_64 nss-sysinit-3.79.0-11.el8_7.x86_64 nss-util-3.79.0-11.el8_7.x86_64 https://access.redhat.com/security/cve/CVE-2023-0767 RHSA-2023:0833 https://access.redhat.com/errata/RHSA-2023:0833 platform-python-3.6.8-48.el8_7.1.x86_64 python3-libs-3.6.8-48.el8_7.1.x86_64 https://access.redhat.com/security/cve/CVE-2020-10735 https://access.redhat.com/security/cve/CVE-2021-28861 https://access.redhat.com/security/cve/CVE-2022-45061 RHSA-2023:0832 https://access.redhat.com/errata/RHSA-2023:0832 kernel-4.18.0-425.13.1.el8_7.x86_64 kernel-core-4.18.0-425.13.1.el8_7.x86_64 kernel-modules-4.18.0-425.13.1.el8_7.x86_64 python3-perf-4.18.0-425.13.1.el8_7.x86_64 https://access.redhat.com/security/cve/CVE-2022-2873 https://access.redhat.com/security/cve/CVE-2022-41222 https://access.redhat.com/security/cve/CVE-2022-43945 RHSA-2023:1569 https://access.redhat.com/errata/RHSA-2023:1569 gnutls-3.6.16-6.el8_7.x86_64 https://access.redhat.com/security/cve/CVE-2023-0361 RHSA-2023:1566 https://access.redhat.com/errata/RHSA-2023:1566 kernel-4.18.0-425.19.2.el8_7.x86_64 kernel-core-4.18.0-425.19.2.el8_7.x86_64 kernel-modules-4.18.0-425.19.2.el8_7.x86_64 python3-perf-4.18.0-425.19.2.el8_7.x86_64

ID	Minimum conditions	Description
		https://access.redhat.com/security/cve/CVE-2022-4269 https://access.redhat.com/security/cve/CVE-2022-4378 https://access.redhat.com/security/cve/CVE-2023-0266 https://access.redhat.com/security/cve/CVE-2023-0386 RHSA-2023:0625 https://access.redhat.com/errata/RHSA-2023:0625 libksba-1.3.5-9.el8_7.x86_64 https://access.redhat.com/security/cve/CVE-2022-47629 RHSA-2023:0842 https://access.redhat.com/errata/RHSA-2023:0842 tar-2:1.30-6.el8_7.1.x86_64 https://access.redhat.com/security/cve/CVE-2022-48303

Fixes in Media Server for 10.1.0 SP 3 (10.1.0.147)

The following table lists the fixes in this release.

ID	Minimum conditions	Description
AMS-13564	Mandatory all deployments	AAMS Timer driver jiffy rollover fix
AMS-13442	All deployments	Element Manager security update to address CVE-2023-24998
AMS-13405	Virtual Appliance	Address firstboot DB setup failures due to stricter DB validation.
AMS-13406	WebRTC deployments	FNTMP crashed accessing stack memory info
AMS-13408	All deployments	ConfMP component restarts due to crash.
AMS-13385	All deployments	Fix the display issue in Element Manager task Event Logs after event removal
AMS-13377	SIP deployments	SIP hung resource terminating call with outstanding transactions
AMS-13371	CM deployments	Ringback and coverage tones sound like an buzz when using Opus codec.
AMS-13136	All deployments	Incorrect MariaDB file permissions.
AMS-13290	1+1 HA clusters deployments.	SC component restarts on HA standby node

ID	Minimum conditions	Description
AMS-13314	Appliance deployments	Unable to configure syslog
AMS-13265	All deployments	Unable to Execute an an Custom Summary Report in the Session Detail Record Browser
AMS-13251	All deployments	Fixed malformed Dual Unicast RTCP packets
AMS-12978 AMS-12983 AMS-12985	All deployments	Several overity fixes.
AMS-13202 AMS-13199 AMS-13198	All deployments	Address several configuration issues within Element Manager related to SIP routes, MRCP, and custom application.
AMS-12477	All deployments	MariaDB and related connectors upgrade.
AMS-12710	All deployments	Fixes for libpng security vulnerabilities

Fixes in System Layer for 10.1.0 SP 4 (10.0.0.13)

The following table lists the fixes in this release.

ID	Minimum conditions	Description
AMS-11715	Appliance deployments	Enable SELinux, add su wrapper, handle major upgrades
AMS-13768	Appliance deployments	Add Java and dependent RPMs
	Appliance deployments	RHSA-2023:3018 https://access.redhat.com/errata/RHSA-2023:3018 libarchive-3.3.3-5.el8.x86_64 https://access.redhat.com/security/cve/CVE-2022-36227 RHSA-2023:2951 https://access.redhat.com/errata/RHSA-2023:2951 kernel-4.18.0-477.10.1.el8_8.x86_64 kernel-core-4.18.0-477.10.1.el8_8.x86_64 kernel-modules-4.18.0-477.10.1.el8_8.x86_64 python3-perf-4.18.0-477.10.1.el8_8.x86_64 https://access.redhat.com/security/cve/CVE-2021-26341 https://access.redhat.com/security/cve/CVE-2021-33655 https://access.redhat.com/security/cve/CVE-2021-33656 https://access.redhat.com/security/cve/CVE-2022-1462 https://access.redhat.com/security/cve/CVE-2022-1679

ID	Minimum conditions	Description
		https://access.redhat.com/security/cve/CVE-2022-1789 https://access.redhat.com/security/cve/CVE-2022-20141 https://access.redhat.com/security/cve/CVE-2022-2196 https://access.redhat.com/security/cve/CVE-2022-25265 https://access.redhat.com/security/cve/CVE-2022-2663 https://access.redhat.com/security/cve/CVE-2022-3028 https://access.redhat.com/security/cve/CVE-2022-30594 https://access.redhat.com/security/cve/CVE-2022-3239 https://access.redhat.com/security/cve/CVE-2022-3522 https://access.redhat.com/security/cve/CVE-2022-3524 https://access.redhat.com/security/cve/CVE-2022-3564 https://access.redhat.com/security/cve/CVE-2022-3566 https://access.redhat.com/security/cve/CVE-2022-3567 https://access.redhat.com/security/cve/CVE-2022-3619 https://access.redhat.com/security/cve/CVE-2022-3623 https://access.redhat.com/security/cve/CVE-2022-3625 https://access.redhat.com/security/cve/CVE-2022-3628 https://access.redhat.com/security/cve/CVE-2022-3707 https://access.redhat.com/security/cve/CVE-2022-39188 https://access.redhat.com/security/cve/CVE-2022-39189 https://access.redhat.com/security/cve/CVE-2022-41218 https://access.redhat.com/security/cve/CVE-2022-4129 https://access.redhat.com/security/cve/CVE-2022-41674 https://access.redhat.com/security/cve/CVE-2022-42703 https://access.redhat.com/security/cve/CVE-2022-42720 https://access.redhat.com/security/cve/CVE-2022-42721 https://access.redhat.com/security/cve/CVE-2022-42722 https://access.redhat.com/security/cve/CVE-2022-43750 https://access.redhat.com/security/cve/CVE-2022-47929 https://access.redhat.com/security/cve/CVE-2023-0394 https://access.redhat.com/security/cve/CVE-2023-0461 https://access.redhat.com/security/cve/CVE-2023-1195 https://access.redhat.com/security/cve/CVE-2023-1582 https://access.redhat.com/security/cve/CVE-2023-22998 https://access.redhat.com/security/cve/CVE-2023-23454 RHSA-2023:2963 https://access.redhat.com/errata/RHSA-2023:2963 curl-7.61.1-30.el8.x86_64 libcurl-7.61.1-30.el8.i686

ID	Minimum conditions	Description
		libcurl-7.61.1-30.el8.x86_64 https://access.redhat.com/security/cve/CVE-2022-35252 https://access.redhat.com/security/cve/CVE-2022-43552 RHSA-2023:2969 https://access.redhat.com/errata/RHSA-2023:2969 net-snmp-1:5.8-27.el8.x86_64 net-snmp-agent-libs-1:5.8-27.el8.x86_64 net-snmp-libs-1:5.8-27.el8.x86_64 https://access.redhat.com/security/cve/CVE-2022-44792 https://access.redhat.com/security/cve/CVE-2022-44793 RHSA-2023:3591 https://access.redhat.com/errata/RHSA-2023:3591 platform-python-3.6.8-51.el8_8.1.x86_64 python3-libs-3.6.8-51.el8_8.1.x86_64 https://access.redhat.com/security/cve/CVE-2023-24329 RHSA-2023:3584 https://access.redhat.com/errata/RHSA-2023:3584 c-ares-1.13.0-6.el8_8.2.x86_64 https://access.redhat.com/security/cve/CVE-2023-32067 RHSA-2023:3780 https://access.redhat.com/errata/RHSA-2023:3780 python2-2.7.18-13.module+el8.8.0+19042+06909d2c.1.x86_64 python2-libs-2.7.18-13.module+el8.8.0+19042+06909d2c.1.x86_64 https://access.redhat.com/security/cve/CVE-2023-24329 RHSA-2023:2800 https://access.redhat.com/errata/RHSA-2023:2800 sysstat-11.7.3-9.el8.x86_64 https://access.redhat.com/security/cve/CVE-2022-39377 RHSA-2023:3949 https://access.redhat.com/errata/RHSA-2023:3949 open-vm-tools-12.1.5-2.el8_8.x86_64 https://access.redhat.com/security/cve/CVE-2023-20867 RHSA-2023:2860 https://access.redhat.com/errata/RHSA-2023:2860 python2-2.7.18-12.module+el8.8.0+17629+2cfc9d03.x86_64 python2-libs-2.7.18-12.module+el8.8.0+17629+2cfc9d03.x86_64 https://access.redhat.com/security/cve/CVE-2022-45061 RHSA-2023:3840 https://access.redhat.com/errata/RHSA-2023:3840

ID	Minimum conditions	Description
		sqlite-3.26.0-18.el8_8.x86_64 sqlite-libs-3.26.0-18.el8_8.x86_64 https://access.redhat.com/security/cve/CVE-2020-24736 RHSA-2023:3847 https://access.redhat.com/errata/RHSA-2023:3847 kernel-4.18.0-477.15.1.el8_8.x86_64 kernel-core-4.18.0-477.15.1.el8_8.x86_64 kernel-modules-4.18.0-477.15.1.el8_8.x86_64 python3-perf-4.18.0-477.15.1.el8_8.x86_64 https://access.redhat.com/security/cve/CVE-2023-28466 RHSA-2023:2771 https://access.redhat.com/errata/RHSA-2023:2771 python3-unbound-1.16.2-5.el8.x86_64 unbound-libs-1.16.2-5.el8.x86_64 https://access.redhat.com/security/cve/CVE-2022-3204 RHSA-2023:3106 https://access.redhat.com/errata/RHSA-2023:3106 curl-7.61.1-30.el8_8.2.x86_64 libcurl-7.61.1-30.el8_8.2.i686 libcurl-7.61.1-30.el8_8.2.x86_64 https://access.redhat.com/security/cve/CVE-2023-27535 RHSA-2023:2948 https://access.redhat.com/errata/RHSA-2023:2948 kpartx-0.8.4-37.el8.x86_64 https://access.redhat.com/security/cve/CVE-2022-41973 RHSA-2023:3349 https://access.redhat.com/errata/RHSA-2023:3349 kernel-4.18.0-477.13.1.el8_8.x86_64 kernel-core-4.18.0-477.13.1.el8_8.x86_64 kernel-modules-4.18.0-477.13.1.el8_8.x86_64 python3-perf-4.18.0-477.13.1.el8_8.x86_64 https://access.redhat.com/security/cve/CVE-2023-32233 RHSA-2023:3839 https://access.redhat.com/errata/RHSA-2023:3839 libssh-0.9.6-10.el8_8.i686 libssh-0.9.6-10.el8_8.x86_64 libssh-config-0.9.6-10.el8_8.noarch https://access.redhat.com/security/cve/CVE-2023-1667 https://access.redhat.com/security/cve/CVE-2023-2283

ID	Minimum conditions	Description
		RHSA-2023:3837 https://access.redhat.com/errata/RHSA-2023:3837 systemd-239-74.el8_8.2.x86_64 systemd-libs-239-74.el8_8.2.x86_64 systemd-pam-239-74.el8_8.2.x86_64 systemd-udev-239-74.el8_8.2.x86_64 https://access.redhat.com/security/cve/CVE-2023-26604 RHSA-2023:3002 https://access.redhat.com/errata/RHSA-2023:3002 bind-32:9.11.36-8.el8.x86_64 bind-libs-32:9.11.36-8.el8.x86_64 bind-libs-lite-32:9.11.36-8.el8.x86_64 bind-license-32:9.11.36-8.el8.noarch bind-utils-32:9.11.36-8.el8.x86_64 python3-bind-32:9.11.36-8.el8.noarch https://access.redhat.com/security/cve/CVE-2022-2795

Fixes in Media Server for 10.1.0 SP 4 (10.1.0.154)

The following table lists the fixes in this release.

ID	Minimum conditions	Description
AMS-13728	All deployments	Fix file upload after search in EM Media Management Provisioning
AMS-13609	All deployments	Update WebUA to return HSTS header.
AMS-13709	1+1 HA or N+1 clusters	Fixed Cstore sync issue
AMS-11457	All deployments	Use RedHat built OpenJDK JRE for AAMS Element Manager
AMS-13642	All deployments	Update EM to check result of backup task execution.

Fixes in System Layer for 10.1.0 September 2023 SSP (10.0.0.14)

The following table lists the fixes in this release.

ID	Minimum conditions	Description
AMS-14162	All appliance deployments	Update to address outstanding security advisories

ID	Minimum conditions	Description
		RHSA-2023:4419 https://access.redhat.com/errata/RHSA-2023:4419 openssh-8.0p1-19.el8_8.x86_64 openssh-clients-8.0p1-19.el8_8.x86_64 openssh-server-8.0p1-19.el8_8.x86_64 https://access.redhat.com/security/cve/CVE-2023-38408 RHSA-2023:4176 https://access.redhat.com/errata/RHSA-2023:4176 java-1.8.0-openjdk-1:1.8.0.382.b05-2.el8.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.382.b05-2.el8.x86_64 https://access.redhat.com/security/cve/CVE-2023-22045 https://access.redhat.com/security/cve/CVE-2023-22049 RHSA-2023:4498 https://access.redhat.com/errata/RHSA-2023:4498 dbus-1:1.12.8-24.el8_8.1.x86_64 dbus-common-1:1.12.8-24.el8_8.1.noarch dbus-daemon-1:1.12.8-24.el8_8.1.x86_64 dbus-libs-1:1.12.8-24.el8_8.1.x86_64 dbus-tools-1:1.12.8-24.el8_8.1.x86_64 https://access.redhat.com/security/cve/CVE-2023-34969 RHSA-2023:4529 https://access.redhat.com/errata/RHSA-2023:4529 libxml2-2.9.7-16.el8_8.1.x86_64 python3-libxml2-2.9.7-16.el8_8.1.x86_64 https://access.redhat.com/security/cve/CVE-2023-28484 https://access.redhat.com/security/cve/CVE-2023-29469 RHSA-2023:4102 https://access.redhat.com/errata/RHSA-2023:4102 bind-32:9.11.36-8.el8_8.1.x86_64 bind-libs-32:9.11.36-8.el8_8.1.x86_64 bind-libs-lite-32:9.11.36-8.el8_8.1.x86_64 bind-license-32:9.11.36-8.el8_8.1.noarch bind-utils-32:9.11.36-8.el8_8.1.x86_64 python3-bind-32:9.11.36-8.el8_8.1.noarch https://access.redhat.com/security/cve/CVE-2023-2828 RHSA-2023:4520 https://access.redhat.com/errata/RHSA-2023:4520 python3-requests-2.20.0-3.el8_8.noarch https://access.redhat.com/security/cve/CVE-2023-32681

ID	Minimum conditions	Description
		RHSA-2023:4523 https://access.redhat.com/errata/RHSA-2023:4523 curl-7.61.1-30.el8_8.3.x86_64 libcurl-7.61.1-30.el8_8.3.i686 libcurl-7.61.1-30.el8_8.3.x86_64 https://access.redhat.com/security/cve/CVE-2023-27536 https://access.redhat.com/security/cve/CVE-2023-28321 RHSA-2023:4524 https://access.redhat.com/errata/RHSA-2023:4524 libcap-2.48-5.el8_8.x86_64 https://access.redhat.com/security/cve/CVE-2023-2602 https://access.redhat.com/security/cve/CVE-2023-2603 RHSA-2023:4517 https://access.redhat.com/errata/RHSA-2023:4517 kernel-4.18.0-477.21.1.el8_8.x86_64 kernel-core-4.18.0-477.21.1.el8_8.x86_64 kernel-modules-4.18.0-477.21.1.el8_8.x86_64 python3-perf-4.18.0-477.21.1.el8_8.x86_64 https://access.redhat.com/security/cve/CVE-2022-42896 https://access.redhat.com/security/cve/CVE-2023-1281 https://access.redhat.com/security/cve/CVE-2023-1829 https://access.redhat.com/security/cve/CVE-2023-2194 https://access.redhat.com/security/cve/CVE-2023-2235

Fixes in System Layer for 10.1.0 SP 5 (10.0.0.15)

The following table lists the fixes in this release.

ID	Minimum conditions	Description
AMS-14612	Appliance deployment	Update to address outstanding security advisories RHSA-2023:5245 https://access.redhat.com/errata/RHSA-2023:5245 linux-firmware-20230404-117.git2e92a49f.el8_8.noarch https://access.redhat.com/security/cve/CVE-2023-20593 RHSA-2023:5244 https://access.redhat.com/errata/RHSA-2023:5244 kernel-4.18.0-477.27.1.el8_8.x86_64 kernel-core-4.18.0-477.27.1.el8_8.x86_64 kernel-modules-4.18.0-477.27.1.el8_8.x86_64 python3-perf-4.18.0-477.27.1.el8_8.x86_64

ID	Minimum conditions	Description
		https://access.redhat.com/security/cve/CVE-2023-1637 https://access.redhat.com/security/cve/CVE-2023-2002 https://access.redhat.com/security/cve/CVE-2023-20593 https://access.redhat.com/security/cve/CVE-2023-3090 https://access.redhat.com/security/cve/CVE-2023-3390 https://access.redhat.com/security/cve/CVE-2023-35001 https://access.redhat.com/security/cve/CVE-2023-35788 https://access.redhat.com/security/cve/CVE-2023-3776 https://access.redhat.com/security/cve/CVE-2023-4004 RHSA-2023:5997 https://access.redhat.com/errata/RHSA-2023:5997 platform-python-3.6.8-51.el8_8.2.x86_64 python3-libs-3.6.8-51.el8_8.2.x86_64 https://access.redhat.com/security/cve/CVE-2023-40217 RHSA-2023:5994 https://access.redhat.com/errata/RHSA-2023:5994 python2-2.7.18-13.module+el8.8.0+20144+beed974d.2.x86_64 python2-libs-2.7.18-13.module+el8.8.0+20144+beed974d.2.x86_64 https://access.redhat.com/security/cve/CVE-2023-40217 RHSA-2023:5249 https://access.redhat.com/errata/RHSA-2023:5249 ncurses-6.1-9.20180224.el8_8.1.x86_64 ncurses-base-6.1-9.20180224.el8_8.1.noarch ncurses-libs-6.1-9.20180224.el8_8.1.i686 ncurses-libs-6.1-9.20180224.el8_8.1.x86_64 https://access.redhat.com/security/cve/CVE-2023-29491 RHSA-2023:5252 https://access.redhat.com/errata/RHSA-2023:5252 dmidecode-1:3.3-4.el8_8.1.x86_64 https://access.redhat.com/security/cve/CVE-2023-30630 RHSA-2023:4706 https://access.redhat.com/errata/RHSA-2023:4706 python3-syspurpose-1.28.36-3.el8_8.x86_64 https://access.redhat.com/security/cve/CVE-2023-3899 RHSA-2023:4864 https://access.redhat.com/errata/RHSA-2023:4864 cups-libs-1:2.2.6-51.el8_8.1.x86_64 https://access.redhat.com/security/cve/CVE-2023-32360

ID	Minimum conditions	Description
		RHSA-2023:5353 https://access.redhat.com/errata/RHSA-2023:5353 libtiff-4.0.9-29.el8_8.x86_64 https://access.redhat.com/security/cve/CVE-2023-0800 https://access.redhat.com/security/cve/CVE-2023-0801 https://access.redhat.com/security/cve/CVE-2023-0802 https://access.redhat.com/security/cve/CVE-2023-0803 https://access.redhat.com/security/cve/CVE-2023-0804 RHSA-2023:5731 https://access.redhat.com/errata/RHSA-2023:5731 java-1.8.0-openjdk-1:1.8.0.392.b08-4.el8.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.392.b08-4.el8.x86_64 https://access.redhat.com/security/cve/CVE-2022-40433 https://access.redhat.com/security/cve/CVE-2023-22067 https://access.redhat.com/security/cve/CVE-2023-22081 RHSA-2023:5455 https://access.redhat.com/errata/RHSA-2023:5455 glibc-2.28-225.el8_8.6.i686 glibc-2.28-225.el8_8.6.x86_64 glibc-common-2.28-225.el8_8.6.x86_64 glibc-gconv-extra-2.28-225.el8_8.6.i686 glibc-gconv-extra-2.28-225.el8_8.6.x86_64 glibc-langpack-en-2.28-225.el8_8.6.x86_64 glibc-locale-source-2.28-225.el8_8.6.x86_64 glibc-minimal-langpack-2.28-225.el8_8.6.x86_64 libnsl-2.28-225.el8_8.6.i686 libnsl-2.28-225.el8_8.6.x86_64 https://access.redhat.com/security/cve/CVE-2023-4527 https://access.redhat.com/security/cve/CVE-2023-4806 https://access.redhat.com/security/cve/CVE-2023-4813 https://access.redhat.com/security/cve/CVE-2023-4911 RHSA-2023:5837 https://access.redhat.com/errata/RHSA-2023:5837 libnghttp2-1.33.0-5.el8_8.i686 libnghttp2-1.33.0-5.el8_8.x86_64 https://access.redhat.com/security/cve/CVE-2023-44487 RHSA-2023:6236 https://access.redhat.com/errata/RHSA-2023:6236 binutils-2.30-119.el8_8.2.x86_64 https://access.redhat.com/security/cve/CVE-2022-4285

ID	Minimum conditions	Description
		RHSA-2023:5312 https://access.redhat.com/errata/RHSA-2023:5312 open-vm-tools-12.1.5-2.el8_8.3.x86_64 https://access.redhat.com/security/cve/CVE-2023-20900 RHSA-2023:5474 https://access.redhat.com/errata/RHSA-2023:5474 bind-32:9.11.36-8.el8_8.2.x86_64 bind-libs-32:9.11.36-8.el8_8.2.x86_64 bind-libs-lite-32:9.11.36-8.el8_8.2.x86_64 bind-license-32:9.11.36-8.el8_8.2.noarch bind-utils-32:9.11.36-8.el8_8.2.x86_64 python3-bind-32:9.11.36-8.el8_8.2.noarch https://access.redhat.com/security/cve/CVE-2023-3341 FEDORA-EPEL-2023-50480e7e18 - https://bodhi.fedoraproject.org/updates/FEDORA-EPEL-2023-50480e7e18 clamav-0.103.10-1.el8.x86_64.rpm clamav-data-0.103.10-1.el8.noarch.rpm clamav-filesystem-0.103.10-1.el8.noarch.rpm clamav-lib-0.103.10-1.el8.x86_64.rpm clamav-update-0.103.10-1.el8.x86_64.rpm

Fixes in Media Server for 10.1.0 SP 5 (10.1.0.176)

The following table lists the fixes in this release.

ID	Minimum conditions	Description
AMS-14377	All deployments	Protect AMS services from CPU accounting impacts
AMS-14453	All deployments	Apache CXF Security Update
AMS-14629	All deployments	Fixed SNMP crash
AMS-14484	All deployments	Woodstox Security Update
AMS-14587	All deployments	Removed the file update from Element Manager Linux init script

ID	Minimum conditions	Description
AMS-14600	All deployments	RFC 2833 digit duplication on IVR underflow.
AMS-14559	All deployments	Re-cache playlist segments if client catches up to last segment
AMS-14511	All deployments	Apache Tomcat Security update
AMS-14533	Streaming media using HLS	Reduce HLS client playlist query rate
AMS-14215	All deployments	Store selected payload types for template offer
AMS-14206	All deployments	ConfMP crash on inactive session
AMS-13730	All deployments	Enable secure communications by default
AMS-14175	All deployments	Crypto tag negotiaton update
AMS-14137	All deployments	Tomcat security updates
AMS-14088	Appliance deployments	Reduce minimum memory requirement to account for UEFI installs
AMS-14040	All deployments	MPQOSSocket data corruption from an InterlockedExchange()

Fixes in System Layer 10.0.0.16

The following table lists the fixes in this release.

ID	Minimum conditions	Description
AMS-14751	Appliance	Remove unbound RPMs to prevent unneeded public DNS queries
AMS-15042	Appliance	Update to RHEL 8.8
AMS-14809	Appliance	Update RPMs to address security advisories RHSA-2023:7010 https://access.redhat.com/errata/RHSA-2023:7010 sysstat-11.7.3-11.el8.x86_64 https://access.redhat.com/security/cve/CVE-2023-33204 RHSA-2024:0119 https://access.redhat.com/errata/RHSA-2024:0119

ID	Minimum conditions	Description
		libxml2-2.9.7-18.el8_9.x86_64 python3-libxml2-2.9.7-18.el8_9.x86_64 https://access.redhat.com/security/cve/CVE-2023-39615 RHSA-2023:7265 https://access.redhat.com/errata/RHSA-2023:7265 open-vm-tools-12.2.5-3.el8_9.1.x86_64 https://access.redhat.com/security/cve/CVE-2023-34058 https://access.redhat.com/security/cve/CVE-2023-34059 RHSA-2024:0627 https://access.redhat.com/errata/RHSA-2024:0627 gnutls-3.6.16-8.el8_9.1.x86_64 https://access.redhat.com/security/cve/CVE-2024-0553 RHSA-2023:7015 https://access.redhat.com/errata/RHSA-2023:7015 wireshark-cli-1:2.6.2-17.el8.x86_64 https://access.redhat.com/security/cve/CVE-2023-0666 https://access.redhat.com/security/cve/CVE-2023-2856 https://access.redhat.com/security/cve/CVE-2023-2858 https://access.redhat.com/security/cve/CVE-2023-2952 RHSA-2024:0113 https://access.redhat.com/errata/RHSA-2024:0113 kernel-4.18.0-513.11.1.el8_9.x86_64 kernel-core-4.18.0-513.11.1.el8_9.x86_64 kernel-modules-4.18.0-513.11.1.el8_9.x86_64 python3-perf-4.18.0-513.11.1.el8_9.x86_64 https://access.redhat.com/security/cve/CVE-2022-36402 https://access.redhat.com/security/cve/CVE-2023-20569 https://access.redhat.com/security/cve/CVE-2023-2162 https://access.redhat.com/security/cve/CVE-2023-42753 https://access.redhat.com/security/cve/CVE-2023-4622 https://access.redhat.com/security/cve/CVE-2023-5633 RHSA-2024:0628 https://access.redhat.com/errata/RHSA-2024:0628 libssh-0.9.6-13.el8_9.i686 libssh-0.9.6-13.el8_9.x86_64 libssh-config-0.9.6-13.el8_9.noarch https://access.redhat.com/security/cve/CVE-2023-48795 RHSA-2023:7177 https://access.redhat.com/errata/RHSA-2023:7177

ID	Minimum conditions	Description
		bind-32:9.11.36-11.el8_9.x86_64 bind-libs-32:9.11.36-11.el8_9.x86_64 bind-libs-lite-32:9.11.36-11.el8_9.x86_64 bind-license-32:9.11.36-11.el8_9.noarch bind-utils-32:9.11.36-11.el8_9.x86_64 python3-bind-32:9.11.36-11.el8_9.noarch https://access.redhat.com/security/cve/CVE-2022-3094 RHSA-2023:7176 https://access.redhat.com/errata/RHSA-2023:7176 platform-python-pip-9.0.3-23.el8.noarch python3-pip-9.0.3-23.el8.noarch python3-pip-wheel-9.0.3-23.el8.noarch https://access.redhat.com/security/cve/CVE-2007-4559 RHSA-2024:0114 https://access.redhat.com/errata/RHSA-2024:0114 platform-python-3.6.8-56.el8_9.2.x86_64 python3-libs-3.6.8-56.el8_9.2.x86_64 https://access.redhat.com/security/cve/CVE-2022-48560 https://access.redhat.com/security/cve/CVE-2022-48564 RHSA-2024:0116 https://access.redhat.com/errata/RHSA-2024:0116 python3-urllib3-1.24.2-5.el8_9.2.noarch https://access.redhat.com/security/cve/CVE-2023-43804 https://access.redhat.com/security/cve/CVE-2023-45803 RHSA-2023:7174 https://access.redhat.com/errata/RHSA-2023:7174 perl-HTTP-Tiny-0.074-2.el8.noarch https://access.redhat.com/security/cve/CVE-2023-31486 RHSA-2024:0647 https://access.redhat.com/errata/RHSA-2024:0647 python3-rpm-4.14.3-28.el8_9.x86_64 rpm-4.14.3-28.el8_9.x86_64 rpm-build-libs-4.14.3-28.el8_9.x86_64 rpm-libs-4.14.3-28.el8_9.x86_64 rpm-plugin-selinux-4.14.3-28.el8_9.x86_64 rpm-plugin-systemd-inhibit-4.14.3-28.el8_9.x86_64 https://access.redhat.com/security/cve/CVE-2021-35937 https://access.redhat.com/security/cve/CVE-2021-35938 https://access.redhat.com/security/cve/CVE-2021-35939

ID	Minimum conditions	Description
		RHSA-2024:0105 https://access.redhat.com/errata/RHSA-2024:0105 nss-3.90.0-4.el8_9.x86_64 nss-softokn-3.90.0-4.el8_9.x86_64 nss-softokn-freebl-3.90.0-4.el8_9.x86_64 nss-sysinit-3.90.0-4.el8_9.x86_64 nss-util-3.90.0-4.el8_9.x86_64 https://access.redhat.com/security/cve/CVE-2023-5388 RHSA-2023:7549 https://access.redhat.com/errata/RHSA-2023:7549 kernel-4.18.0-513.9.1.el8_9.x86_64 kernel-core-4.18.0-513.9.1.el8_9.x86_64 kernel-modules-4.18.0-513.9.1.el8_9.x86_64 python3-perf-4.18.0-513.9.1.el8_9.x86_64 https://access.redhat.com/security/cve/CVE-2022-45884 https://access.redhat.com/security/cve/CVE-2022-45886 https://access.redhat.com/security/cve/CVE-2022-45919 https://access.redhat.com/security/cve/CVE-2023-1192 https://access.redhat.com/security/cve/CVE-2023-2163 https://access.redhat.com/security/cve/CVE-2023-3812 https://access.redhat.com/security/cve/CVE-2023-5178 RHSA-2023:7077 https://access.redhat.com/errata/RHSA-2023:7077 kernel-4.18.0-513.5.1.el8_9.x86_64 kernel-core-4.18.0-513.5.1.el8_9.x86_64 kernel-modules-4.18.0-513.5.1.el8_9.x86_64 python3-perf-4.18.0-513.5.1.el8_9.x86_64 https://access.redhat.com/security/cve/CVE-2021-43975 https://access.redhat.com/security/cve/CVE-2022-28388 https://access.redhat.com/security/cve/CVE-2022-3594 https://access.redhat.com/security/cve/CVE-2022-3640 https://access.redhat.com/security/cve/CVE-2022-38457 https://access.redhat.com/security/cve/CVE-2022-40133 https://access.redhat.com/security/cve/CVE-2022-40982 https://access.redhat.com/security/cve/CVE-2022-42895 https://access.redhat.com/security/cve/CVE-2022-45869 https://access.redhat.com/security/cve/CVE-2022-45887 https://access.redhat.com/security/cve/CVE-2022-4744 https://access.redhat.com/security/cve/CVE-2023-0458

ID	Minimum conditions	Description
		https://access.redhat.com/security/cve/CVE-2023-0590 https://access.redhat.com/security/cve/CVE-2023-0597 https://access.redhat.com/security/cve/CVE-2023-1073 https://access.redhat.com/security/cve/CVE-2023-1074 https://access.redhat.com/security/cve/CVE-2023-1075 https://access.redhat.com/security/cve/CVE-2023-1079 https://access.redhat.com/security/cve/CVE-2023-1118 https://access.redhat.com/security/cve/CVE-2023-1206 https://access.redhat.com/security/cve/CVE-2023-1252 https://access.redhat.com/security/cve/CVE-2023-1382 https://access.redhat.com/security/cve/CVE-2023-1855 https://access.redhat.com/security/cve/CVE-2023-1989 https://access.redhat.com/security/cve/CVE-2023-1998 https://access.redhat.com/security/cve/CVE-2023-2269 https://access.redhat.com/security/cve/CVE-2023-23455 https://access.redhat.com/security/cve/CVE-2023-2513 https://access.redhat.com/security/cve/CVE-2023-26545 https://access.redhat.com/security/cve/CVE-2023-28328 https://access.redhat.com/security/cve/CVE-2023-28772 https://access.redhat.com/security/cve/CVE-2023-30456 https://access.redhat.com/security/cve/CVE-2023-31084 https://access.redhat.com/security/cve/CVE-2023-3141 https://access.redhat.com/security/cve/CVE-2023-31436 https://access.redhat.com/security/cve/CVE-2023-3161 https://access.redhat.com/security/cve/CVE-2023-3212 https://access.redhat.com/security/cve/CVE-2023-3268 https://access.redhat.com/security/cve/CVE-2023-33203 https://access.redhat.com/security/cve/CVE-2023-33951 https://access.redhat.com/security/cve/CVE-2023-33952 https://access.redhat.com/security/cve/CVE-2023-35823 https://access.redhat.com/security/cve/CVE-2023-35824 https://access.redhat.com/security/cve/CVE-2023-35825 https://access.redhat.com/security/cve/CVE-2023-3609 https://access.redhat.com/security/cve/CVE-2023-3611 https://access.redhat.com/security/cve/CVE-2023-3772 https://access.redhat.com/security/cve/CVE-2023-4128 https://access.redhat.com/security/cve/CVE-2023-4132 https://access.redhat.com/security/cve/CVE-2023-4155 https://access.redhat.com/security/cve/CVE-2023-4206

ID	Minimum conditions	Description
		https://access.redhat.com/security/cve/CVE-2023-4207 https://access.redhat.com/security/cve/CVE-2023-4208 https://access.redhat.com/security/cve/CVE-2023-4732 https://access.redhat.com/security/cve/CVE-2024-0443 RHSA-2023:6976 https://access.redhat.com/errata/RHSA-2023:6976 libfastjson-0.99.9-2.el8.x86_64 https://access.redhat.com/security/cve/CVE-2020-12762 RHSA-2023:7116 https://access.redhat.com/errata/RHSA-2023:7116 c-ares-1.13.0-8.el8.x86_64 https://access.redhat.com/security/cve/CVE-2022-4904 RHSA-2023:7165 https://access.redhat.com/errata/RHSA-2023:7165 cups-libs-1:2.2.6-54.el8_9.x86_64 https://access.redhat.com/security/cve/CVE-2023-32324 https://access.redhat.com/security/cve/CVE-2023-34241 RHSA-2023:7166 https://access.redhat.com/errata/RHSA-2023:7166 tpm2-tss-2.3.2-5.el8.x86_64 https://access.redhat.com/security/cve/CVE-2023-22745 RHSA-2023:7112 https://access.redhat.com/errata/RHSA-2023:7112 shadow-utils-2:4.6-19.el8.x86_64 https://access.redhat.com/security/cve/CVE-2023-4641 RHSA-2024:0131 https://access.redhat.com/errata/RHSA-2024:0131 pixman-0.38.4-3.el8_9.x86_64 https://access.redhat.com/security/cve/CVE-2022-44638 RHSA-2023:7109 https://access.redhat.com/errata/RHSA-2023:7109 linux-firmware-20230824-119.git0e048b06.el8_9.noarch https://access.redhat.com/security/cve/CVE-2023-20569 RHSA-2023:7190 https://access.redhat.com/errata/RHSA-2023:7190 avahi-libs-0.7-21.el8.x86_64 https://access.redhat.com/security/cve/CVE-2023-1981 RHSA-2023:7207 https://access.redhat.com/errata/RHSA-2023:7207

ID	Minimum conditions	Description
		c-ares-1.13.0-9.el8_9.1.x86_64 https://access.redhat.com/security/cve/CVE-2020-22217 https://access.redhat.com/security/cve/CVE-2023-31130 RHSA-2024:0256 https://access.redhat.com/errata/RHSA-2024:0256 platform-python-3.6.8-56.el8_9.3.x86_64 python3-libs-3.6.8-56.el8_9.3.x86_64 https://access.redhat.com/security/cve/CVE-2023-27043 RHSA-2024:0253 https://access.redhat.com/errata/RHSA-2024:0253 sqlite-3.26.0-19.el8_9.x86_64 sqlite-libs-3.26.0-19.el8_9.x86_64 https://access.redhat.com/security/cve/CVE-2023-7104 RHSA-2023:7877 https://access.redhat.com/errata/RHSA-2023:7877 openssl-1:1.1.1k-12.el8_9.x86_64 openssl-libs-1:1.1.1k-12.el8_9.i686 openssl-libs-1:1.1.1k-12.el8_9.x86_64 https://access.redhat.com/security/cve/CVE-2023-3446 https://access.redhat.com/security/cve/CVE-2023-3817 https://access.redhat.com/security/cve/CVE-2023-5678 RHSA-2024:0155 https://access.redhat.com/errata/RHSA-2024:0155 gnutls-3.6.16-8.el8_9.x86_64 https://access.redhat.com/security/cve/CVE-2023-5981 RHSA-2024:0811 https://access.redhat.com/errata/RHSA-2024:0811 sudo-1.9.5p2-1.el8_9.x86_64 https://access.redhat.com/security/cve/CVE-2023-28486 https://access.redhat.com/security/cve/CVE-2023-28487 https://access.redhat.com/security/cve/CVE-2023-42465 RHSA-2023:7187 https://access.redhat.com/errata/RHSA-2023:7187 procps-ng-3.3.15-14.el8.x86_64 https://access.redhat.com/security/cve/CVE-2023-4016 RHSA-2023:7189 https://access.redhat.com/errata/RHSA-2023:7189 fwupd-1.7.8-2.el8.x86_64 https://access.redhat.com/security/cve/CVE-2022-3287

ID	Minimum conditions	Description
		RHSA-2024:0265 https://access.redhat.com/errata/RHSA-2024:0265 java-1.8.0-openjdk-1:1.8.0.402.b06-2.el8.x86_64 java-1.8.0-openjdk-headless-1:1.8.0.402.b06-2.el8.x86_64 https://access.redhat.com/security/cve/CVE-2024-20918 https://access.redhat.com/security/cve/CVE-2024-20919 https://access.redhat.com/security/cve/CVE-2024-20921 https://access.redhat.com/security/cve/CVE-2024-20926 https://access.redhat.com/security/cve/CVE-2024-20945 https://access.redhat.com/security/cve/CVE-2024-20952 RHSA-2023:7151 https://access.redhat.com/errata/RHSA-2023:7151 platform-python-3.6.8-56.el8_9.x86_64 python3-libs-3.6.8-56.el8_9.x86_64 https://access.redhat.com/security/cve/CVE-2007-4559 RHSA-2023:7029 https://access.redhat.com/errata/RHSA-2023:7029 libX11-1.6.8-6.el8.x86_64 libX11-common-1.6.8-6.el8.noarch https://access.redhat.com/security/cve/CVE-2023-3138 RHSA-2023:6944 https://access.redhat.com/errata/RHSA-2023:6944 protobuf-c-1.3.0-8.el8.x86_64 https://access.redhat.com/security/cve/CVE-2022-48468 RHSA-2024:0786 https://access.redhat.com/errata/RHSA-2024:0786 nss-3.90.0-6.el8_9.x86_64 nss-softokn-3.90.0-6.el8_9.x86_64 nss-softokn-freebl-3.90.0-6.el8_9.x86_64 nss-sysinit-3.90.0-6.el8_9.x86_64 nss-util-3.90.0-6.el8_9.x86_64 https://access.redhat.com/security/cve/CVE-2023-6135 RHSA-2024:0606 https://access.redhat.com/errata/RHSA-2024:0606 openssh-8.0p1-19.el8_9.2.x86_64 openssh-clients-8.0p1-19.el8_9.2.x86_64 openssh-server-8.0p1-19.el8_9.2.x86_64 https://access.redhat.com/security/cve/CVE-2023-48795 https://access.redhat.com/security/cve/CVE-2023-51385

ID	Minimum conditions	Description
		RHSA-2023:7836 https://access.redhat.com/errata/RHSA-2023:7836 avahi-libs-0.7-21.el8_9.1.x86_64 https://access.redhat.com/security/cve/CVE-2021-3468 https://access.redhat.com/security/cve/CVE-2023-38469 https://access.redhat.com/security/cve/CVE-2023-38470 https://access.redhat.com/security/cve/CVE-2023-38471 https://access.redhat.com/security/cve/CVE-2023-38472 https://access.redhat.com/security/cve/CVE-2023-38473 RHSA-2024:0768 https://access.redhat.com/errata/RHSA-2024:0768 libmaxminddb-1.2.0-10.el8_9.1.x86_64 https://access.redhat.com/security/cve/CVE-2020-28241

Fixes in System Layer for 10.1.0 SP 6 (10.0.0.17)

The following table lists the fixes in this release.

ID	Minimum conditions	Description
AMS-15113	Appliance	Move upload directory to app partition
	Appliance	RHSA-2024:0897 https://access.redhat.com/errata/RHSA-2024:0897 kernel-4.18.0-513.18.1.el8_9.x86_64 kernel-core-4.18.0-513.18.1.el8_9.x86_64 kernel-modules-4.18.0-513.18.1.el8_9.x86_64 python3-perf-4.18.0-513.18.1.el8_9.x86_64 https://access.redhat.com/security/cve/CVE-2022-3545 https://access.redhat.com/security/cve/CVE-2022-41858 https://access.redhat.com/security/cve/CVE-2023-1073 https://access.redhat.com/security/cve/CVE-2023-1838 https://access.redhat.com/security/cve/CVE-2023-2166 https://access.redhat.com/security/cve/CVE-2023-2176 https://access.redhat.com/security/cve/CVE-2023-40283 https://access.redhat.com/security/cve/CVE-2023-45871 https://access.redhat.com/security/cve/CVE-2023-4623 https://access.redhat.com/security/cve/CVE-2023-46813 https://access.redhat.com/security/cve/CVE-2023-4921 https://access.redhat.com/security/cve/CVE-2023-5717 https://access.redhat.com/security/cve/CVE-2023-6356 https://access.redhat.com/security/cve/CVE-2023-6535

ID	Minimum conditions	Description
		https://access.redhat.com/security/cve/CVE-2023-6536 https://access.redhat.com/security/cve/CVE-2023-6606 https://access.redhat.com/security/cve/CVE-2023-6610 https://access.redhat.com/security/cve/CVE-2023-6817 https://access.redhat.com/security/cve/CVE-2024-0646

Fixes in Media Server for 10.1.0 SP 6 (10.1.0.195)

The following table lists the fixes in this release.

ID	Minimum conditions	Description
AMS-15092	All deployments	Changed Avaya Inc. to Avaya LLC
AMS-14086	All deployments	Fixed the file upload issue in EM task Manage Software Update
AMS-14749	All deployments	Apache Tomcat security update
AMS-15016	All deployments	SIP stack stopped responding to incoming connection attempt
AMS-14470	All deployments	Security update for the third-party library JDOM
AMS-14834	All deployments	libvpx security update
AMS-10602	All deployments	Bouncy Castle security updates
AMS-14919	All deployments	Fix the refresh issue in EM Alarms task
AMS-14042	All deployments	Fix sorting in Media Management Provisioning content table
AMS-14811	All deployments	Xalan security update
AMS-14580	All deployments	Allow IPv6 address as Subject Alternative Name in Element Manager
AMS-14782	All deployments	Add audit log for clearing event logs via Element Manager
AMS-14432	All deployments	Hibernate security update
AMS-14692	All deployments	Use server FQDN for Linux default staging certificate common name

ID	Minimum conditions	Description
AMS-14677	All deployments	google-api security update
AMS-14649	All deployments	Spring Framework security update

Known issues and workarounds

Known issues and workarounds

The following table lists the known issues, symptoms, and workarounds in this release.

ID	Minimum conditions	Visible symptoms	Workaround
N/A			

Languages supported

List the languages supported in this release.

- *English*

Documentation errata

Document number	Title	Description
N/A		