



Product Support Notice

© 2022 Avaya Inc. All Rights Reserved.

PSN # PSN006133u

Original publication date: 18-Nov-2022. This is Issue #01, published date: 18-Nov-2022.

Severity/risk level

Medium

Urgency

When
Convenient

Name of problem Avaya Aura® Device Services Release 10.1 Security Service Pack 3.

This Security Service Pack resolves security vulnerabilities referenced in ANNEXURE A.

Products affected

Avaya Aura® Device Services Release 10.1.x

1. 10.1.0.0 GA
2. 10.1.0.1 Service Pack
3. 10.1.1.0 Feature Pack

Problem description

The system will be exposed to the security vulnerabilities referenced in ANNEXURE A.

Resolution

This Security Service Pack 3 updates the list of rpms listed in ANNEXURE A.

The resolution is to apply the Security Service Pack 3 if the AADS server is running with one of the following versions:

- 10.1.0.0 GA
- 10.1.0.1 Service Pack
- 10.1.1.0 Feature Pack

Workaround or alternative remediation

n/a

Remarks

n/a

Patch Notes

The information in this section concerns the patch, if any, recommended in the Resolution above.

Backup before applying the patch

It is recommended to take a VM snapshot before applying the patch.

Download

Follow the instructions below to download the 10.1 Security Service Pack 3:

1. Go to <http://support.avaya.com>
2. Under the “Support by Product” menu click on “Downloads.”
3. Enter the product name as “device services” and then select “Avaya Aura® Device Services.”
4. Select “10.1.x” from the Choose Release dropdown.
5. Click on “Avaya Aura® Device Services 10.1.0.0, 10.1.x”.
6. Click on the file “AV-AADS10.1-RHEL8.4-SSP-003-02.tar.bz2” to download.

Patch install instructions

Service-interrupting?

Yes

Prerequisites:

The Security Service Pack 3 can be applied to the following AADS servers:

- 10.1.0.0 GA
- 10.1.0.1 Service Pack
- 10.1.1.0 Feature Pack

Before applying Security Service Pack 3, please check the output of the command “av-version”

If “AV_SSP_VERSION” is blank, please apply the initial system layer update “ucapp-system-4.0.0.0.7.tgz” first (You can download “ucapp-system-4.0.0.0.7.tgz” from Avaya support site under

Download TITLE “Avaya Aura® Device Services 10.1.0.1 Service Pack, 10.1.x”). Then apply Security Service Pack 3.

Important Note: For FIPS deployment, it must upgrade AADS to the 10.1.0.1 Service Pack before applying Security Service Pack 3.

Steps to apply Security Service Pack 3

- 1. Download "AV-AADS10.1-RHEL8.4-SSP-003-02.tar.bz2" to the admin user’s home directory.
- 2. Stop AADS services.
 - a. `svc aads stop`
- 3. Apply Security Service Pack 3.
 - a. `av-update-os AV-AADS10.1-RHEL8.4-SSP-003-02.tar.bz2`
- 4. SSP3 installation reboots the server at the end. After reboot, verify Security Service Pack 3 version.
 - a. `av-version`

It shows the output below

```
-----  
OS_VERSION: Red Hat Enterprise Linux release 8.4 (Ootpa)  
AV_SSP_VERSION: 003  
AV_BUILD_NUMBER: 02  
-----
```

- 5. Start AADS services
 - a. `svc aads start`

Verification

- a. Run command “av-version”

On successful installation, it shows the output below:

```
-----  
OS_VERSION: Red Hat Enterprise Linux release 8.4 (Ootpa)  
AV_SSP_VERSION: 003  
AV_BUILD_NUMBER: 02  
-----
```

Failure

The command output is self-explanatory about the status of the run and refers to the verification process to check the failure.

Patch uninstall instructions

N/A

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks

Failure to keep updated to the latest tested version of the application RPMs may reduce the security of the system.

Avaya Security Vulnerability Classification

n/a

Mitigation

n/a

ANNEXURE A

This Security Service Pack 3 updates following RPMS

bind-export-libs-9.11.36-3.el8_6.1.x86_64
bind-libs-9.11.36-3.el8_6.1.x86_64
bind-libs-lite-9.11.36-3.el8_6.1.x86_64
bind-license-9.11.36-3.el8_6.1.noarch
bind-utils-9.11.36-3.el8_6.1.x86_64

python3-bind-9.11.36-3.el8_6.1.noarch
 RHSA-2022:6778 Important/Sec.
 RHSA-2022:2092 Moderate/Sec.
 RHSA-2021:4384 Moderate/Sec.
 RHSA-2021:1989 Important/Sec.
compat-openssl10-1.0.2o-4.el8_6.x86_64
 RHSA-2022:5326 Low/Sec.
curl-7.61.1-22.el8_6.4.x86_64
libcurl-7.61.1-22.el8_6.4.x86_64
 RHSA-2022:5313 Moderate/Sec.
 RHSA-2022:6159 Moderate/Sec.
expat-2.2.5-8.el8_6.3.x86_64
 RHSA-2022:5314 Moderate/Sec.
 RHSA-2022:6878 Important/Sec.
gnupg2-2.2.20-3.el8_6.x86_64
gnupg2-smime-2.2.20-3.el8_6.x86_64
 RHSA-2022:6463 Moderate/Sec.
java-1.8.0-openjdk-1.8.0.342.b07-2.el8_6.x86_64
java-1.8.0-openjdk-devel-1.8.0.342.b07-2.el8_6.x86_64
java-1.8.0-openjdk-headless-1.8.0.342.b07-2.el8_6.x86_64
 RHSA-2022:5696 Important/Sec.
kernel-4.18.0-372.26.1.el8_6.x86_64
kernel-core-4.18.0-372.26.1.el8_6.x86_64
kernel-modules-4.18.0-372.26.1.el8_6.x86_64
kernel-tools-4.18.0-372.26.1.el8_6.x86_64
kernel-tools-libs-4.18.0-372.26.1.el8_6.x86_64
python3-perf-4.18.0-372.26.1.el8_6.x86_64
 RHSA-2022:5316 Important/Sec.
 RHSA-2022:5564 Important/Sec.
 RHSA-2022:5819 Important/Sec.
 RHSA-2022:6460 Moderate/Sec.
libgcrypt-1.8.5-7.el8_6.x86_64
 RHSA-2022:5311 Moderate/Sec.
libxml2-2.9.7-13.el8_6.1.x86_64
python3-libxml2-2.9.7-13.el8_6.1.x86_64
 RHSA-2022:5317 Moderate/Sec.
open-vm-tools-11.3.5-1.el8_6.1.x86_64
 RHSA-2022:6357 Important/Sec.
openssl-1.1.1k-7.el8_6.x86_64
openssl-libs-1.1.1k-7.el8_6.x86_64
 RHSA-2022:5818 Moderate/Sec.
pcre2-10.32-3.el8_6.x86_64
 RHSA-2022:5809 Moderate/Sec.
platform-python-3.6.8-47.el8_6.x86_64
python3-libs-3.6.8-47.el8_6.x86_64
 RHSA-2022:6457 Moderate/Sec.
systemd-239-58.el8_6.4.x86_64
systemd-libs-239-58.el8_6.4.x86_64
systemd-pam-239-58.el8_6.4.x86_64
systemd-udev-239-58.el8_6.4.x86_64
 RHSA-2022:6206 Important/Sec.
vim-minimal-8.0.1763-19.el8_6.4.x86_64
 RHSA-2022:5319 Moderate/Sec.
 RHSA-2022:5813 Moderate/Sec.

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

Disclaimer: ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED “AS IS”. AVAYA INC., ON BEHALF OF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES (HEREINAFTER COLLECTIVELY REFERRED TO AS “AVAYA”), DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND FURTHERMORE, AVAYA MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE STEPS RECOMMENDED WILL ELIMINATE SECURITY OR VIRUS THREATS TO CUSTOMERS’ SYSTEMS. IN NO EVENT SHALL AVAYA BE LIABLE FOR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE INFORMATION OR RECOMMENDED ACTIONS PROVIDED HEREIN, INCLUDING DIRECT, INDIRECT, CONSEQUENTIAL DAMAGES, LOSS OF BUSINESS PROFITS, OR SPECIAL DAMAGES, EVEN IF AVAYA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE INFORMATION PROVIDED HERE DOES NOT AFFECT THE SUPPORT AGREEMENTS IN PLACE FOR AVAYA PRODUCTS. SUPPORT FOR AVAYA PRODUCTS CONTINUES TO BE EXECUTED AS PER EXISTING AGREEMENTS WITH AVAYA.

All trademarks identified by ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc.
All other trademarks are the property of their respective owners.