



Product Support Notice

© 2022 Avaya Inc. All Rights Reserved.

PSN # PSN006080u

Original publication date: 22-Jul-2022. This is Issue #02, published date: 2-Aug-2022.

Severity/risk level Medium

Urgency

When Convenient

Name of problem Avaya Aura® Device Services Release 10.1 Security Service Pack 2

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

Problem description

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

Resolution

This Security Service Pack 2 updates the list of rpms listed in ANNEXURE A

The resolution is to apply the Security Service Pack 2 if the AADS server is running with one of the following versions

- 10.1.0.0 GA
- 10.1.0.1 Service 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 2

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-002-04.tar.bz2” to download

Patch install instructions

Service-interrupting?

Yes

Prerequisites:

The Security Service Pack 2 can be applied to the following AADS servers

- 10.1.0.0 GA
- 10.1.0.1 Service Pack

Before applying Security Service Pack 2, please check the output of the command “av-version” and ensure that “AV_SSP_VERSION” is “001”. 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 2

Important Note: For FIPs deployment, it must upgrade AADS to 10.1.0.1 Service Pack before applying Security Service Pack 2.

Steps to apply Security Service Pack 2

1. Download "AV-AADS10.1-RHEL8.4-SSP-002-04.tar.bz2" to the admin user's home directory
2. Stop AADS services
 - a. `svc aads stop`
3. Apply Security Service Pack 2
 - a. `av-update-os AV-AADS10.1-RHEL8.4-SSP-002-04.tar.bz2`
4. SSP2 installation reboots the server at the end. After reboot, verify Security Service Pack 2 version
 - a. `av-version`

It shows the output as below

```
-----  
OS_VERSION: Red Hat Enterprise Linux release 8.4 (Ootpa)  
AV_SSP_VERSION: 002  
AV_BUILD_NUMBER: 04  
-----
```

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

Verification

- a. Run command "`av-version`"

On successful installation, it shows the output as below

```
-----  
OS_VERSION: Red Hat Enterprise Linux release 8.4 (Ootpa)  
AV_SSP_VERSION: 002  
AV_BUILD_NUMBER: 04  
-----
```

Failure

The command output is self-explanatory about the status of the run and refers to the verification process to check 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 2 updates following RPMS

```
kernel-4.18.0-372.9.1.el8.x86_64  
kernel-core-4.18.0-372.9.1.el8.x86_64  
kernel-modules-4.18.0-372.9.1.el8.x86_64  
kernel-tools-4.18.0-372.9.1.el8.x86_64  
kernel-tools-libs-4.18.0-372.9.1.el8.x86_64  
Important/Sec. python3-perf-4.18.0-372.9.1.el8.x86_64  
RHSA-2022:0825 Important/Sec.  
RHSA-2022:1550 Important/Sec.  
RHSA-2022:1988 Important/Sec.  
  
httpd-2.4.37-47.module+el8.6.0+15654+427eba2e.2.x86_64  
httpd-filesystem-2.4.37-47.module+el8.6.0+15654+427eba2e.2.noarch
```

httpd-tools-2.4.37-47.module+el8.6.0+15654+427eba2e.2.x86_64
mod_http2-1.15.7-5.module+el8.6.0+13996+01710940.x86_64
mod_ssl-1:2.4.37-47.module+el8.6.0+15654+427eba2e.2.x86_64
RHSA-2022:0891 Moderate/Sec.
RHSA-2022:1049 Important/Sec.
RHSA-2022:1915 Moderate/Sec.
RHSA-2022:5163 Low/Sec.

libarchive-3.3.3-3.el8_5.x86_64
RHSA-2022:0892 Moderate/Sec.

vim-minimal-8.0.1763-16.el8_5.13.x86_64
RHSA-2022:0894 Moderate/Sec.
RHSA-2022:1552 Moderate/Sec.

glibc-2.28-164.el8_5.3.x86_64
glibc-all-langpacks-2.28-164.el8_5.3.x86_64
glibc-common-2.28-164.el8_5.3.x86_64
glibc-langpack-en-2.28-164.el8_5.3.x86_64
RHSA-2022:0896 Moderate/Sec.

libxml2-2.9.7-12.el8_5.x86_64
python3-libxml2-2.9.7-12.el8_5.x86_644
RHSA-2022:0899 Moderate/Sec.

expat-2.2.5-4.el8_5.3.x86_64
RHSA-2022:0951 Important/Sec.

openssl-1.1.1k-6.el8_5.x86_64
openssl-libs-1.1.1k-6.el8_5.x86_644
RHSA-2022:1065 Important/Sec.

java-1.8.0-openjdk-1.8.0.332.b09-1.el8_5.x86_64
java-1.8.0-openjdk-devel-1.8.0.332.b09-1.el8_5.x86_64
java-1.8.0-openjdk-headless-1.8.0.332.b09-1.el8_5.x86_64
RHSA-2022:1491 Important/Sec.

gzip-1.9-13.el8_5.x86_64
RHSA-2022:1537 Important/Sec.

polkit-0.115-13.el8_5.2.x86_64
polkit-libs-0.115-13.el8_5.2.x86_64
RHSA-2022:1546 Moderate/Sec.

zlib-1.2.11-18.el8_5.x86_64
RHSA-2022:1642 Important/Sec.

libtiff-4.0.9-21.el8.x86_64
RHSA-2022:1810 Moderate/Sec.

libudisks2-2.9.0-9.el8.x86_64
udisks2-2.9.0-9.el8.x86_64
RHSA-2022:1820 Low/Sec.

python2-2.7.18-10.module+el8.6.0+14191+7fdd52cd.x86_64
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-pip-wheel-9.0.3-19.module+el8.6.0+13001+ad200bd9.noarch
RHSA-2022:1821 Moderate/Sec.

libpq-13.5-1.el8.x86_64
RHSA-2022:1891 Low/Sec.

platform-python-3.6.8-45.el8.x86_64
python3-libs-3.6.8-45.el8.x86_64
RHSA-2022:1986 Moderate/Sec.

cpio-2.12-11.el8.x86_64
RHSA-2022:1991 Moderate/Sec.

openssh-8.0p1-13.el8.x86_64
openssh-clients-8.0p1-13.el8.x86_64
openssh-server-8.0p1-13.el8.x86_64
RHSA-2022:2013 Moderate/Sec.

libssh-0.9.6-3.el8.x86_64
libssh-config-0.9.6-3.el8.noarch
RHSA-2022:2031 Low/Sec.

c-ares-1.13.0-6.el8.x86_64
RHSA-2022:2043 Moderate/Sec.

bind-export-libs-9.11.36-3.el8.x86_64
RHSA-2022:2092 Moderate/Sec.

grub2-common-2.02-123.el8_6.8.noarch
grub2-efi-x64-2.02-123.el8_6.8.x86_64
grub2-pc-2.02-123.el8_6.8.x86_64
grub2-pc-modules-2.02-123.el8_6.8.noarch
grub2-tools-2.02-123.el8_6.8.x86_64
grub2-tools-extra-2.02-123.el8_6.8.x86_64
grub2-tools-minimal-2.02-123.el8_6.8.x86_64
mokutil-0.3.0-11.el8_6.1.x86_64
shim-x64-15.6-1.el8.x86_64
RHSA-2022:2110 Low/Sec.
RHSA-2022:5095 Important/Sec.

rsyslog-8.2102.0-7.el8_6.1.x86_64
rsyslog-gnutls-8.2102.0-7.el8_6.1.x86_64
RHSA-2022:4799 Important/Sec.

xz-5.2.4-4.el8_6.x86_64
xz-libs-5.2.4-4.el8_6.x86_64
RHSA-2022:4991 Important/Sec.

cups-libs-2.2.6-45.el8_6.2.x86_64
RHSA-2022:5056 Important/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.