Product Support Notice

PSN #	PSN006057u				
Original publication date: 31-May-2022. This is Issue #01, published date: 31-May-2022.		Severity/risk level	Medium	Urgency	When convenient
Name of problem	Avaya Aura® Device Services Release 10.1 Security Service Pack (System Layer Update 4.0.0.0.7)				

Products affected

Avaya Aura® Device Services Release 10.1.x

Problem description

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

Resolution

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

Note: To apply this Security Service Pack the system should be in AADS 10.1.0.0.120 with "System layer version: 4.0.0.0.5"

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

Recommendation to take a VM snapshot before applying the patch.

Download

Follow the instructions below to download

1. Go to http://support.avaya.com
2. Under the “Support by Product” menu click on “Downloads”
3. Enter the product name as “system manager” and then select “Avaya Aura® Device Services ”
4. Select “10.1.x” from the Choose Release dropdown
5. Click on “Avaya Aura® Device Services 10.1.0.1 Service Pack, 10.1.x”.
6. Click on the file “ucapp-system-4.0.0.0.7.tgz, 10.1.x” to download

Patch install instructions — **Service-interrupting?** Yes

Steps to apply Security Service Pack

1. Download "ucapp-system-4.0.0.0.7.tgz" to the admin user’s home directory
2. tar xvzf ucapp-system-4.0.0.0.7.tgz
3. sudo ./update.sh -s
4. sysUpdate --status, in case it shows "sysUpdate: command not found", log off and log in again and then check "sysUpdate --status"
5. sysUpdate --install
    a. After this command completes the server will reboot
6. After the reboot, run the command “sys versions” to verify that it shows the updated system layer version - 4.0.0.0.7

Verification

Run the command “sys versions” to verify that it shows the updated system layer version - 4.0.0.0.7

Failure

n/a

Patch uninstall instructions

The patch cannot be uninstalled. Please use the VM snapshot version to move to the initial state of the system.

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 (System Layer Update 4.0.0.0.7) updates following RPMS
NetworkManager-1.32.10-4.el8.x86_64 NetworkManager-libnm-1.32.10-4.el8.x86_64 RHSA-2021:4361 Moderate/Sec. CVE-2020-13529 aide-0.16-14.el8_5.1.x86_64 RHSA-2022:0441 Important/Sec. CVE-2021-45417 bind-export-libs-9.11.26-6.el8.x86_64 RHSA-2021:4384 Moderate/Sec. CVE-2021-25214 cryptsetup-2.3.3-4.el8_5.1.x86_64 cryptsetup-libs-2.3.3-4.el8_5.1.x86_64 RHSA-2022:0370 Moderate/Sec. CVE-2021-4122 cups-libs-2.2.6-40.el8.x86_64 RHSA-2021:4393 Moderate/Sec. CVE-2020-10001 curl-7.61.1-22.el8.x86_64 libcurl-7.61.1-22.el8.x86_64 RHSA-2021:4511 Moderate/Sec. CVE-2021-22876 CVE-2021-22898 CVE-2021-22925 RHSA-2021:4059 Moderate/Sec. CVE-2021-22946 CVE-2021-22947

cyrus-sasl-lib-2.1.27-6.el8_5.x86_64
RHSA-2022:0658 Important/Sec.
CVE-2022-24407
dnf-4.7.0-4.el8.noarch
dnf-data-4.7.0-4.el8.noarch
libdnf-0.63.0-3.el8.x86_64
python3-dnf-4.7.0-4.el8.noarch
python3-hawkey-0.63.0-3.el8.x86_64
python3-libdnf-0.63.0-3.el8.x86_64
yum-4.7.0-4.el8.noarch
RHSA-2021:4464 Moderate/Sec.
CVE-2021-3445
file-5.33-20.el8.x86_64
file-libs-5.33-20.el8.x86_64
RHSA-2021:4374 Moderate/Sec.
CVE-2019-18218
glib2-2.56.4-156.el8.x86_64
RHSA-2021:4385 Moderate/Sec.
CVE-2021-3800
CVE-2021-28153
glibc-2.28-164.el8.x86_64
glibc-all-langpacks-2.28-164.el8.x86_64
glibc-common-2.28-164.el8.x86_64
glibc-langpack-en-2.28-164.el8.x86_64
RHSA-2021:4358 Moderate/Sec.
CVE-2021-27645
CVE-2021-33574
CVE-2021-35942
gnutls-3.6.16-4.el8.x86_64
nettle-3.4.1-7.el8.x86_64
RHSA-2021:4451 Moderate/Sec.
CVE-2021-3580
CVE-2021-20231
CVE-2021-20232
httpd-2.4.37-43.module+el8.5.0+13806+b30d9eec.1.x86_64
httpd-filesystem-2.4.37-43.module+el8.5.0+13806+b30d9eec.1.noarch
httpd-tools-2.4.37-43.module+el8.5.0+13806+b30d9eec.1.x86_64
mod_ssl-2.4.37-43.module+el8.5.0+13806+b30d9eec.1.x86_64
RHSA-2021:3816 Important/Sec.
CVE-2021-26691
CVE-2021-40438
RHSA-2021:4257 Moderate/Sec.
CVE-2021-26690
CVE-2021-30641
RHSA-2021:4537 Important/Sec.
CVE-2021-20325
RHSA-2022:0258 Important/Sec.
CVE-2021-44790

java-1.8.0-openjdk-1.8.0.322.b06-2.el8_5.x86_64
java-1.8.0-openjdk-devel-1.8.0.322.b06-2.el8_5.x86_64
java-1.8.0-openjdk-headless-1.8.0.322.b06-2.el8_5.x86_64
    RHSA-2022:0307 Moderate/Sec.
        CVE-2022-21248
        CVE-2022-21282
        CVE-2022-21283
        CVE-2022-21293
        CVE-2022-21294
        CVE-2022-21296
        CVE-2022-21299
        CVE-2022-21305
        CVE-2022-21340
        CVE-2022-21341
        CVE-2022-21360
        CVE-2022-21365
json-c-0.13.1-2.el8.x86_64
    RHSA-2021:4382 Moderate/Sec.
        CVE-2020-12762
kernel-4.18.0-348.12.2.el8_5.x86_64
kernel-core-4.18.0-348.12.2.el8_5.x86_64
kernel-modules-4.18.0-348.12.2.el8_5.x86_64
kernel-tools-4.18.0-348.12.2.el8_5.x86_64
kernel-tools-libs-4.18.0-348.12.2.el8_5.x86_64
python3-perf-4.18.0-348.12.2.el8_5.x86_64
    RHSA-2021:4056 Important/Sec.
        CVE-2020-36385
        CVE-2021-0512
        CVE-2021-3656
    RHSA-2022:0188 Important/Sec.
        CVE-2021-4155
        CVE-2022-0185
    RHSA-2021:4647 Important/Sec.
        CVE-2021-20317
        CVE-2021-43267
    RHSA-2021:5227 Moderate/Sec.
        CVE-2021-20321
    RHSA-2021:4356 Moderate/Sec.
        CVE-2019-14615
        CVE-2020-0427
        CVE-2020-24502
        CVE-2020-24503
        CVE-2020-24504
        CVE-2020-24586
        CVE-2020-24587
        CVE-2020-24588
        CVE-2020-26139
        CVE-2020-26140

CVE-2020-26141
CVE-2020-26143
CVE-2020-26144
CVE-2020-26145
CVE-2020-26146
CVE-2020-26147
CVE-2020-27777
CVE-2020-29368
CVE-2020-29660
CVE-2020-36158
CVE-2020-36312
CVE-2020-36386
CVE-2021-0129
CVE-2021-3348
CVE-2021-3489
CVE-2021-3564
CVE-2021-3573
CVE-2021-3600
CVE-2021-3635
CVE-2021-3659
CVE-2021-3679
CVE-2021-3732
CVE-2021-20194
CVE-2021-20239
CVE-2021-23133
CVE-2021-28950
CVE-2021-28971
CVE-2021-29155
CVE-2021-29646
CVE-2021-29650
CVE-2021-31440
CVE-2021-31829
CVE-2021-31916
CVE-2021-33033
CVE-2021-33200
kexec-tools-2.0.20-57.el8.x86_64
RHSA-2021:4404 Low/Sec.
CVE-2021-20269
libX11-1.6.8-5.el8.x86_64
libX11-common-1.6.8-5.el8.noarch
RHSA-2021:4326 Moderate/Sec.
CVE-2021-31535
libgcc-8.5.0-4.el8_5.x86_64
libgomp-8.5.0-4.el8_5.x86_64
libstdc++-8.5.0-4.el8_5.x86_64
RHSA-2021:4386 Low/Sec.
CVE-2018-20673
RHSA-2021:4587 Moderate/Sec.

CVE-2021-42574
libgcrypt-1.8.5-6.el8.x86_64
RHSA-2021:4409 Moderate/Sec.
CVE-2021-33560
libjpeg-turbo-1.5.3-12.el8.x86_64
RHSA-2021:4288 Moderate/Sec.
CVE-2020-17541
libsepol-2.9-3.el8.x86_64
RHSA-2021:4513 Moderate/Sec.
CVE-2021-36084
CVE-2021-36085
CVE-2021-36086
CVE-2021-36087
libsolv-0.7.19-1.el8.x86_64
RHSA-2021:4060 Moderate/Sec.
CVE-2021-33928
CVE-2021-33929
CVE-2021-33930
CVE-2021-33938
RHSA-2021:4408 Low/Sec.
CVE-2021-3200
libssh-0.9.4-3.el8.x86_64
libssh-config-0.9.4-3.el8.noarch
RHSA-2021:4387 Low/Sec.
CVE-2020-16135
libtiff-4.0.9-20.el8.x86_64
RHSA-2021:4241 Moderate/Sec.
CVE-2020-35521
CVE-2020-35522
CVE-2020-35523
CVE-2020-35524
libwebp-1.0.0-5.el8.x86_64
RHSA-2021:4231 Moderate/Sec.
CVE-2018-25009
CVE-2018-25010
CVE-2018-25012
CVE-2018-25013
CVE-2018-25014
CVE-2020-36330
CVE-2020-36331
CVE-2020-36332
lua-5.3.4-12.el8.x86_64
lua-libs-5.3.4-12.el8.x86_64
RHSA-2021:4510 Low/Sec.
CVE-2020-24370
ncurses-6.1-9.20180224.el8.x86_64
ncurses-base-6.1-9.20180224.el8.noarch
ncurses-libs-6.1-9.20180224.el8.x86_64

RHSA-2021:4426 Moderate/Sec.
CVE-2019-17594
CVE-2019-17595
nss-3.67.0-7.el8_5.x86_64
nss-softokn-3.67.0-7.el8_5.x86_64
nss-softokn-freebl-3.67.0-7.el8_5.x86_64
nss-sysinit-3.67.0-7.el8_5.x86_64
nss-util-3.67.0-7.el8_5.x86_64
RHSA-2021:4903 Critical/Sec.
CVE-2021-43527
openssh-8.0p1-10.el8.x86_64
openssh-clients-8.0p1-10.el8.x86_64
openssh-server-8.0p1-10.el8.x86_64
RHSA-2021:4368 Moderate/Sec.
CVE-2020-14145
openssl-1.1.1k-5.el8_5.x86_64
openssl-libs-1.1.1k-5.el8_5.x86_64
RHSA-2021:4424 Moderate/Sec.
CVE-2021-23840
CVE-2021-23841
RHSA-2021:5226 Moderate/Sec.
CVE-2021-3712
pcre-8.42-6.el8.x86_64
RHSA-2021:4373 Low/Sec.
CVE-2019-20838
CVE-2020-14155
platform-python-3.6.8-41.el8.x86_64
python3-libs-3.6.8-41.el8.x86_64
RHSA-2021:4057 Moderate/Sec.
CVE-2021-3733
RHSA-2021:4399 Moderate/Sec.
CVE-2021-3426
platform-python-pip-9.0.3-20.el8.noarch
python3-pip-9.0.3-20.el8.noarch
python3-pip-wheel-9.0.3-20.el8.noarch
RHSA-2021:4455 Low/Sec.
CVE-2021-3572
polkit-0.115-13.el8_5.1.x86_64
polkit-libs-0.115-13.el8_5.1.x86_64
RHSA-2022:0267 Important/Sec.
CVE-2021-4034
python2-2.7.18-7.module+el8.5.0+12203+77770ab7.x86_64
python2-libs-2.7.18-7.module+el8.5.0+12203+77770ab7.x86_64
RHSA-2021:4151 Moderate/Sec.
CVE-2020-27619
CVE-2020-28493
CVE-2021-20095
CVE-2021-20270

CVE-2021-23336
CVE-2021-27291
CVE-2021-28957
CVE-2021-42771
python3-rpm-4.14.3-19.el8_5.2.x86_64
rpm-4.14.3-19.el8_5.2.x86_64
rpm-build-libs-4.14.3-19.el8_5.2.x86_64
rpm-libs-4.14.3-19.el8_5.2.x86_64
rpm-plugin-selinux-4.14.3-19.el8_5.2.x86_64
rpm-plugin-systemd-inhibit-4.14.3-19.el8_5.2.x86_64
RHSA-2021:4489 Low/Sec.
CVE-2021-20266
RHSA-2022:0368 Moderate/Sec.
CVE-2021-3521
python36-3.6.8-38.module+el8.5.0+12207+5c5719bc.x86_64
RHSA-2021:4150 Moderate/Sec.
CVE-2021-20270
CVE-2021-27291
qt5-srpm-macros-5.15.2-1.el8.noarch
RHSA-2021:4172 Moderate/Sec.
CVE-2021-3481
sqlite-3.26.0-15.el8.x86_64
sqlite-libs-3.26.0-15.el8.x86_64
RHSA-2021:4396 Moderate/Sec.
CVE-2019-5827
CVE-2019-13750
CVE-2019-13751
CVE-2019-19603
CVE-2020-13435
tpm2-tools-4.1.1-5.el8.x86_64
RHSA-2021:4413 Moderate/Sec.
CVE-2021-3565
vim-minimal-8.0.1763-16.el8_5.4.x86_64
RHSA-2021:4517 Moderate/Sec.
CVE-2021-3778
CVE-2021-3796
RHSA-2022:0366 Moderate/Sec.
CVE-2021-3872
CVE-2021-3984
CVE-2021-4019
CVE-2021-4192
CVE-2021-4193

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.