Product Support Notice

PSN # PSN006224u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.			
Original publication date: 17-Nov-23. This is Issue #02, published date: 22-Nov-23	Severity/risk level	High	Urgency	Immediately
Name of problem	IP Office - Apache ActiveMQ vulnerability			

Products affected

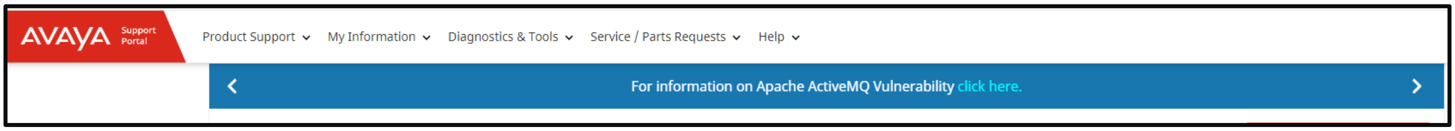
IP Office with one-X-Portal deployments versions 11.1.3.0 and 11.1.2.x

Problem description

Ensure that you are signed up for Avaya E-notifications so that you will be notified when new issues of this PSN are posted.

High Impact

Avaya is aware of the recently identified ActiveMQ vulnerability (CVE-2023-46604) and is conducting impact assessments across its portfolio. Reference the Avaya Product Security Apache ActiveMQ Vulnerability (CVE-2023-46604) - Impact for Avaya products on support.avaya.com. This link is also accessible when navigating to support.avaya.com and selecting the link in the crawler at the top of the page (see screenshot below).



For information on Apache ActiveMQ Vulnerability click here.

End of Manufacturer's Support (EoMS):

Avaya is prioritizing our GA products in a phased approach based on risk level and expected impact. Products/versions designated EoMS are not being investigated at this time and customers are encouraged to upgrade to a supported product/version.

Internal analysis has determined:

- IP Office releases are vulnerable to this CVE and development has provided guidance to mitigate the vulnerability in the mitigation section under Security Notes of this PSN.

This PSN will be updated as more information becomes available.

Resolution

No, a patch is not available yet.

Workaround or alternative remediation

See mitigation section under Security Notes below.

Remarks

Issue 1: Original publication November 17, 2023.

Patch Notes

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

Backup before applying the patch

n/a

Download

n/a

Patch install instructions	Service-interrupting?
n/a	No

Verification

n/a

Failure

n/a

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

Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-46604

Avaya Security Vulnerability Classification

High

Mitigation

The IP Office one-X Portal component uses Active MQ and exposes its services over port 61615. The port is only opened when the one-X Portal is configured in Resiliency mode.

Until a permanent solution is available, please implement firewall rules as a mitigation measure to

a) block external access (direct internet access) to port 61615.
b) Restrict the port to only allow communication from the IP address of the peer IP Office server.
c) You may also stop the one-X portal service from the IP Office WebControl 7071 login.

Avaya has created a script to help facilitate the addition of Firewall rules to mitigate the issue.
This script, “apply_patch.sh”, is available on PLDS under Download ID: IPO00009499.

Please utilize the steps below to apply the script.
If additional support is required, open an Avaya Service Request for guidance.

Steps for application of the script
1. Use WinSCP to connect and upload script to the one-X Portal Server (Both Primary and Secondary)

2. Connect as root on the machine, using machine direct console or by using putty/ssh:
By default, root is disabled to connect via putty/ssh.
To connect remotely first connect using Administrator and get in the root console using CLI commands:

```
login as: Administrator
Administrator@<ip-address>'s password:

*******************************************
*            Avaya IP Office            *
*                                  *
*     WARNING: Authorised Access Only     *
*******************************************

Welcome Administrator it is Thu Nov  9 05:45:09 EST 2023
> admin
Please enter Service User:Administrator
Please enter Administrator password:
Login successful
```

```
Admin> root
Please enter password:

Login Successful.
Last login: Thu Nov  9 05:33:03 EST 2023 on tty1
[root@test1 ~]#
```

3. Execute:

```
cd <directory-of-patch>
chown root:root ./apply_patch.sh
chmod +x ./apply_patch.sh
```

4. Execute script:

   For Primary(if no secondary remove the second argument)

```
./apply_patch.sh <Primary IP Address> <Secondary IP Address>
```

   For Secondary(if no primary remove the second argument)

```
./apply_patch.sh <Secondary IP Address> <Primary IP Address>
```

5. Leave the script in the same location

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 LLC, 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.