Description of ActiveMQ Remote Code Execution Vulnerability (CVE-2023-46604)

Notice ID: *DHCC-SN-202311-001*

First Published: *2023-11-01*

Summary

We are concerned that Apache ActiveMQ has been exposed to a remote code execution vulnerability. The vulnerability number is CVE-2023-46604 CVSS score is 10.0, and attackers can exploit this vulnerability to execute arbitrary code remotely.

Dahua immediately investigated the affected situation of Dahua products in response to this missing exhibition technology. The current investigation results are as follows:

1) Embedded device products (including but not limited to: IPC, HDCVI, PTZ, ITC, NVR, DVR storage, etc.) are NOT by this vulnerability.

2) The list of software products affected is as follows:

Affected Product	Affected Version
DSS-Professional	V7.0-V8.3
DSS-Express	V7.0-V8.3
DHI-DSS7016DR-S2	V1.0-V8.3
DHI-DSS4004-S2	V1.0-V8.3

If the products you use are affected, we suggest that you take the following measures immediately to prevent them:

1) Prohibit ActiveMQ ports from being open to the public or change ActiveMQ default port 61616 to another port (Note: the default port is 61616. You can view the port enabled by ActiveMQ service by logging in to the config web page or DSS config tool).
2) Contact Dahua local technical support or software_support@dahuatech.com for help.

We are urgently fixing the vulnerability patch and release it on our Dahua Wiki: https://dahuawiki.com/DSS

Support Resources

For any cybersecurity questions or concerns related to Dahua products and solutions, please contact Dahua Tech Support Team at support.usa@dahuatech.com.