VECTOR

PREEvision

Important Security Information (last update: 11.12.2023)

Apache ActiveMQ security vulnerabilities

Following critical security vulnerabilities within Apache ActiveMQ has been discovered lately.

CVE-2023-46604	The Java OpenWire protocol marshaller is vulnerable to Remote Code Execution. This vulnerability may allow a remote attacker with network access to a Java-based OpenWire broker to run arbitrary shell commands by manipulating serialized class types in the OpenWire protocol to cause the broker (respectively) to instantiate any class on the classpath.

Applicability to PREEvision

Apache Active MQ libraries affected by the security vulnerability are integrated in the PREEvision messaging server component.

Risk analysis

Apache ActiveMQ is vulnerable to Remote Code Execution (RCE). This vulnerability exists due to a flaw in the OpenWire protocol handling and could allow an attacker with network access to a broker to potentially run arbitrary shell commands. This is considered a high risk.

There is no known workaround for this issue.

Recommended actions

We have resolved the security issue in the PREEvision releases 10.10 and 10.0 SP17.
The Apache ActiveMQ libraries, which are integrated in the PREEvision messaging server component, have been updated to version 5.16.7.
We highly recommend that you update your PREEvision system to these new versions.

For previous PREEvision 9.0, 9.5, 10.0 versions and 10.5 to 10.9 versions, we highly recommend that you patch the PREEvision messaging server component.
You can download the patch and an installation instruction from the Vector download center:
https://www.vector.com/int/en/download/preevision-messaging-server-component-patch/