KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

KRONES Security Advisory “Apache ActiveMQ Deserialization of Untrusted Data Vulnerability, Nov 2023” (KSA-2023-4)

In November 2023, the Apache Software Foundation released a security advisory on a security vulnerability affecting their ActiveMQ software. An attacker, who successfully exploits the vulnerability, can execute arbitrary code on affected systems.

For the affected products and services, Krones rates the likelihood of being exploited as low. Therefore, no specific action is required.

Affected products and services

The following table lists affected products or services, and specific remediation. Krones recommends implementing the suggested remediation measures.

No.	Likelihood of exploitation[1]	Affected products or services	Default state and remediation
1	Low	System Logistics GmbH Warehouse Control System (WCS)	• By default, systems running WCS aren’t exposed to the internet and an attacker would need a VM account as a precondition to exploit the vulnerability. • System Logistics may offer customer-specific updates. Please get in touch with System Logistics Customer Services via Customer.Service@systemlogistics.de.
	Krones may add additional affected products or services, or update remediations as soon as there is new information available.		

Workarounds and mitigation

The following specific workarounds and mitigation are recommended in addition to the remediation measures listed above to further reduce the risk originating from the security vulnerability:

- Use firewalls to limit network traffic between servers running WCS and other necessary systems.
- If applicable, monitor your complete network traffic to detect abnormal traffic to WCS.
- Log and monitor access to VMs (e.g., access to the VMs of WCS).

Security contact

If you have any questions regarding this security advisory or other security-related questions, please contact the Product Security Incident Response Team (PSIRT) of Krones: cyber.security@krones.com

OpenPGP key for confidential messages:
https://www.krones.com/ext/securitytxt/cyber.security@krones.com.asc

[1] The likelihood of exploitation is rated by Krones for the default Krones use case of the product in its delivery condition. This value may vary in case of customer-specific solutions or changes of the delivery condition.

KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

Appendix A: Technical description of the security vulnerabilities

This section describes security vulnerabilities covered by this Krones Security Advisory. For each security vulnerability, Krones includes the following public information:

- **Description:** A brief description of the security vulnerability as mentioned in the original security advisory or in the National Vulnerability Database (NVD).
- **CVSS v3.1 Base Score:** The current CVSS v3.1 Base Score as mentioned in the original security advisory or in the National Vulnerability Database (NVD).
- **Listed in CISA Known Exploited Vulnerability Catalog:** Information whether the CISA KEV Catalog lists the security vulnerability. Being listed in the CISA KEV Catalog means that exploitation of the security vulnerability is publicly known. Krones recommends prioritizing handling security vulnerabilities listed in the CISA KEV Catalog.
- **EPSSv3 Score:** The current EPSSv3 Score as available via the FIRST EPSS API. Krones recommends prioritizing handling security vulnerabilities having a high EPSSv3 Score as this may indicate an increased likelihood of being exploited.

Vulnerability CVE-2023-46604

- **Description:** The Java OpenWire protocol marshaller is vulnerable to Remote Code Execution. This vulnerability may allow a remote attacker with network access to either a Java-based OpenWire broker or client to run arbitrary shell commands by manipulating serialized class types in the OpenWire protocol to cause either the client or the broker (respectively) to instantiate any class on the classpath.
- **CVSS v3.1 Base Score:** 10.0 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:H)
- **Listed in CISA Known Exploited Vulnerability Catalog:** Yes
- **EPSSv3 Score:** Exploited

Appendix B: Further information

- Original security advisory by Apache Software Foundation - activemq.apache.org/security-advisories.data/CVE-2023-46604

Appendix C: Changelog

Version	Date	Changes
1.0	2023-12-01	Initial publication by the Krones PSIRT