

## Xylem Product Security Advisory

### CVE-2023-46604 for Sensus RNI

2023-11-16

#### Overview

Xylem is aware of vulnerability CVE-2023-46604 associated with specific versions of Apache ActiveMQ that exist within the RNI product. A pre-condition to exploit the vulnerability is the use of serialized class types; the RNI implementation does not make use of serialized class types and cannot be configured to do so. Therefore, the RNI is not exposed to this vulnerability. This conclusion of no impact was further reinforced through internal security testing.

#### Affected Products and Versions

Analysis of the RNI product concludes that there are no vulnerability impacts from CVE-2023-46604 to the RNI product. The following RNI versions were tested to confirm the analysis:

- RNI – 4.12.1, confirmed no impact
- RNI – 4.13.1, confirmed no impact
- RNI – 4.14.1, confirmed no impact

#### Vulnerability Details

##### CVE-2023-46604

CVSS v3.1 Base Score 9.8 | CRITICAL | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

#### Mitigations

No mitigation to RNI products is required.

#### References

- [Xylem Product Security Advisories](#)
- CVE-2023-46604: [NIST National Vulnerability Database \(NVD\)](#) and [MITRE CVE® List](#)

#### Contact Information

For any questions related to this Xylem Product Security Advisory, please contact [product.security@xylem.com](mailto:product.security@xylem.com).

| Revision History |               |
|------------------|---------------|
| Version          | Updates       |
| 1.0              | Initial draft |

### Disclaimer

This document is provided on an as-is basis and does not imply any kind of guarantee or warranty, including the warranties of merchantability or fitness for a particular use. Use of the information in this document or materials linked from this document is at your own risk. Xylem reserves the right the change or update this document any time.