Contribution ID: **333** Type: **Paper presentation**

Exploiting Log4J for Remote Code Execution: A Cybersecurity Analysis of the Particularities of CVE-2023-50780 in RedHat AMQ

Friday 19 September 2025 11:30 (15 minutes)

Java Management Extensions (JMX) are essential for administrating Java applications, yet their exposure via HTTP bridges like Jolokia can create significant security risks. This paper investigates how vendor-specific modifications in downstream enterprise products can alter the attack surface of known vulnerabilities. Focusing on CVE-2023-50780, we analyze a critical misconfiguration in RedHat AMQ where Log4J's scripting capabilities are enabled by default. This research demonstrates a direct "fire and forget" remote code execution (RCE) vector that is significantly more efficient than the complex, multi-stage file-write exploits documented in its upstream counterpart, Apache ActiveMQ Artemis. Through empirical analysis and a reproducible methodology, we answer our research question by confirming that insecure-by-default settings in commercial products can introduce simpler, more direct attack paths, challenging the assumption that downstream derivatives, even enterprise grade ones, are inherently more secure. Our findings underscore the need for rigorous, independent security validation of vendor-specific configurations in the software supply chain.

Authors: Mr CĂCIULESCU, Alexandru Răzvan (National University of Science and Technology POLITEHNICA Bucharest); Mr BĂDĂNOIU, Matei (Independent Researcher)

Co-author: RUGHINIȘ, Caius (National University of Science and Technology POLITEHNICA Bucharest)

Presenter: Mr CĂCIULESCU, Alexandru Răzvan (National University of Science and Technology POLITEHNICA Bucharest)

Session Classification: Network Security