computers

MDPI

Article

Exploiting Jolokia for Remote Code Execution: A Cybersecurity Analysis of CVE-2023-50780 in Apache ActiveMQ Artemis

Alexandru Răzvan Căciulescu [1], Matei Bădănoiu [2], Răzvan Rughiniș [1,3,*] and Dinu Țurcanu [4]

[1] Faculty of Automatic Control and Computers, National University of Science and Technology POLITEHNICA Bucharest, 060042 Bucharest, Romania; acaciulescu@upb.ro
[2] Independent Researcher, 060042 Bucharest, Romania
[3] Academy of Romanian Scientists, 3 Ilfov, 050044 Bucharest, Romania
[4] Faculty of Electronics and Telecommunications and National Institute of Innovations in Cybersecurity "CYBERCOR", Technical University of Moldova, 168, Stefan cel Mare Blvd, MD-2004 Chisinau, Moldova; dinu.turcanu@adm.utm.md
* Correspondence: razvan.rughinis@upb.ro

Abstract

Java middleware platforms expose powerful management functions through HTTP-accessible interfaces such as Jolokia. This article discusses the analysis of CVE-2023-50780 in Apache ActiveMQ Artemis by framing the vulnerability as a management-plane state-transition problem rather than as a set of isolated exploit recipes. We analyze three remote-code-execution paths that combine Jolokia-accessible MBeans with Log4J2 configuration mutability, Artemis filesystem and deployment semantics, broker or web-server restart behavior, and, in one vector, the Java DiagnosticCommand interface. The study defines a formal attacker model; separates demonstrated preconditions from deployment-dependent assumptions; compares the three vectors across required privileges, network dependencies, writable artifacts, execution triggers, reliability, detection opportunities, and mitigations; and evaluates defensive controls at the level of the exploit stage they interrupt. The paper also clarifies the responsible-disclosure context and reduces operational payload detail in favor of defender-oriented evidence, validation tables, and architectural analysis. The resulting contribution is a reproducible but bounded case study of how legitimate administrative operations can compose into code execution when management interfaces are exposed without sufficient privilege separation, MBean restriction, filesystem hardening, and upgrade controls.

Keywords: Apache ActiveMQ Artemis; Jolokia; JMX; Log4J2; management-plane security; remote code execution; vulnerability analysis; middleware security

Academic Editor: Paolo Bellavista

Received: 1 May 2026
Revised: 30 May 2026
Accepted: 31 May 2026
Published: 4 June 2026

References

1. Oracle Corporation. Java Management Extensions (JMX) Technology. Available online: https://www.oracle.com/java/technologies/javase/javamanagement.html (accessed on 27 April 2026).
2. Huss, R. Jolokia—Overview and Introduction. Available online: https://jolokia.org/ (accessed on 27 April 2026).
3. Block, A. Jolokia JVM Monitoring in OpenShift. Red Hat Developer Blog. 30 March 2016. Available online: https://developers.redhat.com/blog/2016/03/30/jolokia-jvm-monitoring-in-openshift (accessed on 27 April 2026).
4. Apache Software Foundation. Apache Log4j 2—Introduction. Available online: https://logging.apache.org/log4j/2.x/ (accessed on 27 April 2026).
5. Apache Software Foundation. Apache Log4j 2.x Manual. Available online: https://logging.apache.org/log4j/2.x/manual/ (accessed on 27 April 2026).
6. Apache Software Foundation. CVE-2023-50780: Apache ActiveMQ Artemis. Available online: https://www.cve.org/CVERecord?id=CVE-2023-50780 (accessed on 27 April 2026).
7. National Institute of Standards and Technology (NIST). CVE-2021-44228 Detail. National Vulnerability Database, 2021. Available online: https://nvd.nist.gov/vuln/detail/CVE-2021-44228 (accessed on 27 April 2026).
8. Cybersecurity and Infrastructure Security Agency (CISA). Log4Shell (CVE-2021-44228) Guidance, 2021. Available online: https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance (accessed on 27 April 2026).
9. Apache Software Foundation. Apache ActiveMQ Artemis—Overview. Available online: https://activemq.apache.org/components/artemis/ (accessed on 27 April 2026).
10. Sayar, I.; Bartel, A.; Bodden, E.; Le Traon, Y. An In-Depth Study of Java Deserialization Remote-Code Execution Exploits and Vulnerabilities. *ACM Trans. Softw. Eng. Methodol.* **2023**, *32*, 1–45. [CrossRef]
11. Bartel, A.; Klein, J.; Le Traon, Y. MUSTI: Dynamic Prevention of Invalid Object Initialization Attacks. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 2167–2178. [CrossRef]
12. Shcherbakov, M.; Balliu, M. SerialDetector: Principled and Practical Exploration of Object Injection Vulnerabilities for the Web. In Proceedings of the Network and Distributed System Security Symposium (NDSS), Online, 21–25 February 2021. [CrossRef]
13. Meng, N.; Nagy, S.; Yao, D.D.; Zhuang, W.; Arango-Argoty, G. Secure Coding Practices in Java: Challenges and Vulnerabilities. In *Proceedings of the 40th International Conference on Software Engineering (ICSE), Gothenburg, Sweden, 27 May–3 June 2018*; Association for Computing Machinery: New York, NY, USA, 2018; pp. 372–383. [CrossRef]
14. Mousavi, Z.; Islam, C.; Babar, M.A.; Abuadbba, A.; Moore, K. Detecting Misuse of Security APIs: A Systematic Review. *ACM Comput. Surv.* **2025**, *57*, 1–39. [CrossRef]
15. Zhao, L.; Chen, S.; Xu, Z.; Liu, C.; Zhang, L.; Wu, J.; Sun, J.; Liu, Y. Software Composition Analysis for Vulnerability Detection: An Empirical Study on Java Projects. In Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE), San Francisco, CA, USA, 3–9 December 2023. [CrossRef]
16. Pour, M.S.; Nader, C.; Friday, K.; Bou-Harb, E. A Comprehensive Survey of Recent Internet Measurement Techniques for Cyber Security. *Comput. Secur.* **2023**, *128*, 103123. [CrossRef]
17. Everson, D.; Cheng, L. A Survey on Network Attack Surface Mapping. *Digit. Threat. Res. Pract.* **2024**, *5*, 1–25. [CrossRef]
18. Dahlmanns, M.; Lohmöller, J.; Fink, I.B.; Pennekamp, J.; Wehrle, K.; Henze, M. Easing the Conscience with OPC UA: An Internet-Wide Study on Insecure Deployments. In *Proceedings of the ACM Internet Measurement Conference, Virtual, 27–29 October 2020*; Association for Computing Machinery: New York, NY, USA, 2020; pp. 101–110. [CrossRef]
19. Dahlmanns, M.; Lohmöller, J.; Pennekamp, J.; Bodenhausen, J.; Wehrle, K.; Henze, M. Missed Opportunities: Measuring the Untapped TLS Support in the Industrial Internet of Things. In *Proceedings of the ACM Asia Conference on Computer and Communications Security (ASIACCS), Virtual, 30 May–3 June 2022*; Association for Computing Machinery: New York, NY, USA, 2022; pp. 252–266. [CrossRef]
20. Babenko, T.; Kolesnikova, K.; Abramkina, O.; Vitulyova, Y. Automated OSINT Techniques for Digital Asset Discovery and Cyber Risk Assessment. *Computers* **2025**, *14*, 430. [CrossRef]
21. Kalra, G.S. Threat Analysis of an Enterprise Messaging System. *Netw. Secur.* **2014**, *2014*, 5–9. [CrossRef]
22. McAteer, I.N.; Malik, M.I.; Baig, Z.; Hannay, P. Security Vulnerabilities and Cyber Threat Analysis of the AMQP Protocol for the Internet of Things. In *Proceedings of the 15th Australian Information Security Management Conference, Perth, Australia, 5–6 December 2017*; Edith Cowan University: Perth, Australia, 2017; pp. 70–80. [CrossRef]
23. Baouya, A.; Hamid, B.; Gürgen, L.; Bensalem, S. Rigorous Security Analysis of RabbitMQ Broker with Concurrent Stochastic Games. *Internet Things* **2024**, *26*, 101161. [CrossRef]

24. Abioye, T.E.; Arogundade, O.T.; Misra, S.; Adesemowo, K.; Damaševičius, R. Cloud-Based Business Process Security Risk Management: A Systematic Review, Taxonomy, and Future Directions. *Computers* **2021**, *10*, 160. [CrossRef]
25. Wang, M.; Sun, Y.; Sun, H.; Zhang, B. Security Issues on Industrial Internet of Things: Overview and Challenges. *Computers* **2023**, *12*, 256. [CrossRef]
26. Obaidat, M.A.; Obeidat, S.; Holst, J.; Al Hayajneh, A.; Brown, J. A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures. *Computers* **2020**, *9*, 44. [CrossRef]
27. Everson, D.; Cheng, L.; Zhang, Z. Log4shell: Redefining the Web Attack Surface. In Proceedings of the Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb), San Diego, CA, USA, 3 March 2022. [CrossRef]
28. Hiesgen, R.; Nawrocki, M.; Kristoff, J.; Waehlisch, M. The Log4j Incident: A Comprehensive Measurement Study of a Critical Vulnerability. *IEEE Trans. Netw. Serv. Manag.* **2024**, *21*, 5921–5934. [CrossRef]
29. Caciulescu, A.R.; Badanoiu, M.; Rughinis, R.; Turcanu, D. Remote Code Execution via Log4J MBeans: Case Study of Apache ActiveMQ (CVE-2022-41678). *Computers* **2025**, *14*, 355. [CrossRef]
30. Laluka. Jolokia Exploitation Toolkit. GitHub Repository. Available online: https://github.com/laluka/jolokia-exploitation-toolkit (accessed on 27 April 2026).
31. Pyn3rd. A New Way of Jolokia Remote Code Execution. 15 November 2022. Available online: https://pyn3rd.github.io/2022/11/15/A-New-Way-of-Jolokia-Remote-Code-Execution/ (accessed on 27 April 2026).
32. Badanoiu, M. Log4Jolokia. GitHub Repository. Available online: https://github.com/mbadanoiu/Log4Jolokia (accessed on 27 April 2026).
33. Badanoiu, M. jvmtiAgentLoad-Exploit. GitHub Repository. Available online: https://github.com/mbadanoiu/jvmtiAgentLoad-Exploit (accessed on 27 April 2026).
34. Apache Software Foundation. ActiveMQ Artemis Documentation: Configuration Reference. Available online: https://activemq.apache.org/components/artemis/documentation/latest/configuration-index.html (accessed on 27 April 2026).
35. Badanoiu, M. Java-Servlets-Shell. GitHub Repository. Available online: https://github.com/mbadanoiu/Java-Servlets-Shell (accessed on 27 April 2026).
36. Offensive Security. MSFvenom. Available online: https://www.offsec.com/metasploit-unleashed/msfvenom/ (accessed on 27 April 2026).
37. Bray, T.; Paoli, J.; Sperberg-McQueen, C.M.; Maler, E.; Yergeau, F.; Cowan, J. Extensible Markup Language (XML) 1.0 (Fifth Edition). W3C Recommendation. 26 November 2008. Available online: https://www.w3.org/TR/xml/ (accessed on 27 April 2026).
38. Ain, Q.U.; Ahmed, S.; Zafar, A.; Mehmood, M.A.; Waheed, A. Analysis of Hotspot Methods in JVM for Best-Effort Run-Time Parallelization. In *Proceedings of the International Conference on Computing and Electronic Engineering (IC4E 2018), San Diego, CA, USA, 11–13 January 2018*; Association for Computing Machinery: New York, NY, USA, 2018; pp. 60–63. [CrossRef]
39. Oracle Corporation. JVM Tool Interface (JVMTI), Java SE 8. Available online: https://docs.oracle.com/javase/8/docs/platform/jvmti/jvmti.html (accessed on 27 April 2026).