

Alert: Exploitation of CVE-2026-34197 in Apache ActiveMQ

By Cyber Threat Intelligence

Published: 2026-06-10 · Archived: 2026-06-12 02:00:47 UTC

本文改寫自 TeamT5 〈2026 年 4 月第二期的漏洞情資報告 (2026 April H2 Vulnerability Insights Report)〉。TeamT5 漏洞研究團隊致力於針對重大漏洞提供即時的應對措施與緩解方案。如欲進一步了解 TeamT5 的漏洞情資報告，[請與我們聯繫](#)。

TeamT5 偵測到 Apache ActiveMQ 中的一個嚴重漏洞 (CVE-2026-34197) 已被包括中國 APT 組織 SLIME88 積極利用。我們的調查顯示，SLIME88 在利用該漏洞後部署了 SoxAgent RAT，以入侵 Linux 設備並建置 ORB 網路。我們目前以臨時名稱 GOBLIN14 追蹤該 ORB 網路。SLIME88 最早的攻擊可以追溯到 4 月 7 日。SLIME88 攻擊活動的受害者包括美國以及韓國、印度、法國和美國的 IT 與製造業。本文詳細說明攻擊手法與情況。

The following blog post is based on our 2026 April H2 Vulnerability Insights Report. TeamT5 Vulnerability Research Team is dedicated to providing timely mitigation and response guidelines to critical vulnerabilities. [Contact us](#) for more information about our vulnerability intelligence.

Active Exploitation of CVE-2026-34197 in Apache ActiveMQ

TeamT5 has detected that a critical vulnerability (CVE-2026-34197) in Apache ActiveMQ has been actively exploited by threat actors, including the China-nexus APT SLIME88. Our investigation revealed that after exploitation, SLIME88 deployed SoxAgent RAT to compromise Linux devices and build an ORB network. We currently track the ORB network under the temporary name, GOBLIN14. The earliest SLIME88 attack can be traced back to April 7, shortly after the vulnerability was disclosed. The victims of SLIME88's campaign included IT and manufacturing entities in the US, as well as entities in South Korea, India, France, and the US.

We conclude the affected entities in **Exploitation Status** below.

Executive Summary

We assessed the severity of CVE-2026-34197 as critical and advised our customers to use this report to mitigate the impact. CVE-2026-34197 is a remote code execution (RCE) vulnerability in Apache ActiveMQ, an open-source Java message broker widely used in enterprise environments, across financial institutions, healthcare sector, governments, and more.

Threat actors would send a crafted HTTP request to Apache ActiveMQ's Jolokia API endpoint, triggering the ActiveMQ broker to fetch a malicious XML configuration file from the C2 server and ultimately resulting in remote code execution. Although CVE-2026-34197 requires authentication, default credentials (`admin/admin`) are common in many cases. On some versions of Apache ActiveMQ, actors can exploit CVE-2024-32114[1] to bypass authentication.

Apache disclosed CVE-2026-34197 on April 7 with mitigation information[2]. Public report indicated the vulnerability had been detected prior to the disclosure[3]. A proof-of-concept (PoC) exploit subsequently became publicly available,[4] and threat actors were observed exploiting the vulnerability in the wild shortly after disclosure.[5]

Based on our investigation and current exploitation status of CVE-2026-34197, we depicted the Forensic Artifacts in this report and prepared a comprehensive Mitigation and Response Advisory for our customers.

The Mitigation and Response Advisory includes:

- Official Information
- Related Indicators of Compromise of this vulnerability.
- Threat Hunting Tool:
 - Log parsers to analyze ActiveMQ broker log produced by the exploitation of CVE-2026-34197

Exploitation Status

CVE-2026-34197 has been actively exploited by threat actors, including the Chinese APT SLIME88. The victims included IT and manufacturing entities in the US, as well as entities in South Korea, India, France, and the US.

- China-nexus SLIME88[6] exploited CVE-2026-34197 to implant SoxAgent on Apache ActiveMQ entity.
 - After receiving the crafted HTTP request, the victim host would fetch a malicious XML payload[7] from the C2 to exploit CVE-2026-34197, resulting in remote code execution.
 - Afterwards, the actor deployed a download script[8] for SoxAgent.
 - The C2 of the download script is 103.201.131.121.
 - We detected sample of SoxAgent[9].
 - The C2s of SoxAgent are `www.fastsecurey.info` and 103.201.131.121.
 - The victims included IT and manufacturing entities in the US, as well as entities in South Korea, India, France, and the US.
 - We assessed that SLIME88 sought to compromise these devices with SoxAgent to build an ORB network, which we currently track as GOBLIN14.
- All malicious indicators associated with CVE-2026-34197 are summarized in the IoC section of this report. The full list can be downloaded via download page of ThreatVision.

Mitigation and Response Advisory

1. Official Information

Apache patched CVE-2026-34197 in ActiveMQ Classic Version `6.2.3` and `5.19.4` , released respectively on March 30 and 31. We highly recommend our clients and partners apply the patch as soon as possible.

-

2. Mitigation

It is recommended to change the default credentials (e.g. `admin/admin`) and restrict access to Jolokia (`/api/jolokia`) and the Web Console, as these management interfaces expose sensitive broker operations.

3. Threat Hunting Tools

CVE-2026-34197 has been actively exploited by threat actors. Our vulnerability team provided log parsers to analyze broker logs produced by the exploitation of CVE-2026-34197.

The tools can also be downloaded from ThreatVision **Threat Hunting Tools**.

Forensic Artifacts

Threat actors would send a crafted HTTP request to Apache ActiveMQ's Jolokia API endpoint. After receiving the request, the ActiveMQ broker would then process a malicious URI embedded in the HTTP request and retrieve a remote XML configuration file from the C2 server, triggering the exploitation of CVE-2026-34197 and ultimately achieving remote code execution.

Therefore, we recommend using the log parser[10] to check the ActiveMQ broker log (`activemq.log`) for URIs containing `vm://` and `?brokerConfig` , which may indicate exploitation attempts.

- Below is an example of a broker log produced by the exploitation of CVE-2026-34197:

```
2026-04-27 08:44:38,999 | INFO | Establishing network connection from vm://localhost to vm://evil?brokerConfig=
2026-04-27 08:44:39,028 | WARN | Could not connect to remote URI: vm://evil?brokerConfig=xbean:http://<REDACTED>
2026-04-27 08:44:39,029 | INFO | Network Connector DiscoveryNetworkConnector:NC:BrokerService[localhost] started
```

In some cases, the ActiveMQ broker may attempt to reconnect to the C2 server indefinitely. Each retry would attempt to re-fetch the malicious XML configuration file, generating failure errors in `activemq.log` . The error logs will contain `Failed to load URL` and `connection error` , which also serves as forensic artifacts of exploitation attempts.

- Below is an example of the error log:

```
2026-04-27 08:50:10,379 | ERROR | Failed to load: URL [http://<REDACTED>/evil.xml], reason: IOException parsing
org.springframework.beans.factory.BeanDefinitionStoreException: IOException parsing XML document from URL [http:
at org.springframework.beans.factory.xml.XmlBeanDefinitionReader.loadBeanDefinitions(XmlBeanDefinitionReader.jav
at org.springframework.beans.factory.xml.XmlBeanDefinitionReader.loadBeanDefinitions(XmlBeanDefinitionReader.jav
at org.apache.xbean.spring.context.ResourceXmlApplicationContext.loadBeanDefinitions(ResourceXmlApplicationConte
```

Appendix I: Malware Table

Malware Table introduces the malware mentioned in this report.

Name	Type	Description	Used by	First Seen
SoxAgent	RAT	SoxAgent is a Linux backdoor that silently converts compromised hosts into SOCKS5 relay nodes. It maintains a persistent reverse connection to a hardcoded C2, negotiates AES-encrypted tunnels dynamically, and forwards TCP traffic through the victim to conceal attacker origin. Its supporting capabilities include remote update, self-deletion, and heartbeat reporting with falsified tunnel metrics.	SLIME88	2026.04

Appendix II: Other critical CVEs

TeamT5 also provides **Patch Management Report (PMR)**. Published every week (or more), the PMR will provide our customers with concise yet comprehensive updates on the most critical and exploitable vulnerabilities selected by TeamT5 vulnerability research team during the period. Each vulnerability will be provided with patch information. If you are interested in subscribing to this new report series, please [contact TeamT5 for more information](#).

Reference

[1] CVE-2024-32114 is a vulnerability in Apache ActiveMQ Classic versions 6.0.0 through 6.1.1 which exposes the Jolokia API endpoint without authentication, allowing unauthenticated actors to interact directly with broker management operations.

<https://nvd.nist.gov/vuln/detail/cve-2024-32114>

[6] SLIME88 is a China-nexus APT. SLIME88 has targeted Taiwan's energy sector through phishing emails and fake certificate installer, attempting to deploy backdoor programs such as AdaptixC2 and CobaltStrike. SLIME88 often uses Cloudflare to hide the real C2 IP address in order to evade tracking by researchers.

[7] SHA-256: c5eacffa5c909209f97f720740802024761c432e8ebbd2d6e5b30fe0e79e19de

[8] SHA-256: 968ec5e0c4aa7e15f0a04c5e7f96393aa7cbf12d2125dfe7dd20351408dd0615

[9] SHA-256: 60521e103bb134aea3169da6d3dfdcdae8e4d5e82df265a377b648bae39aca5f

Source: https://teamt5.org/tw/posts/alert-exploitation-of-cve-2026-34197-in-apache-active-mq?utm_source=rss&tm_medium=rss