FORTINET

# OUTBREAK ALERTS

## Apache ActiveMQ Ransomware Attack

### Ransomware attackers actively targeting Apache ActiveMQ flaw

https://activemq.apache.org/news/cve-2023-46604

CVEs: CVE-2023-46604

Ransomware attackers are targeting servers running outdated and vulnerable versions of Apache ActiveMQ by exploiting a recently fixed vulnerability (CVE-2023-46604).

**Background**

Apache ActiveMQ is a popular open source message broker – a program that translates a messages from one messaging protocol to another, allowing communication between diverse services and systems. ActiveMQ supports a variety of protocols, including OpenWire, MQTT (messaging protocol for IoT), AMQP (protocol for business messaging and IoT device management), REST, STOMP, etc.

This vulnerability CVE2023-46604, may allow a remote attacker with network access to a broker to run arbitrary shell commands by manipulating serialized class types in the OpenWire protocol. Technical details and proof-of-concept (PoC) code for CVE-2023-46604 are publicly available and could be leveraged by other threat groups looking to exploit the vulnerability.

As of 6th Oct, 2023, according to shadow server there are more than 3000+ servers accessible for the internet which are vulnerable to CVE-2023-46604.
https://dashboard.shadowserver.org/statistics/combined/time-series/?date_range=7&source=activemq&tag=cve-2023-46604&style=stacked

**Announced**

Oct, 2023: Apache released an advisory:
https://activemq.apache.org/security-advisories.data/CVE-2023-46604-announcement.txt

Oct 25, 2023: Apache released the patch fix for CVE-2023-46604
https://activemq.apache.org/components/classic/download/

Nov 02, 2023: CISA added CVE-2023-46604 to its known exploited list, KEV Catalog.

**Latest Developments**

FortiGuard Labs recommends applying available patches for Apache ActiveMQ as soon as possible if not already done. Apache also has information on improving the security of ActiveMQ implementations.
https://activemq.apache.org/security

# PROTECT

**Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:**

## Reconnaissance

### Lure

FortiDeceptor
v3.3+

### Decoy VM

FortiDeceptor
v3.3+

## Weaponization

## Delivery

### AV

**Detects and blocks malware related to Apache ActiveMQ Ransomware Attack**

FortiGate *DB 91.08565*
FortiClient *DB 91.08565*
FortiSASE *DB 91.08565*
FortiMail *DB 91.08565*
FortiCASB *DB 91.08565*
FortiCWP *DB 91.08565*
FortiADC *DB 91.08565*
FortiProxy *DB 91.08565*

### Vulnerability

**Detects and blocks attack targeting Apache ActiveMQ servers (CVE-2023-46604)**

FortiClient *DB 1.569*

### AV (Pre-filter)

**Detects and blocks malware related to Apache ActiveMQ Ransomware Attack**

FortiEDR *DB 91.08565*
FortiSandbox *DB 91.08565*
FortiNDR *DB 91.08565*

### Behavior Detection

**Behavior Destection Engine detects HelloKitty ransomware malware as "High risk" and blocks other 0-day threats**

FortiSandbox
v5.0+

## Exploitation

### IPS

**Detects and blocks attack targeting Apache ActiveMQ servers (CVE-2023-46604)**

FortiGate *DB 26.673*
FortiSASE *DB 26.673*
FortiNDR *DB 26.673*
FortiADC *DB 26.673*
FortiProxy *DB 26.673*

## Installation

## C2

## Action

# DETECT

**Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:**

### Outbreak Detection

FortiClient *DB 1.00016*
FortiAnalyzer *DB 2.00025*
FortiSIEM *DB 601*

### Threat Hunting

FortiEDR

### IOC

FortiAnalyzer
FortiSIEM
FortiSOCaaS

# RESPOND

**Develop containment techniques to mitigate impacts of security events:**

### Automated Response

**Services that can automaticlly respond to this outbreak.**

FortiXDR

### Assisted Response Services

**Experts to assist you with analysis, containment and response activities.**

Incident Response
FortiRecon: ACI

# RECOVER

**Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:**

### NOC/SOC Training

**Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.**

NSE Training
Response Readiness

### End-User Training

**Raise security awareness to your employees that are continuously being targetted by phishing, drive-by download and other forms of cyberattacks.**

Security Awareness & Training

# IDENTIFY

**Identify processes and assets that need protection:**

### Attack Surface Hardening

**Check Security Fabric devices to build actionable configuration recommendations and key indicators.**

Security Rating

### Vulnerability Management

**Reduce the attack surface on software vulnerabilities via systematic and automated patching.**

FortiClient

### Business Reputation

**Know attackers next move to protect against your business branding.**

FortiRecon: EASM

## Additional Resources

| | |
|---|---|
| **FortiGuard Threat Signal** | https://www.fortiguard.com/threat-signal-report/5307/ |
| **Helpnet Security** | https://www.helpnetsecurity.com/2023/11/02/cve-2023-46604-ransomware/ |
| **The Hacker News** | https://thehackernews.com/2023/11/hellokitty-ransomware-group-exploiting.html |
| **Security Week** | https://www.securityweek.com/critical-apache-activemq-vulnerability-exploited-to-deliver-ransomware/ |
| **Shadow Server Report** | https://www.shadowserver.org/what-we-do/network-reporting/accessible-activemq-service-report/ |
| **Bleeping Computer** | https://www.bleepingcomputer.com/news/security/lethuvirtheseass-ransomware-joins-apache-activemq-rce-attacks/#google_vignette |

Learn more about FortiGuard Outbreak Alerts