

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## **Ransomware Threats Exploit CVE-2023-46604 in Apache ActiveMQ Servers**

Date of Publication

November 3, 2023

Last updated date

November 7, 2023

Admiralty Code

A1

TA Number

TA2023444

# Summary




**First Seen:** October 25, 2023

**Affected Platform:** Apache ActiveMQ

**Malware:** HelloKitty ransomware, TellYouThePass ransomware, SparkRAT

**Impact:** Ransomware groups and SparkRAT exploiting a critical vulnerability (CVE-2023-46604) in Apache ActiveMQ, despite a security update on October 27, 2023, affecting systems with outdated ActiveMQ versions. Promptly updating ActiveMQ versions is crucial to mitigate this vulnerability.

## CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-46604	Apache ActiveMQ Deserialization of Untrusted Data Vulnerability	Apache ActiveMQ			

# Vulnerability Details

## #1

CVE-2023-46604 is a remote code execution (RCE) vulnerability in Apache ActiveMQ, a widely-used open-source multi-protocol message broker. It was disclosed on October 25, 2023, and has been exploited in the wild by ransomware operators, also deploying SparkRAT malware.

## #2

This particular CVE allows a remote attacker to execute arbitrary shell commands by manipulating serialized class types in the OpenWire protocol. Although Apache released security updates on October 27 to address this vulnerability, more than 9,200 ActiveMQ servers are exposed online, with over 4,770 vulnerable to CVE-2023-46604 exploits. Proof-of-concept exploit code is publicly available.

## #3

The attackers took advantage of the vulnerability to execute arbitrary commands, leading to the deployment of ransomware on the targeted systems. However, the attempts to encrypt files were not entirely successful, resulting in several failed encryption efforts.

## #4

HelloKitty ransomware binaries analyzed contained a 32-bit .NET executable named dllloader, which, upon decoding a Base64 payload, revealed a DLL named EncDLL. This DLL displayed typical ransomware behavior, such as searching for processes to stop, encrypting specific file types, appending ".locked" to encrypted files, and attempting communication with an HTTP server. The ransom note directed communication through the email address [service@hellokittycat\[.\]online](mailto:service@hellokittycat[.]online).

## #5

TellYouThePass ransomware has experienced increased activity after Log4Shell proof-of-concept exploits were published online two years ago and has recently resurfaced as a Golang-compiled malware, expanding its cross-platform capabilities to target Linux and potentially macOS systems. Threat actors had also been exploiting this vulnerability for over two weeks, deploying SparkRAT malware.

## #6

These incidents underscore the importance of promptly updating Apache ActiveMQ to patched versions, as exploitation of this vulnerability led to attempted ransomware deployment in both cases.

## Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-46604	Apache ActiveMQ 5.18.0 before 5.18.3, Apache ActiveMQ 5.17.0 before 5.17.6, Apache ActiveMQ 5.16.0 before 5.16.7, Apache ActiveMQ before 5.15.16, Apache ActiveMQ Legacy OpenWire Module 5.18.0 before 5.18.3, Apache ActiveMQ Legacy OpenWire Module 5.17.0 before 5.17.6, Apache ActiveMQ Legacy OpenWire Module 5.16.0 before 5.16.7, Apache ActiveMQ Legacy OpenWire Module 5.8.0 before 5.15.16	cpe:2.3:a:apache:activemq:*:*:*:*:* .* cpe:2.3:a:apache:activemq_legacy_openwire_module:*:*:*:*	CWE-502

# Recommendations



**Patch and Update Immediately:** Ensure all systems running Apache ActiveMQ are updated to the latest patched versions (5.18.3, 5.17.6, 5.16.7, or 5.15.16 as appropriate) to address the CVE-2023-46604 vulnerability. Regularly check for updates and security patches for all software and applications.



**Network Segmentation and Access Controls:** Implement proper network segmentation and access controls to limit the exposure of critical systems. Employ firewalls, VLANs, and access control lists to restrict unnecessary access to Apache ActiveMQ servers from untrusted networks.



**Conduct Regular Data Backups:** Implement a robust data backup strategy that includes regular backups of critical data and systems, ad hoc and periodic backup restoration test. In the event of a ransomware attack, having up-to-date backups will allow organizations to restore their systems and data without paying the ransom. Ensure backups are adequately protected, employ 3-2-1-1 back up principle and Deploy specialized tools to ensure backup protection.



**Vulnerability Scanning and Assessment:** Conduct regular vulnerability scans and assessments of your IT infrastructure. Identify and address any vulnerabilities promptly to reduce the attack surface.

## Potential MITRE ATT&CK TTPs

<b><u>TA0005</u></b> Defense Evasion	<b><u>TA0042</u></b> Resource Development	<b><u>TA0011</u></b> Command and Control	<b><u>TA0002</u></b> Execution
<b><u>TA0040</u></b> Impact	<b><u>T1574.001</u></b> DLL Search Order Hijacking	<b><u>T1574</u></b> Hijack Execution Flow	<b><u>T1132</u></b> Data Encoding
<b><u>T1071.001</u></b> Web Protocols	<b><u>T1036</u></b> Masquerading	<b><u>T1486</u></b> Data Encrypted for Impact	<b><u>T1059</u></b> Command and Scripting Interpreter
<b><u>T1218.007</u></b> Msiexec	<b><u>T1588.006</u></b> Vulnerabilities	<b><u>T1588.005</u></b> Exploits	<b><u>T1588</u></b> Obtain Capabilities
<b><u>T1036</u></b> Masquerading	<b><u>T1132.001</u></b> Standard Encoding	<b><u>T1071</u></b> Application Layer Protocol	<b><u>T1203</u></b> Exploitation for Client Execution
<b><u>T1218</u></b> System Binary Proxy Execution	<b><u>T1027</u></b> Obfuscated Files or Information		

## 🔪 Indicators of Compromise (IOCs)

TYPE	VALUE
<b>Email</b>	service@hellokittycat[.]online
<b>URLs</b>	hxxp://172.245.16[.]125/m4.png, hxxp://172.245.16[.]125/m2.png
<b>MD5</b>	e19e1601b92f456dcbc21b7024237d60
<b>SHA256</b>	d065d44d0412aef867f66626b5c4a3d7d0a3bdb59c61712b0c71efbf9865a7a6, 7af5c37cc308a222f910d6a7b0759837f37e3270e22ce242a8b59ed4d7ec7ceb, 5c8710638fad8eeac382b0323461892a3e1a8865da3625403769a4378622077e, dd13cf13c1fbdc76da63e76adcf36727cfe594e60af0dc823c5a509a13ae1e15, 4c9fa87e72fe59cf15131bd2f3bd7baa7a9555ceec438c1df78dd5d5b8394910, 43c8eea4bab853cda8a5ca8e9eb1a9d68ac38b32c8fee3583df33d2dfcef42ac, 6cdc10000d9291291c7ce0c63438796614bd21ec7e327c7f48c4ddd16ccf036f, c3c0cf25d682e981c7ce1cc0a00fa2b8b46cce2fa49abe38bb412da21da99cb7, 8c226e1f640b570a4a542078a7db59bb1f1a55cf143782d93514e3bd86dc07a0, 8177455ab89cc96f0c26bc42907da1a4f0b21fdc96a0cc96650843fd616551f4
<b>Domains</b>	mail4[.]amazuorn[.]com, hellokittycat[.]online, hellowinter[.]online
<b>Bitcoin Wallet Address</b>	bc1ql8an5slxutu3yjyu9rvhsfcpv29tsfhv3j9lr4
<b>IPv4:PORT</b>	172.245.16[.]125:80, 4.216.93[.]211:5981, 27.102.128[.]152:8098

TYPE	VALUE
IPv4	137.175.17[.]172, 45.32.120[.]181, 172.245.16[.]125, 4.216.93[.]211, 38.6.160[.]44, 23.94.248[.]134, 23.225.116[.]3, 193.187.172[.]73

## Patch Details

<https://activemq.apache.org/security-advisories.data/CVE-2023-46604>

## References

<https://www.rapid7.com/blog/post/2023/11/01/etr-suspected-exploitation-of-apache-activemq-cve-2023-46604/>

<https://www.shadowserver.org/what-we-do/network-reporting/accessible-activemq-service-report/>

<https://www.hivepro.com/hellokitty-is-launching-a-ddos-attack-by-exploiting-known-vulnerabilities/>

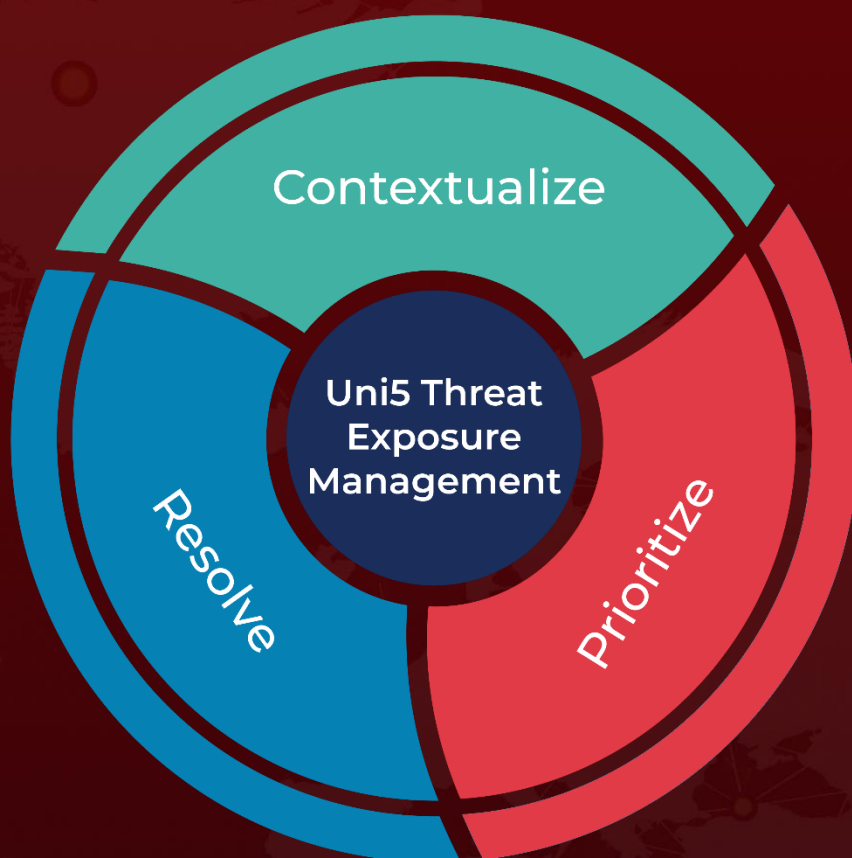
<https://arcticwolf.com/resources/blog/tellmethetruth-exploitation-of-cve-2023-46604-leading-to-ransomware/>

<https://www.huntress.com/blog/critical-vulnerability-exploitation-of-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

**November 3, 2023 • 5:30 AM**

© 2023 All Rights are Reserved by Hive Pro<sup>®</sup>



More at [www.hivepro.com](http://www.hivepro.com)