Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

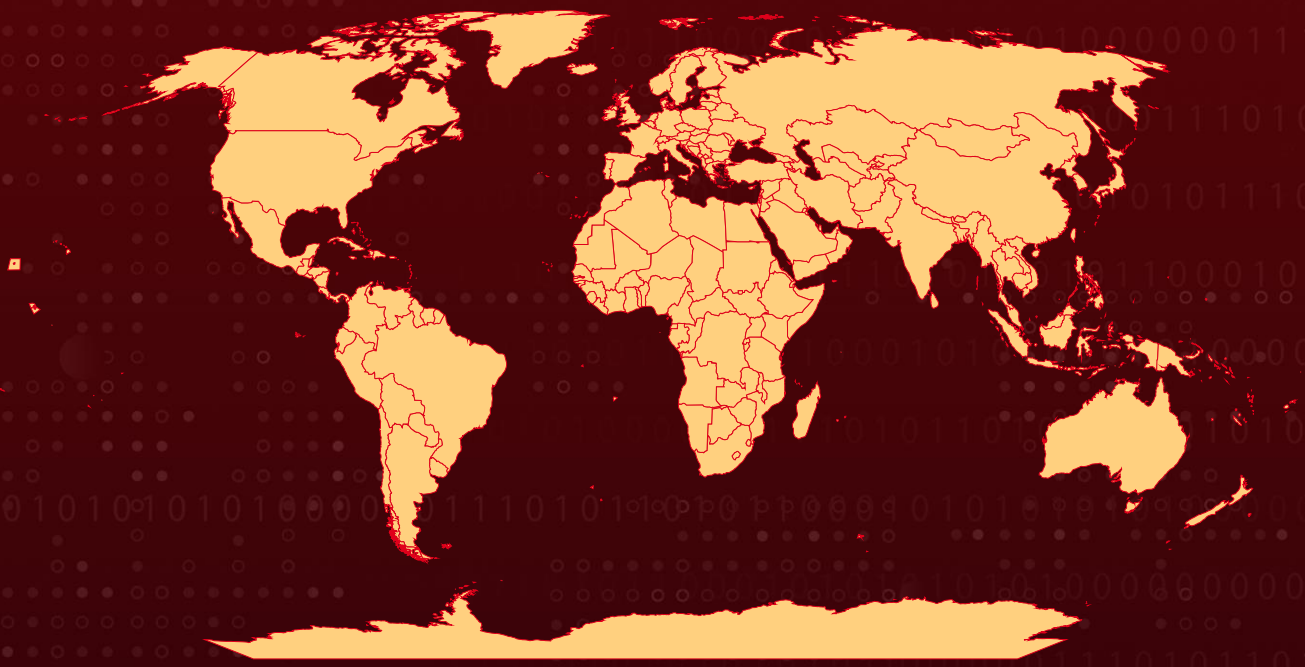
Persistent Attacks Exploiting Apache ActiveMQ CVE-2023-46604

Date of Publication	Admiralty Code	TA Number
December 11, 2024	A1	TA2024458

Summary

Attack Began: December 2024
Malware: Mauri ransomware, Quasar RAT
Targeted Countries: Worldwide
Affected Products: Apache ActiveMQ
Attack: Threat actors exploiting CVE-2023-46604 in Apache ActiveMQ are gaining remote code execution to install backdoors, Quasar RAT, and proxy tools, potentially deploying Mauri ransomware. This multi-phase attack compromises systems and encrypts data. Immediate patching of vulnerable systems and proactive security measures are critical to mitigate the threat.

Attack Regions



CVE

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

Attack Details

#1

Threat actors are actively exploiting the CVE-2023-46604 vulnerability in Apache ActiveMQ servers, enabling remote code execution. This flaw has been frequently targeted, particularly in Korea, to deploy malware such as CoinMiners and ransomware variants like Mauri. The attackers leverage this vulnerability to gain persistent access and compromise systems, leading to potential data loss and encryption.

#2

CVE-2023-46604 is a critical vulnerability that allows attackers to execute malicious commands on unpatched Apache ActiveMQ servers. The exploitation occurs through manipulation of serialized class types in the OpenWire protocol, enabling attackers to load malicious XML configuration files from external URLs. Previously, this vulnerability has been exploited by HelloKitty ransomware, TellYouThePass ransomware, and SparkRAT. Systems left unpatched after its disclosure remain at significant risk.

#3

Attackers are targeting systems with vulnerable versions of Apache ActiveMQ. Logs indicate ongoing attempts to install CoinMiners and other malware. The Mauri ransomware has also been linked to these attacks, utilizing the vulnerability to install additional tools like Frpc, which facilitates remote access through reverse proxying.

#4

Once access is gained, attackers may execute commands to create backdoor accounts and install various malware types, including Quasar RAT. This allows them to maintain control over the infected systems and potentially exfiltrate sensitive data.

#5

Commands executed during these attacks often include creating hidden user accounts with administrative privileges, enabling Remote Desktop Protocol (RDP) access for further exploitation. The use of tools like CreateHiddenAccount suggests a sophisticated level of planning by the attackers.

Recommendations

Patch and Update Software: Ensure all systems running Apache ActiveMQ are updated to the latest versions, which address this critical vulnerability.

Disable OpenWire Protocol (if feasible): If upgrading is not immediately possible, consider disabling the OpenWire protocol temporarily. While this may restrict some functionalities, it can help limit exposure to attacks until a proper upgrade can be performed.

Implement Robust Endpoint Protection: Deploy advanced endpoint protection solutions that include behavior-based detection, machine learning algorithms, and threat intelligence. These solutions can detect and block malicious activities associated with Mauri ransomware, such as file encryption and unauthorized processes. Regularly update endpoint security software to ensure protection against the latest threats.

Conduct Regular Data Backups and Test Restoration: Regularly backup critical data and systems, store them securely offline. Test restoration processes to ensure backup integrity and availability. In case of a Mauri ransomware attack, up-to-date backups enable recovery without paying the ransom.

Access Control and Least Privilege: Enforce the principle of least privilege, ensuring that users and applications have only the minimum access required to perform their functions. This limits the potential impact of a ransomware attack.

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	TA0042 Resource Development	TA0004 Privilege Escalation	TA0002 Execution
TA0007 Discovery	TA0010 Exfiltration	TA0009 Collection	TA0011 Command and Control
TA0003 Persistence	TA0040 Impact	T1486 Data Encrypted for Impact	T1087 Account Discovery
T1021.001 Remote Desktop Protocol	T1021 Remote Services	T1490 Inhibit System Recovery	T1070 Indicator Removal

T1027 Obfuscated Files or Information	T1059.001 PowerShell	T1090 Proxy	T1068 Exploitation for Privilege Escalation
T1041 Exfiltration Over C2 Channel	T1059 Command and Scripting Interpreter	T1588.006 Vulnerabilities	T1588 Obtain Capabilities
T1056.001 Keylogging	T1056 Input Capture		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	07894bc946bd742cec694562e730bac8, 25b1c94cf09076eb8ce590ee2f7f108e, 2c93a213f08a9f31af0c7fc4566a0e56, 2e8a3baeaa0fc85ed787a3c7dfd462e7, 3b56e1881d8708c48150978da14da91e
IPv4	18[.]139[.]156[.]111
URLs	hxxp[:]//18[.]139[.]156[.]111[:]83/Google[.]zip, hxxp[:]//18[.]139[.]156[.]111[:]83/a[.]exe, hxxp[:]//18[.]139[.]156[.]111[:]83/brave[.]exe, hxxp[:]//18[.]139[.]156[.]111[:]83/c[.]ini, hxxp[:]//18[.]139[.]156[.]111[:]83/chrome[.]exe

Patch Link

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

References

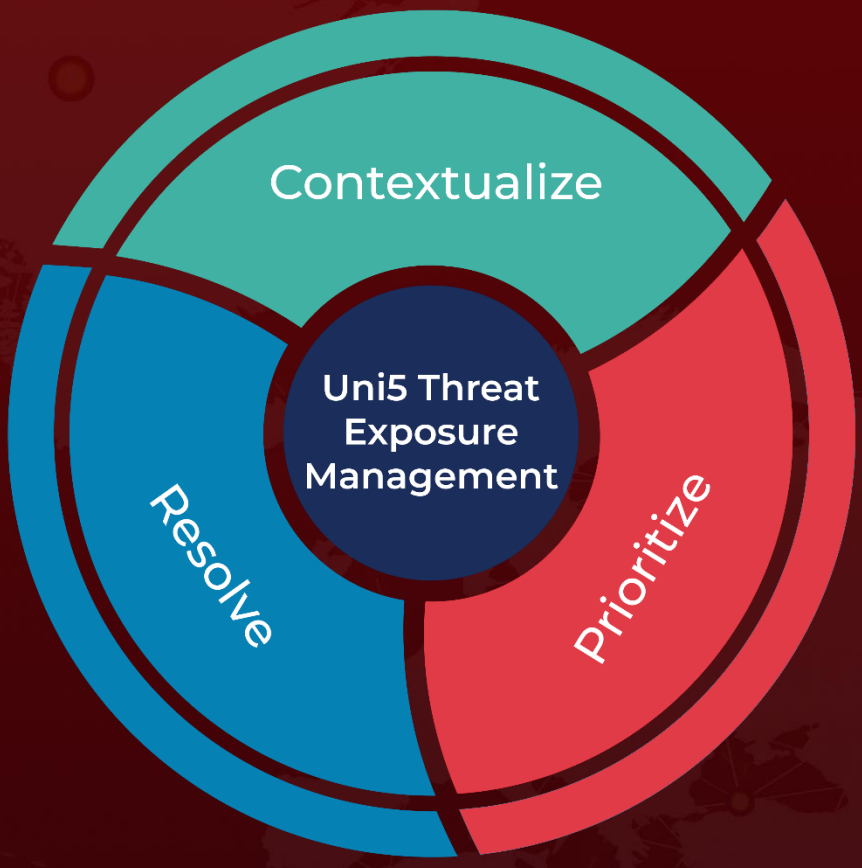
https://asec.ahnlab.com/en/85000/

https://www.hivepro.com/hellokitty-ransomware-exploited-apache-activemq-rce-vulnerability/

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

Decmber 11, 2024 . 03:00 AM

More at www.hivepro.com