Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

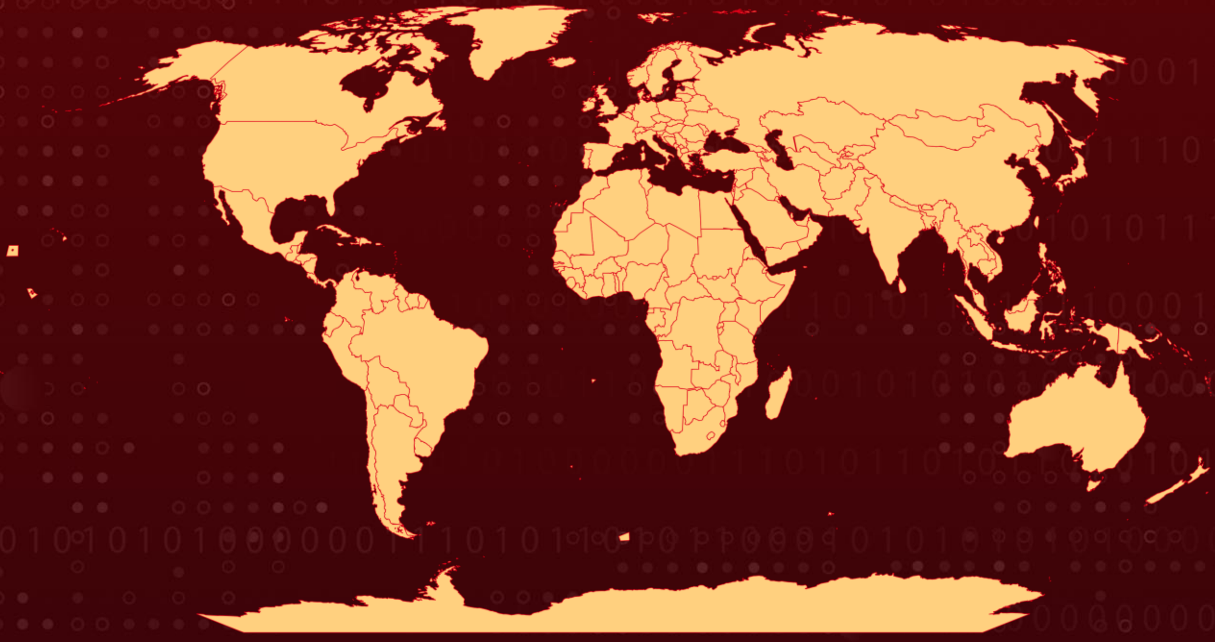
Kinsing Malware Utilizes Apache ActiveMQ RCE to Deploy Rootkits

Date of Publication	Admiralty Code	TA Number
November 21, 2023	A1	TA2023468

Summary

Attack Discovered: Early November 2023
Attack Region: Worldwide
Malware: Kinsing (aka h2miner)
Attack: The Kinsing malware operator is actively taking advantage of the critical vulnerability CVE-2023-46604 in Apache ActiveMQ, an open-source message broker. The vulnerability allows remote code execution, facilitating deployment of Kinsing malware (aka h2miner), which functions as a cryptocurrency miner.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

CVEs

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

Attack Details

#1 The Apache ActiveMQ vulnerability CVE-2023-46604 is actively being exploited, leading to the download and infection of Linux systems with the Kinsing malware(aka h2miner), which operates as a cryptocurrency miner. The vulnerability, allowing remote code execution, stems from the ability to run arbitrary shell commands by exploiting serialized class types in the OpenWire protocol.

#2 The Kinsing malware particularly targets Linux-based systems. Its infiltration of servers and rapid spread across networks are facilitated by exploiting vulnerabilities in web applications or taking advantage of misconfigured container environments. Notably, the malware utilizes the 'ProcessBuilder' method to execute malicious bash scripts, enabling the downloading of additional payloads onto the infected device through the creation of new system-level processes.

#3 Kinsing malware not only functions as a cryptocurrency miner but also takes aggressive measures against competing miners. It terminates their processes, connections, and crontab entries on the infected host. Simultaneously, it establishes its own persistence mechanism by adding a cronjob that fetches and executes its malicious bootstrap script every minute. Furthermore, the inclusion of a rootkit in /etc/ld.so.preload ensures a comprehensive compromise of the entire system, making it challenging to detect and remove.

#4 The increasing exploitation of CVE-2023-46604 poses a significant risk to organizations across various sectors. It emphasizes the critical importance of promptly patching vulnerabilities and actively monitoring for any signs of compromise.

Recommendations

Apply Patch: Install the security patch provided by Apache to address the CVE-2023-46604 vulnerability. This patch closes the security gap that allows attackers to exploit the vulnerability.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Network Segmentation: Implement proper network segmentation to limit the lateral movement of malware within the network. By dividing the network into smaller, isolated segments, organizations can contain the spread of malware and prevent it from accessing critical systems and sensitive data.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0002** Execution	**TA0005** Defense Evasion	**TA0008** Lateral Movement
TA0011 Command and Control	**TA0040** Impact	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities
T1588.005 Exploits	**T1105** Ingress Tool Transfer	**T1014** Rootkit	**T1496** Resource Hijacking
T1210 Exploitation of Remote Services	**T1059** Command and Scripting Interpreter		

Indicators of Compromise (IOCs)

TYPE	VALUE
URL	hxxp[://]185[.]122[.]204[.]197/acb[.]sh, hxxp[://]194[.]38[.]22[.]53/curl-aarch64, hxxp[://]194[.]38[.]22[.]53/curl-amd64, hxxp[://]194[.]38[.]22[.]53/kinsing, hxxp[://]194[.]38[.]22[.]53/kinsing_aarch64, hxxp[://]194[.]38[.]22[.]53/libsystem[.]so

TYPE	VALUE
SHA256	d8f55bbbcc20e81e46b9bf78f93b73f002c76a8fcdb4dc2ae21b8609445c14f9, 0cc60a0c480e4d898fa77ab501bbd2afaf3f5fb89a2917a31e7f5fdaa6c3879c, 787e2c94e6d9ce5ec01f5cbe9ee2518431eca8523155526d6dc85934c9c5787c, c6fbd6896d162a12d9c900056781eb82f44649945808b7b009646b5397bcf6bf, c38c21120d8c17688f9aeb2af5bdafb6b75e1d2673b025b720e50232f888808a

Patch Link

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

References

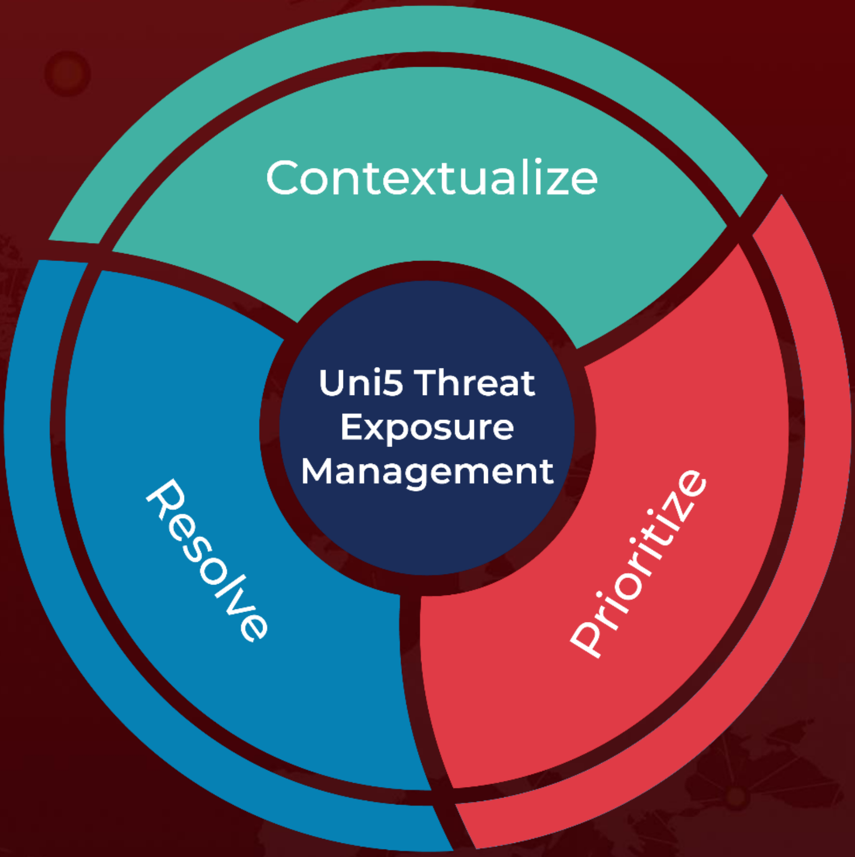
https://www.trendmicro.com/en_us/research/23/k/cve-2023-46604-exploited-by-kinsing.html

https://www.hivepro.com/threat-advisory/ransomware-threats-exploit-cve-2023-46604-in-apache-activemq-servers/

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 21, 2023 • 3:40 AM

More at www.hivepro.com