

HiveForce Labs

THREAT ADVISORY

**ACTOR REPORT**

Kinsing Exploits Looney Tunables Vulnerability to Breach Cloud Environments

Date of Publication

November 06, 2023

Admiralty code

A1

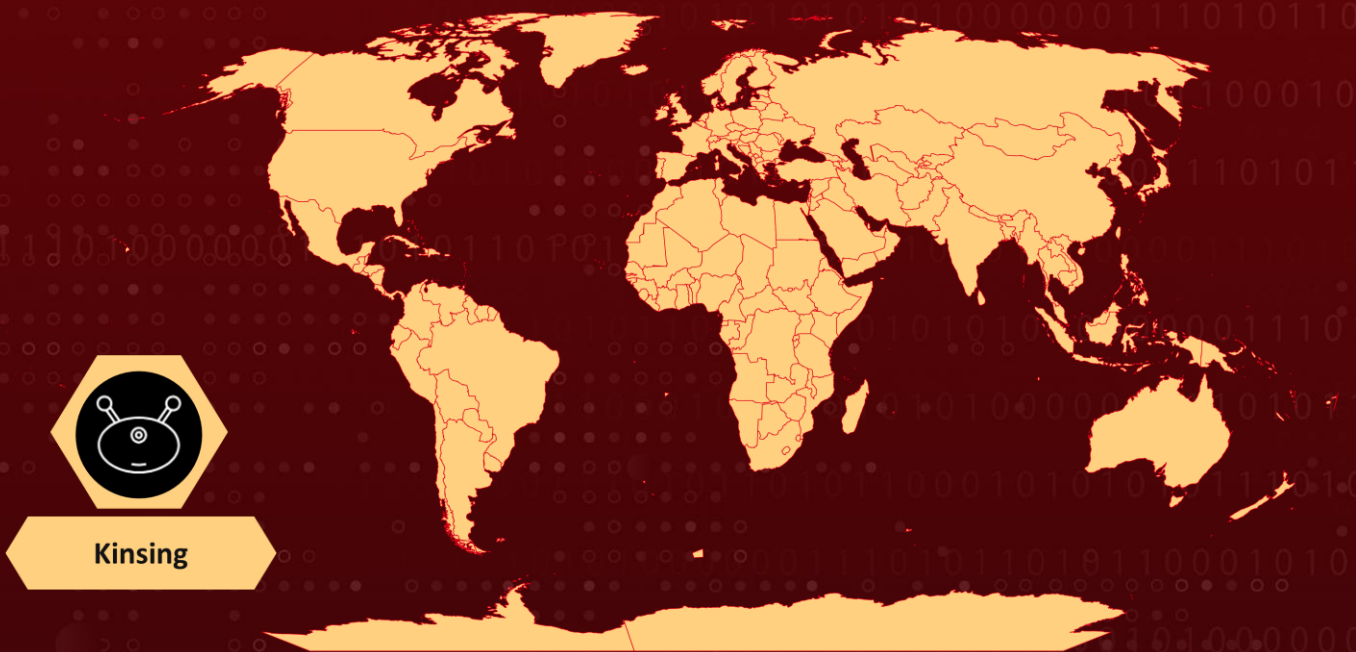
TA Number

TA2023447

Summary







Attack Began: November 2023
Actor Name: Kinsing (aka Money Libra)
Target Industries: Cryptocurrency
Target Region: Worldwide

Actor Map



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

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-4911	Glibc Buffer Overflow Vulnerability	GNU C Library (glibc)			
CVE-2017-9841	PHPUnit Command Injection Vulnerability	Oracle Communications Diameter Signaling Router			

Actor Details

#1

The Kinsing threat actor, emerged in the first quarter of 2022, poses a substantial threat to cloud-native environments and were spotted targeting Kubernetes clusters, Docker APIs, Redis servers, Jenkins servers. They have engaged in attacking containerized setups capitalizing on newly discovered vulnerabilities and improperly configured open Docker daemon API ports to install cryptominers.

#2

The Kinsing threat actor has been using rootkits to conceal their presence on compromised systems. Additionally, they actively terminate and uninstall resource-intensive services and processes to optimize their cryptocurrency mining operations. They have also been observed scanning for open default WebLogic ports to execute shell commands and deploy malware. Previously the threat actor has been observed exploiting vulnerable Openfire servers to achieve remote code execution.

#3

In a recent campaign, the Kinsing threat actor was observed attempting to exploit the recently disclosed Linux privilege escalation vulnerability known as Looney Tunables [CVE-2023-4911](#). This vulnerability allows unauthorized users to escalate their privileges on Linux systems.

#4

The initial access in this Kinsing campaign was achieved through the exploitation of the PHPUnit vulnerability (CVE-2017-9841). Subsequently, Kinsing downloaded and executed a Perl script named bc.pl, which opened a reverse shell on port 1337. Following this, the threat actors manually scanned the victim's environment for the presence of the Linux privilege escalation vulnerability "Looney Tunables" using a Python-based exploit.

#5

The attacker uses the de-obfuscated exploit to reveal a JavaScript script, which acts as a web shell allowing them backdoor access to the server. They perform file management, command execution, and gather information. The ultimate goal is to extract cloud service provider credentials, a shift from their previous tactics.

#6

The Kinsing threat actor has recently changed their approach, which raises the possibility that their operational reach will grow. This suggests that the Kinsing operation might expand its scope and level of aggression, posing a greater risk to cloud-native environments.

NAME	ORIGIN	TARGET REGIONS	TARGETED INDUSTRIES
Kinsing (aka Money Libra)	-	Worldwide	Cryptocurrency
	MOTIVE		
	Information Theft		

Recommendations



Apply Patch: Install the security patch to address the known PHPUnit vulnerability (CVE-2017-9841) and Looney Tunables (CVE-2023-4911). These patches close the security gap that allows attackers to exploit the vulnerability.



Behavioral Anomaly Detection: Deploy advanced behavioral anomaly detection systems that can identify deviations from normal user and system behavior, flagging activities such as unusual execution of commands or tools, attempts to access or enumerate CSP credentials, and the execution of known malicious scripts.



Implement Cloud-Native Detection and Response (CNDR): It will provide real-time monitoring and detection of malicious activities within cloud environments. These solutions work by continuously analyzing the behavior of running containers and applications. They can detect and respond to anomalies that might indicate a compromise, including actions like manual command executions and lateral movements that are often associated with Kinsing attacks.

Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>TA0003</u> Persistence
<u>TA0004</u> Privilege Escalation	<u>TA0005</u> Defense Evasion	<u>TA0006</u> Credential Access	<u>TA0007</u> Discovery
<u>TA0040</u> Impact	<u>T1059</u> Command and Scripting Interpreter	<u>T1059.006</u> Python	<u>T1059.007</u> JavaScript
<u>T1505</u> Server Software Component	<u>T1068</u> Exploitation for Privilege Escalation	<u>T1190</u> Exploit Public-Facing Application	<u>T1588</u> Obtain Capabilities
<u>T1588.006</u> Vulnerabilities	<u>T1027</u> Obfuscated Files or Information	<u>T1003</u> OS Credential Dumping	<u>T1082</u> System Information Discovery
<u>T1083</u> File and Directory Discovery	<u>T1140</u> Deobfuscate/Decode Files or Information	<u>T1496</u> Resource Hijacking	

Indicator of Compromise (IOCs)

TYPE	VALUE
IP	194.233.65[.].92
Domain	haxx.in
MD5	ea685e738adedc02ca1a63ebe8ed939e, 9a868bb2456bcde27cde7985145ef6fc, 5dce322f5284213912012e7ba2440da0, 5d3c00b79be956d4175d0d5fd1d4f1f9

Patch Details

For addressing the CVE-2023-4911, upgrade the glibc to 2.38 or later versions.

Apply the patches available to address the CVE-2017-9841.

Link: <https://www.oracle.com/security-alerts/cpuoct2021.html>

References

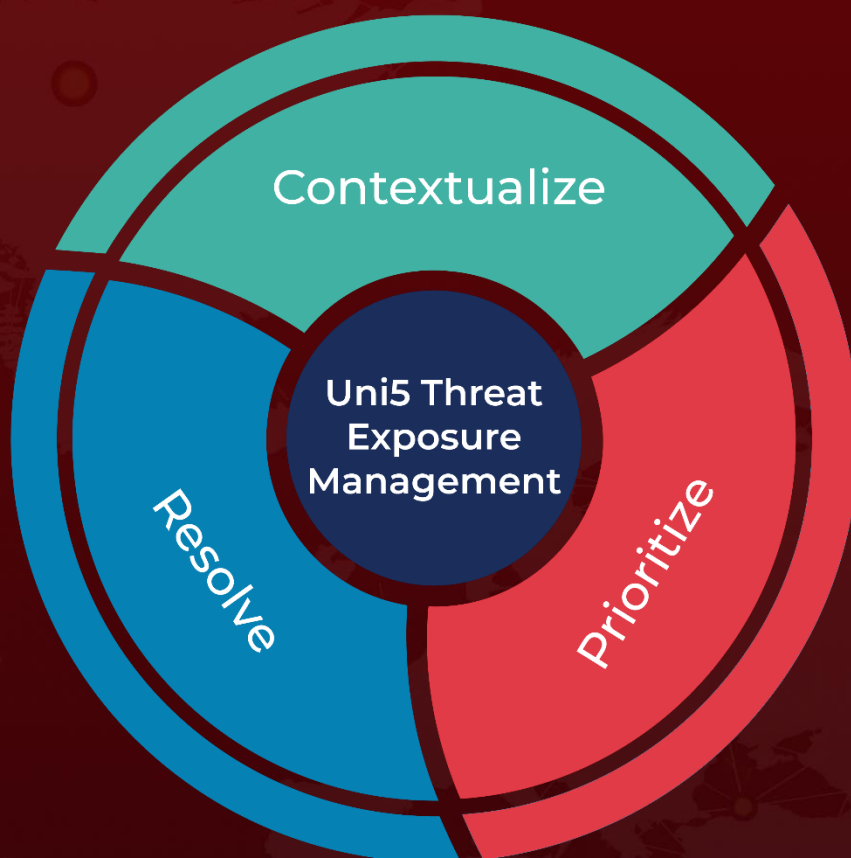
<https://blog.aquasec.com/loony-tunables-vulnerability-exploited-by-kinsing>

<https://www.hivepro.com/looney-tunables-flaw-enables-local-privilege-escalation-in-glibc/>

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 06, 2023 • 4:25 AM

© 2023 All Rights are Reserved by Hive Pro®



More at www.hivepro.com