



THREAT ADVISORY

**ATTACK
REPORT**

Kinsing malware continues to exploit these
two-year-old vulnerabilities

Date of Publication

September 21, 2022

Admiralty Code

A1



TA Number

TA2022208

Summary

Malicious actors are exploiting these two-year-old remote code execution vulnerabilities in Oracle WebLogic Server to deploy Kinsing malware.

CVEs Table

CVE	NAME	PATCH
CVE-2020-14882	Code Injection Vulnerability	
CVE-2020-14883	Improper input validation Vulnerability	

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	T1190 Exploit Public-Facing Application	TA0002 Execution	T1059 Command and Scripting Interpreter
T1059.004 Unix Shell	T1053 Scheduled Task/Job	T1053.003 Cron	TA0040 Impact
T1496 Resource Hijacking	TA0005 Defense Evasion	T1070 Indicator Removal on Host	T1070.002 Clear Linux or Mac System Logs
T1070.004 File Deletion	T1222 File and Directory Permissions Modification	T1222.002 Linux and Mac File and Directory Permissions Modification	T1562 Impair Defenses
T1562.004 Disable or Modify System Firewall	T1562.008 Disable Cloud Logs		

Technical Details

#1

The infection chain begins with the attacker running scripts to exploit vulnerabilities(CVE-2020-14882, CVE-2020-14883) on vulnerable versions of the Oracle WebLogic Server. Successful exploitation of these vulnerabilities leads to the download of the wb.sh file into the host machine.

#2

Upon execution, the script adds a cron job for persistence and disables the firewall. After checking the user's root status, it would select the path and utility (wget and curl) to download the malicious binary.

#3

Once these steps are completed, the attacker installs Kinsing malware, which is responsible for cryptomining and sending data to the attacker's C2 channel.

✂ Indicator of Compromise (IOC)

TYPE	VALUE
SHA256	020c14b7bf5ff410ea12226f9ca070540bd46eff80cf20416871143464f7d546 5d2530b809fd069f97b30a5938d471dd2145341b5793a70656aad6045445cf6d
IPV4	212[.]22[.]77[.]79 185[.]234[.]247[.]8 185[.]154[.]53[.]140
URLs	hxxp://91[.]241[.]19[.]134/wb.sh hxxp://185[.]14[.]30[.]35/kinsing hxxp://185[.]14[.]30[.]35/wb.sh hxxp://195[.]2[.]79[.]26/kinsing hxxp://195[.]2[.]79[.]26/wb.sh hxxp://195[.]2[.]78[.]230/wb.sh hxxp://193[.]178[.]170[.]47/wb.sh hxxp://178[.]20[.]40[.]200/wb.sh hxxp://94[.]103[.]89[.]159/wb.sh hxxp://185[.]231[.]153[.]4/wb.sh hxxp://195[.]2[.]85[.]171/wb.sh hxxp://80[.]92[.]204[.]82/wb.sh hxxp://195[.]2[.]84[.]209/kinsing hxxp://193[.]178[.]170[.]47/kinsing hxxp://178[.]20[.]40[.]200/kinsing

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2020-14882	Oracle WebLogic Server: 10.3.6.0.0 - 14.1.1.0.0	cpe:2.3:a:oracle:oracle_ weblogic_server:*:*:*:* .*:*:*.*	CWE-94
CVE-2020-14883			CWE-20

Patch Link

<https://www.oracle.com/security-alerts/cpuoct2020.html>

References

https://www.trendmicro.com/en_us/research/22/i/a-post-exploitation-look-at-coinminers-abusing-weblogic-vulnerab.html

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Continuous Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.



At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

September 21, 2022 • 4:00 AM

© 2022 All Rights are Reserved by HivePro



More at www.hivepro.com