Hive Pro

THREAT ADVISORY

Muhstik botnet adds another vulnerability exploit to its arsenal

TA2022079

Threat Level RED

Publish Date – Mar 29, 2022

Muhstik malware has begun attacking Redis Servers by exploiting a recently reported vulnerability, CVE-2022-0543. This flaw can be found in several Redis Debian packages. The attack began on March 11, 2022 and was carried out by threat actor who targeted Confluence servers in September 2021 and Log4j in December. The payload is a Muhstik bot variation that may be used to perform DDOS assaults.

The threat actor first executes the Lua scripts to exploit the vulnerability found in Redis Debian servers. The threat actor attempts to download "russia.sh" from "106[.]246.224.219" using wget or curl. It stores it as "/tmp/russ" and runs it which will download and run Linux payload from 160[.]16.58.163. These binaries have been recognized as Muhstik bot variants. This botnet then connects to an IRC server to receive commands that download files, run shell commands, and carry out attacks like flood attacks and SSH brute force attacks.

The Mitre TTPs commonly used by Muhstik malware are:
TA0001: Initial Access
TA0011: Command and Control
TA0042: Resource Development
TA0008: Lateral Movement
T1071: Application Layer Protocol
T1588.006: Obtain Capabilities: Vulnerabilities
T1190: Exploit Public-Facing Application
T1021.004: Remote Services: SSH
T1059.004: Command and Scripting Interpreter: Unix Shell

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-0543	Redis (Debian package): 5.0.3-4+deb10u1 - 5:6.0.16-1+deb11u1	cpe:2.3:a:redis:redis:-:*:*:*:*:*:*:*	Remote code execution in Redis package for Debian Linux	CWE-94
CVE-2017-10271	Oracle WebLogic Server: 12.1.3.0.0 - 12.2.1.2	cpe:2.3:a:oracle:weblogic_server:*:*:*:*:*:*:*:*,	Denial of service in Oracle WebLogic Server	CWE-284

Hive Pro

THREAT ADVISORY

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2018-7600	Drupal7 (Debian package): <7.57, 8.0.0 – 8.3.9, 8.4.0 – 8.4.6, 8.5.0 – 8.5.1	cpe:2.3:a:drupal:drupal:*:*:*:*:*:*:*:*	Debian input validation for drupal7	CWE-20
CVE-2019-2725	Oracle Weblogic server 10.3.6 - 12.1.3	cpe:2.3:a:oracle:weblogic_server:10.3.6.0.0:*:*:*:*:*:*:*, cpe:2.3:a:oracle:weblogic_server:12.1.3.0.0:*:*:*:*:*:*:*	Remote code execution in Oracle WebLogic Server	CWE-74
CVE-2021-26084	Atlassian confluence Servers and Datacenters versions Up to 6.13.22, 6.14.0-7.4.10, 7.5.0-7.11.5, 7.12.0-7.12.4	cpe:2.3:a:atlassian:confluence:*:*:*:*:*:*:*:*, cpe:2.3:a:atlassian:confluence_server:*:*:*:*:*:*:*:*, cpe:2.3:a:atlassian:data_center:*:*:*:*:*:*:*:*	Atlassian Confluence Server and Center code execution vulnerability	CWE-74
CVE-2021-44228	Apache log4j versions 2.0 to 2.14.1	cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:*	Apache Log4j remote code execution	CWE-20 CWE-400 CWE-502

Indicators of Compromise (IoCs)

Type	Value
SHA-256	4817893f8e724cbc5186e17f46d316223b7683dcbc9643e364b5913f8d2a9197, 46389c117c5f41b60e10f965b3674b3b77189b504b0aeb5c2da67adf55a7129f, 95d1fca8bea30d9629fdf05e6ba0fc6195eb0a86f99ea021b17cb8823db9d78b, 7d3855bb09f2f6111d6c71e06e1e6b06dd47b1dade49af0235b220966c2f5be3, 16b4093813e2923e9ee70b888f0d50f972ac607253b00f25e4be44993d263bd2, 28443c0a9bfd8a12c12a2aad3cc97d2e8998a9d8825fcf3643d46012f18713f0, 36a2ac597030f3f3425153f5933adc3ca62259c35f687fde5587b8f5466d7d54
Domain	disneycareers[.]net, find-dreamjob[.]com, indeedus[.]org, varietyjob[.]com, ziprecruiters[.]org

Type	Value
Domain	ziprecruiters[.]org, blockchainnews[.]vip, chainnews-star[.]com, financialtimes365[.]com, fireblocks[.]vip, gatexpiring[.]com, gbclabs[.]com, giantblock[.]org, humingbot[.]io, onlynova[.]org, teenbeanjs[.]com
IPs	170[.]210.45.163, 191[.]232.38.25, 79[.]172.212.132, 104[.]236.150.159, 170[.]210.45.163, 146[.]185.136.187, 178[.]62.69.4, 191[.]232.38.25, 79[.]172.212.132, 221[.]120.103.253, 106[.]246.224.219, 160[.]16.58.163

Patch

http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
https://security-tracker.debian.org/tracker/CVE-2022-0543
http://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2725-5466295.html
https://github.com/g0rx/CVE-2018-7600-Drupal-RCE
https://jira.atlassian.com/browse/CONFSERVER-67940
https://logging.apache.org/log4j/2.x/manual/migration.html

References

https://blogs.juniper.net/en-us/security/muhstik-gang-targets-redis-servers