

行政院國家資通安全會報技術服務中心

Log4Shell(CVE-2021-44228)漏洞資訊與修補方式說明

發布日

111/2/14

1. 概述

Apache Log4j 是一個 Java 日誌記錄工具，研究人員發現 Log4j 存在安全漏洞(CVE-2021-44228)，攻擊者可藉由發送特製 HTTP 請求觸發 JNDI 查詢功能，利用漏洞進而遠端執行任意程式碼。

2. 漏洞檢測方式

2.1.使用 CVE-2021-44228_scanner 檢測

CVE-2021-44228_scanner 由美國卡內基美隆大學軟體工程研究所(Software Engineering Institute, SEI)負責維運之 CERT/CC 提供，包含 PowerShell、Python 及 Bash 等 3 種檢測方式與腳本。

- 下載網址：https://github.com/CERTCC/CVE-2021-44228_scanner

- PowerShell 版腳本檢測方式

- 請下載「checkjndi.ps1」並放置於欲檢測之標的目錄。

- 開啟 PowerShell，切換至標的目錄，執行「.\checkjndi.ps1」指令進行檢測。

- 檢測結果顯示「WARNING」，代表受此漏洞影響。

- 檢測結果顯示「** BUT APPEARS TO BE [已修補版本]**」，代表不受此漏洞影響(詳見圖 1)。

```

PS C:\tmp> .\checkjndi.ps1
WARNING: C:\tmp\2.15\log4j-core-2.15.0.jar contains org/apache/logging/log4j/core/lookup/JndiLookup.class
C:\tmp\2.16\log4j-core-2.16.0.jar contains "JndiLookup.class" ** BUT APPEARS TO BE 2.16 OR NEWER **
WARNING: C:\tmp\ghidra_10.0_PUBLIC\Ghidra\Framework\Generic\lib\log4j-core-2.12.1.jar contains org/apache/logging/log4j/core/lookup/JndiLookup.class
WARNING: C:\tmp\log4jRCE-0.0.1-SNAPSHOT.ear contains BOOT-INF\lib\log4j-core-2.14.1.jar contains org/apache/logging/log4j/core/lookup/JndiLookup.class
WARNING: C:\tmp\log4jRCE-0.0.1-SNAPSHOT.war contains BOOT-INF\lib\log4j-core-2.14.1.jar contains org/apache/logging/log4j/core/lookup/JndiLookup.class
WARNING: C:\tmp\log4shell-vulnerable-app-0.0.1-SNAPSHOT.jar contains BOOT-INF\lib\log4j-core-2.14.1.jar contains org/apache/logging/log4j/core/lookup/JndiLookup.class
WARNING: C:\tmp\nested.war contains BOOT-INF\lib\log4j-core-2.14.1.jar contains org/apache/logging/log4j/core/lookup/JndiLookup.class
WARNING: C:\tmp\test_nested.jar contains BOOT-INF\lib\log4j-core-2.14.1.jar contains org/apache/logging/log4j/core/lookup/JndiLookup.class
WARNING: C:\tmp\UPPERCASE.JAR contains BOOT-INF\lib\log4j-core-2.14.1.jar contains org/apache/logging/log4j/core/lookup/JndiLookup.class
C:\tmp>

```

圖1 PowerShell 腳本檢測示意圖

●Python 版腳本檢測方式

- 請下載「checkjndi.py」，並開啟命令提示字元(cmd)視窗，切換至存放「checkjndi.py」腳本之目錄。
- 執行「python checkjndi.py [標的目錄]」指令進行檢測。
 - 檢測結果顯示「WARNING」，代表受此漏洞影響。
 - 檢測結果顯示「** BUT APPEARS TO BE [已修補版本]**」，代表不受此漏洞影響(詳見圖 2)。

```

C:\WINDOWS\system32\cmd.exe
C:\tmp>python checkjndi.py c:\tmp
WARNING: c:\tmp\2.15\log4j-core-2.15.0.jar contains "JndiLookup.class"
C:\tmp\2.16\log4j-core-2.16.0.jar contains "JndiLookup.class" ** BUT APPEARS TO BE 2.16 OR NEWER **
WARNING: c:\tmp\ghidra_10.0_PUBLIC\Ghidra\Framework\Generic\lib\log4j-core-2.12.1.jar contains "JndiLookup.class"
WARNING: c:\tmp\log4jRCE-0.0.1-SNAPSHOT.ear contains BOOT-INF\lib\log4j-core-2.14.1.jar contains "JndiLookup.class"
WARNING: c:\tmp\log4jRCE-0.0.1-SNAPSHOT.war contains BOOT-INF\lib\log4j-core-2.14.1.jar contains "JndiLookup.class"
WARNING: c:\tmp\log4shell-vulnerable-app-0.0.1-SNAPSHOT.jar contains BOOT-INF\lib\log4j-core-2.14.1.jar contains "JndiLookup.class"
WARNING: c:\tmp\nested.war contains log4jRCE-0.0.1-SNAPSHOT.ear contains BOOT-INF\lib\log4j-core-2.14.1.jar contains "JndiLookup.class"
WARNING: c:\tmp\test_nested.jar contains log4jRCE-0.0.1-SNAPSHOT.jar contains BOOT-INF\lib\log4j-core-2.14.1.jar contains "JndiLookup.class"
WARNING: c:\tmp\UPPERCASE.JAR contains BOOT-INF\lib\log4j-core-2.14.1.jar contains "JndiLookup.class"
C:\tmp>

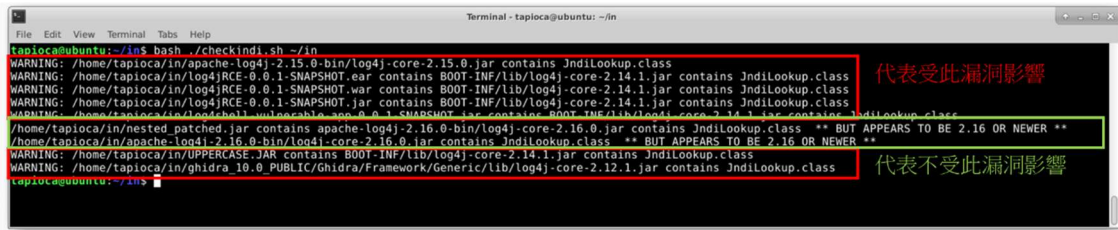
```

圖2 Python 腳本檢測示意圖

●Bash 版腳本檢測方式

- 請下載「checkjndi.sh」，並開啟 Terminal 視窗，切換至存放「checkjndi.sh」腳本之目錄。
- 執行「bash checkjndi.sh [標的目錄]」指令進行檢測(詳見圖 3)。
 - 檢測結果顯示「WARNING」，代表受此漏洞影響。

- 檢測結果顯示「** BUT APPEARS TO BE [已修補版本]**」，代表不受此漏洞影響。



```
Terminal - tapioca@ubuntu: ~\in
tapioca@ubuntu:~/in$ ./checkindi.sh ~/in
WARNING: /home/tapioca/in/apache-log4j-2.15.0-bin/log4j-core-2.15.0.jar contains JndiLookup.class
WARNING: /home/tapioca/in/apache-log4j-2.15.0-bin/log4j-core-2.14.1.jar contains JndiLookup.class
WARNING: /home/tapioca/in/log4jrce-0.0.1-SNAPSHOT.ear contains BOOT-INF/lib/log4j-core-2.14.1.jar contains JndiLookup.class
WARNING: /home/tapioca/in/log4jrce-0.0.1-SNAPSHOT.war contains BOOT-INF/lib/log4j-core-2.14.1.jar contains JndiLookup.class
WARNING: /home/tapioca/in/log4jrce-0.0.1-SNAPSHOT.jar contains BOOT-INF/lib/log4j-core-2.14.1.jar contains JndiLookup.class
WARNING: /home/tapioca/in/log4jchall-multipleable-0.0.1-SNAPSHOT.jar contains BOOT-INF/lib/log4j-core-2.14.1.jar contains JndiLookup.class
/home/tapioca/in/nested_patched.jar contains apache-log4j-2.16.0-bin/log4j-core-2.16.0.jar contains JndiLookup.class ** BUT APPEARS TO BE 2.16 OR NEWER **
/home/tapioca/in/apache-log4j-2.16.0-bin/log4j-core-2.16.0.jar contains JndiLookup.class ** BUT APPEARS TO BE 2.16 OR NEWER **
WARNING: /home/tapioca/in/UPPERCASE.JAR contains BOOT-INF/lib/log4j-core-2.14.1.jar contains JndiLookup.class
WARNING: /home/tapioca/in/ghidra_10.0_PUBLIC/Ghidra/Framework/Generic/lib/log4j-core-2.12.1.jar contains JndiLookup.class
tapioca@ubuntu:~/in$
```

代表受此漏洞影響

代表不受此漏洞影響

圖3 Bash 腳本檢測示意圖

2.2.使用 Log4j Scanner 工具檢測

Log4j Scanner 由美國網路安全及基礎設施安全局(Cybersecurity and Infrastructure Security Agency, CISA)提供。

- 下載網址：<https://github.com/cisagov/log4j-scanner/tree/master/log4-scanner>

- 檢測方式

- 請下載「log4-scanner」資料夾，並開啟 Terminal 視窗，切換至「log4-scanner」資料夾，再進入「log4scanner」資料夾。

- 執行「python3 log4j-scan.py -u [標的 URL]」指令進行檢測(詳見圖 4)。

- 檢測結果出現「Targets Affected」，代表受此漏洞影響。

- 檢測結果出現「Target do not seem to be vulnerable」，代表不受此漏洞影響。

```
(root@kali) ~/log4j-scanner/log4j-scanner
└─$ python3 log4j-scan.py -u http://172.20.10.7:8080
[*] CVE-2021-44228 - Apache Log4j RCE Scanner
[*] Scanner provided by FullHunt.io - The Next-Gen Attack Surface Management Platform.
[*] Secure your External Attack Surface with FullHunt.io.
[*] Initiating DNS callback server (Interact.sh).
[*] Checking for Log4j RCE CVE-2021-44228.
[*] URL: http://172.20.10.7:8080
[*] URL: http://172.20.10.7:8080 | PAYLOAD: ${jndi:ldap://172.20.10.7.c0p68958968j430196746g1s1rva6424r.interact.sh/wihlflf}
[*] Payloads sent to all URLs. Waiting for DNS OOB callbacks.
[*] Waiting...
[!!!] Targets Affected : 1 (2022-02-11T01:51:17.07623296Z)
{"timestamp": "2022-02-11T01:51:17.07623296Z", "host": "172.20.10.7.c0p68958968j430196746g1s1rva6424r.interact.sh", "remote_address": "202.144.211.169"}

(root@kali) ~/log4j-scanner/log4j-scanner
└─$ python3 log4j-scan.py -u http://172.20.10.8:8080
[*] CVE-2021-44228 - Apache Log4j RCE Scanner
[*] Scanner provided by FullHunt.io - The Next-Gen Attack Surface Management Platform.
[*] Secure your External Attack Surface with FullHunt.io.
[*] Initiating DNS callback server (Interact.sh).
[*] Checking for Log4j RCE CVE-2021-44228.
[*] URL: http://172.20.10.8:8080
[*] URL: http://172.20.10.8:8080 | PAYLOAD: ${jndi:ldap://172.20.10.8.hq01s3dtu4s44eht9393je91w62x24g6s.interact.sh/lw92wvt}
[*] Payloads sent to all URLs. Waiting for DNS OOB callbacks.
[*] Waiting...
[*] Targets do not seem to be vulnerable 代表不受此漏洞影響
```

圖4 Log4j Scanner

3. 防護建議

- Apache Log4j 官方網頁已針對此漏洞釋出更新程式，請各機關聯絡設備維護廠商進行版本確認並進行更新，其中 Java 8 環境請更新至 Log4j 2.17.0 或之後版本、Java 7 環境請更新至 Log4j 2.12.3 或之後版本、Java 6 環境請更新至 Log4j 2.3.1 或之後版本：

<https://logging.apache.org/log4j/2.x/security.html>

- 漏洞修補前，亦可透過以下步驟停用 JNDI Lookup 功能，以緩解此漏洞

(1) 針對 log4j 版本 >= 2.10 的系統

- A. 請設定屬性「log4j2.formatMsgNoLookups=true」。
- B. 請設定環境變數「LOG4J_FORMAT_MSG_NO_LOOKUPS=true」。

(2) 針對 log4j 版本為 2.0-beta9 到 2.10.0 的系統

請自類別路徑(class path)中移除 JndiLookup.class。如執行下列指令，以自 log4j-core 中移除該類別：

```
└─$ zip -q -d log4j-core-*.jar
```

org/apache/logging/log4j/core/lookup/JndiLookup.class」。

- 透過 WAF 對相關惡意語法進行過濾及阻擋

使用對外防護設備針對 JNDI 之相關惡意攻擊行為設定規則進行阻擋，例如”\$(jndi:ldap://”。

- 評估於 Java 伺服器增加以下設定以防止下載與執行可能具風險之惡意 Java Class

將 com.sun.jndi.ldap.object.trustURLCodebase 設定為 false，使 JNDI 無法使用 LDAP 下載遠端 Java Class。

4. 參考資料

[1]<https://www.cisa.gov/uscert/ncas/alerts/aa21-356a>

[2]<https://github.com/cisagov/log4j-scanner>

[3]https://github.com/CERTCC/CVE-2021-44228_scanner

[4]<https://www.nccst.nat.gov.tw/VulnerabilityDetail?lang=zh&seq=1194>

[5]<https://blog.cloudflare.com/zh-tw/inside-the-log4j2-vulnerability-cve-2021-44228-zh-tw/>

[6]https://www.trendmicro.com/zh_tw/about/newsletter/2021/patch-now-apache-log4j-vulnerability-called-log4shell-being-acti.html

5. 聯絡資訊

如果您對此通告的內容有疑問或有關於此事件的建議，請勿直接回覆此信件，請以下述聯絡資訊與我們聯絡。

地 址：台北市富陽街 116 號

聯絡電話：02-27339922

傳真電話：02-27331655

電子郵件信箱：service@nccst.nat.gov.tw