SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

2023.08.05 (六) —— 2023.08.11 (五)

https://stb.stpi.narl.org.tw/

資安暨智慧科技研發大樓

▶ 五眼聯盟公布去年最常被利用的12個安全漏洞

美國、澳洲、加拿大、紐西蘭與英國等5個國家的網路安全機構連袂公布了2022年最常遭到駭客利用的安全漏洞，相較於新漏洞，駭客更青睞舊漏洞，而且專注於尋找那些可透過網路存取且未被修補的漏洞。在這12個最常被利用的安全漏洞中，有6個屬於遠端程式攻擊漏洞，分別是存在於微軟Exchange Server的CVE-2021-34473，位於Zoho ManageEngine ADSelfService Plus的CVE-2021-40539，出現在Apache Log4j2的CVE-2021-44228，現身於VMware Workspace ONE存取暨身分管理功能中的CVE-2022-22954，微軟多個產品中的CVE-2022-30190，以及Atlassian Confluence Server and Data Center的CVE-2022-26134。

【資料來源：iThome 2023.08.07】

▶ 微軟8月Patch Tuesday修補2個零時差漏洞

微軟周二（8/8）修補了超過70個安全漏洞，包含兩個已遭到駭客利用的零時差漏洞CVE-2023-36884及CVE-2023-38180。其中的CVE-2023-36884是個Windows Search遠端程式執行漏洞，在透過電子郵件或即時訊息的攻擊場景中，駭客只要傳遞一個特製的檔案予目標對象就能利用該漏洞，條件是受害者必須開啟該檔案。至於CVE-2023-38180則為.NET與Visual Studio的服務阻斷漏洞，微軟僅說該漏洞已遭到駭客利用，並未說明漏洞細節。

【資料來源：iThome 2023.08.09】

SHALUN
CYBER SECURITY HUB

資安週報

沙崙資安基地

2023.08.05 (六) —— 2023.08.11(五)

https://stb.stpi.narl.org.tw/
資安暨智慧科技研發大樓

▶ SSH仍是最熱門的雲端攻擊目標

雲端安全事件回應解決方案供應商CadoSecurity近日發佈2023年雲威脅調查報告。

本次報告主要發現包含：僵屍網路代理程式在惡意軟體領域佔主導地位，是所有流量的40.3%，僵屍網路在俄烏戰爭中由駭客驅動的DDoS攻擊中有重要作用。SSH仍然是最具針對性攻擊的服務，占觀察樣本的68.2%。Redis佔 27.6%，而Log4Shell漏洞的利用則下降至僅4.3%。此現象表示雲端攻擊駭客的策略改變，不再優先以漏洞作為初始攻擊手段。高達97.5%的惡意攻擊者針對單一特定服務中的漏洞，這表明攻擊者傾向利用已知的漏洞。

【資料來源：INFO SECURITY 2023.08.07】

▶ 英國選舉委員會遭駭客入侵，選民資料全曝光

英國的選舉委員會（Electoral Commission）在周二（8/8）坦承，該委員會自2021年8月以來就遭到駭客入侵，而一直到去年10月才發現，在這期間，駭客已存取了其存有電子郵件、控制系統與選民登記名冊的伺服器。選舉委員會並未透露外洩名冊含有多少筆資料，僅說被存取的名冊涉及2014年至2022年之間所登記的當地及海外選民，且只含有他們的姓名、地址，以及到達投票年齡的日期。

【資料來源：iThome 2023.08.09】