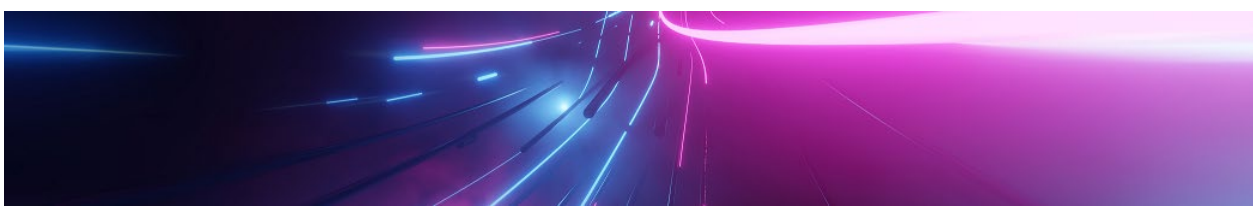
111年第2季資通安全技術報告

Quarterly Technical Report



目　次

圖 目 次

摘要

「第 2 季資通安全技術報告」除分析本季全球資安威脅、政府通報資安事件外，並提供相對應之資安防護建議。同時，藉由資安專題分享與資安技術研析，提供政府機關需關注之資安風險重點。

「第 2 季資通安全技術報告」分為以下 4 個章節。

●1.資安威脅現況與防護重點

從分析全球資安威脅現況開始，第 1 起案例為 Spring4Shell 零時差(Zero Day)漏洞遭利用造成廣泛攻擊；另一起案例為醫院專用機器人 Tug 存在多項零時差漏洞。

分析政府資安威脅現況，發現政府機關通報事件原因，以「非法入侵」(占 53.64%)類型為主，排除綜合類型「其他」外，其次分別為「設備問題」(占 9.09%)與「網頁攻擊」(占 6.36 %)為主要通報類型。

●2.資安專題分享

資安專題分享主題為零信任網路智慧信任推斷研析，零信任網路以決策引擎為核心，包含身分鑑別、設備鑑別及信任推斷 3 大關鍵技術，其中信任推斷為決策引擎最後一環，其綜合考量各項內外部參數並計算信任等級，以決定主體請求存取之資源是否被核可。

●3.資安技術研析

資安技術研析主題為 Dirty Pipe 弱點研析與驗證實作，網路服務託管公司 CM4all 之軟體工程師於處理客戶反應之日誌壓縮檔損毀問題時，發現 Gzip 出現循環冗餘校驗錯誤，同樣問題持續發生，而在陸續測試排除硬體、應用程式及網路服務問題後，從而發現此弱點(CVE-2022-0847)。

●4.結論

本報告透過分析全球與政府之資安事件與統計數據，了解最新資安威脅趨勢與因應之資安防護重點。資安專題分享零信任網路智慧信任推斷研析，經由概念性驗證，分析機器學習信任推斷結果。此外，資安技術研析概述 Dirty Pipe 弱點成因與利用方式，並進行弱點攻擊驗證實作。

1. 資安威脅現況與防護重點

本報告藉由檢視當季國內外所發生之資安事件或議題，研析事件發生之主要原因及可能之衝擊與影響。111 年第 2 季(以下簡稱本季)探討零時差漏洞與軟體下載安裝之相關資安議題，研析如何加強零時差漏洞之防範與軟體下載、安裝之資安意識與作為。

本章節之事件與議題皆配合整理相關之資安防護重點，提供政府機關就相關資安風險或議題進行評估，並依循資安管理規範與技術防禦進行強化。

1.1 全球資安威脅現況

111 年 WEF 全球風險報告中，在科技類型風險新增一項負面之科技進步(Adverse Tech Advances)，此項分類打破普世價值認為科技始終帶來進步之傳統印象。科技進步如人工智慧、生物技術及量子計算等，若用於正面科技發展，將為人類帶來進步之福音；反之，若讓惡意人士用於危害用途，如 AI 技術之濫用或量子電腦用於暴力破解密碼，則將帶來新的資安威脅。此外，當廠商不斷提升其技術與樣態，釋出更多便利使用者之介面或功能時，若未能兼顧資安議題，則可能造成另一波負面之科技進步影響。

本季全球資安威脅聚焦討論零時差漏洞遭利用之資安事件，駭客利用揭露產品漏洞而獲取利益，又因現今科技產品運用廣泛，以致漏洞一旦被暴露影響極大。另一方面，若駭客鎖定對象為創新科技產品，如機器人或無人駕駛之交通運輸載具，更需積極注意產品安全狀態。

本季具指標性案例為 Spring4Shell 零時差(Zero Day)漏洞遭利用造成廣泛攻擊；另一起案例為醫院專用機器人 Tug 存在多項零時差漏洞。

首先，探討案例為資安業者 Sonatype 指出，日前遭發現之零時差漏洞 Spring4Shell(CVE-2022-22965)，在原廠緊急推出更新修補程式後，仍發現

該漏洞遭駭客大規模用於攻擊活動中。據統計近期全球約 1/6 組織遭受 Spring4Shell 零時差漏洞影響成為駭客攻擊目標，根據 Check Point 分析，3 月 31 日至 4 月 2 日期間即偵測出高達 37,000 次 Spring4Shell 攻擊。遭受影響最大之行業為軟體供應商，占總數 28%，分析原因可能為駭客發動供應鏈攻擊所致。至於受影響地區，20%位於歐洲，北美地區亦占 11%。

Spring4Shell 漏洞發生原因為在傳送參數時未能進行安全之反序列化(Deserialization)，該錯誤可讓駭客遠端執行任意程式碼(Remote Code Execution, RCE)，CVSS 風險程度評分高達 9.8 分，為最高之「嚴重」(Critical)等級。SpringShell 漏洞遭揭露後，儼然成為駭客之新目標，如一直活躍於網路之殭屍網路程式 Mirai，藉著 SpringShell 漏洞感染 IoT 裝置，展開新一波攻擊活動，趨勢科技於 4 月初監測到 SpringShell 漏洞之攻擊活動，駭客將 Mirai 下載到 IoT 裝置之/tmp 資料夾，利用 chmod 指令變更權限後執行；該公司另於網路上偵測發現惡意檔案伺服器，內含針對不同 CPU 架構設計之其他 Mirai 變種程式。

第 2 起案例為醫療物聯網安全解決方案廠商 Cynerio 於 4 月宣布發現，Aethon 公司所生產之醫院專用機器人 Tug 存在 5 項零時差漏洞，統稱為 JekyllBot:5，這些漏洞預估將可能會影響全球數百家醫院。Aethon 公司所生產之醫院機器人 Tug 可用於藥物發送、清掃及運送備品，在利用無線電波、傳感器、攝影鏡頭頭及其他技術於無人協助情況下自在移動，不會撞到人或物體，且可自動開關門、搭乘電梯等。

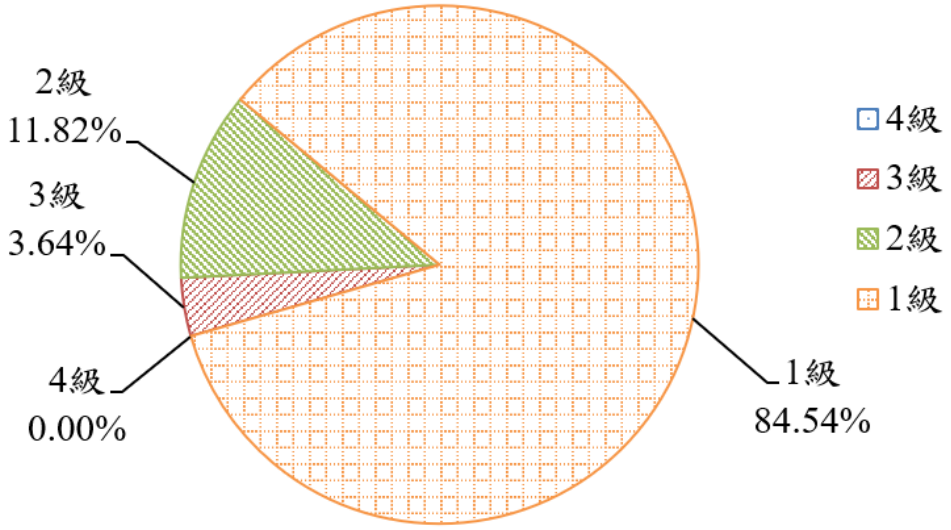
因為 Tug 機器人可於醫院內獨立移動之技術，使得 Cynerio 所發現之 JekyllBot:5 漏洞可能造成極大之風險，如干擾醫療用品之運送、侵犯醫護人員或病患隱私及竊取醫療紀錄等。此 5 項零時差漏洞包含 CVE-2022-1066、CVE-2022-26423、CVE-2022-1070、CVE-2022-27494 及 CVE-2022-1059，分別位於 Tug 伺服器之 JavaScript、API 實作及 WebSocket 協定

中。其中一項高風險漏洞允許駭客接管運作中之 Tug 機器人，透過連接 Tug 伺服器 WebSocket 以接管機器人，直接操作其移動路線與位置。其他漏洞可讓駭客藉由新增具管理權限之用戶帳號與刪改現有帳號、存取用戶之加密憑證、竊取 Cookie、攔截對話資料，甚至可能進一步被利用進行網路釣魚等行為。Cynerio 研究發現入侵此 5 項零時差漏洞，不需高超技術且無需特殊權限或任何使用者互動，就能成功運用這些漏洞。

綜覽本季重大資安事件，駭客利用尚未修補之漏洞展開攻擊，因產品廠商未能及時釋出修補程式，受駭者通常對此類未具備足夠之防範意識或抵抗力，因此造成之衝擊往往無法預期其影響範圍與後果。隨著科技所帶來之生活便利外，系統開發者應注意開發過程中之資安要求與上線前完成驗證。另一方面，組織內部管理者應提高警覺，監測所使用產品之安全性與更新程式相關訊息。

1.2 政府資安威脅現況

彙整本季所接獲之政府機關通報事件，藉由事件之影響等級、通報類型及事件原因，了解目前政府機關之資安威脅現況。通報事件依「機密性」、「完整性」、「可用性」3 個面向所造成之衝擊，將事件影響等級由輕至重分為 1 級、2 級、3 級及 4 級。彙整事件影響等級，本季以 1 級事件占 84.54%為大宗，2 級事件占 11.82%次之，3 級事件僅占 3.64%，而 4 級通報事件則未發生，相關統計情形詳見圖 1。

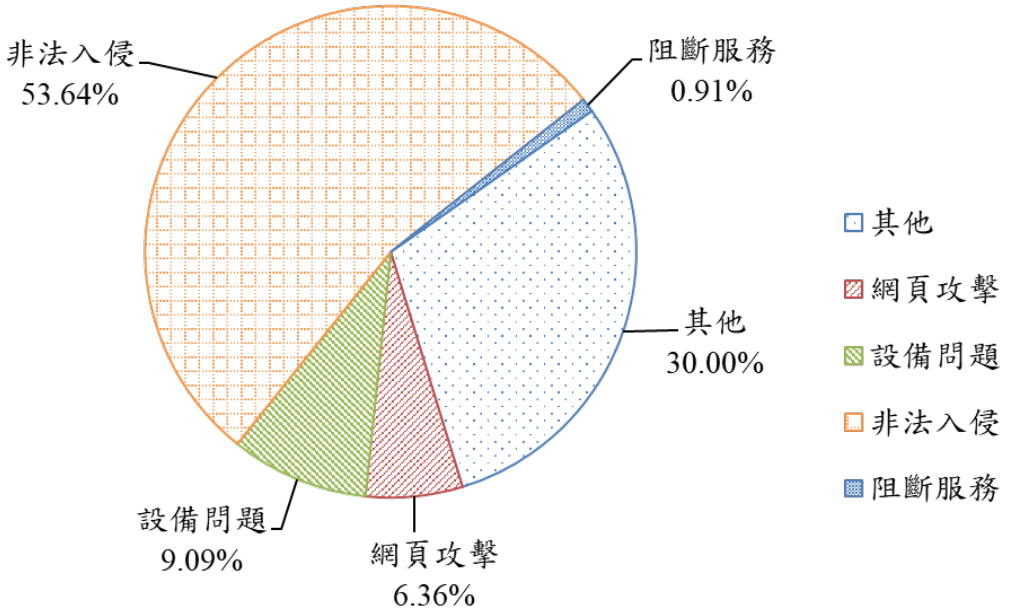


資料來源：本報告整理

圖1　111 年第 2 季通報事件影響等級比率圖

本季接獲之 3 級重要通報事件，大多為設備故障引起，如某機關進行例行性系統維護後因內部零組件故障導致重啓失敗，僅存之資料庫無法負荷造成業務中斷；另有核心業務系統資料庫主機之主機板或核心交換器故障等，因機關判斷「涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作」，故通報為 3 級重要事件。

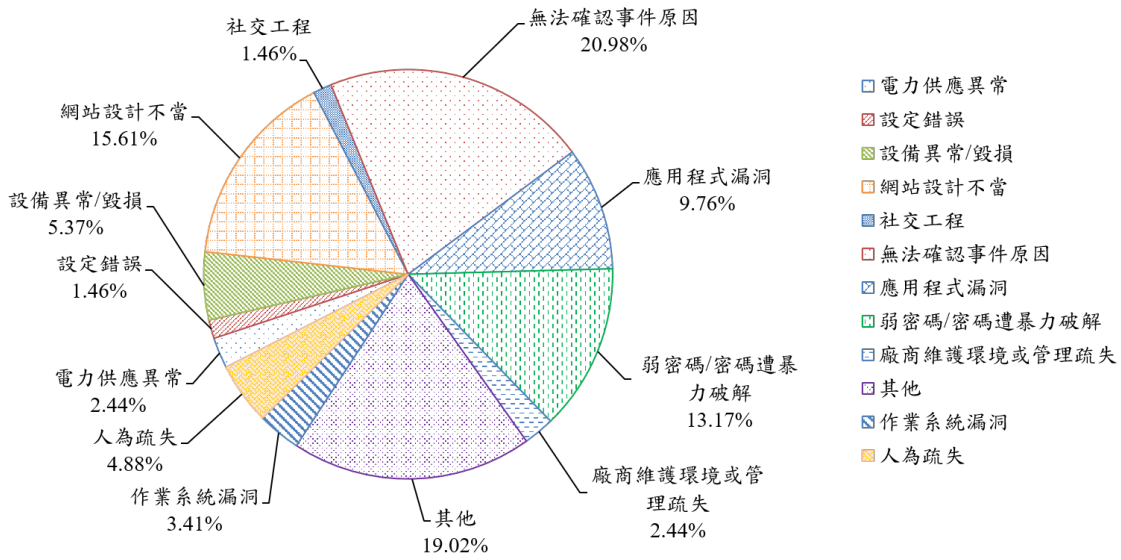
通報事件中發現其他資訊設備所引起之資安事件，如技服中心發現部分機關資訊設備出現符合惡意程式行為之連線，調查後發現為機關之監視器設備使用弱密碼，且其韌體版本老舊未更新，存在許多漏洞而引發資安事件。整體事件比率，以「非法入侵」(占 53.64%)類型為主，排除綜合類型「其他」外，「設備問題」與「網頁攻擊」類型次之，詳見圖 2。



資料來源：本報告整理

圖2　111 年第 2 季通報類型比率圖

最後，分析通報事件發生原因，可發現除無法確認事件原因(20.98%)外，其次分別為其他(19.02%)、網站設計不當(15.61%)、弱密碼/密碼遭暴力破解(13.17%)、應用程式漏洞(9.76%)、設備異常/毀損(5.37%)、人為疏失(4.88%)、作業系統漏洞(3.41%)、電力供應異常(2.44%)、廠商維護環境或管理疏失(2.44%)、設定錯誤(1.46%)及社交工程(1.46%)，詳見圖 3。本季一般事件發生原因以無法確認事件原因為主，占 20.98%，經歸納有近 5 成為調查後仍無法確認事件發生原因，顯示積極發展溯源機制之重要性，另亦突顯駭客入侵來源之多樣性，致無法找出根因。另外，有部分原因為系統汰換逕行下架、無相關紀錄可供檢視及相關紀錄遭異常刪除或變更等原因，上述這些因素都會影響正常鑑識過程與結果，建議機關若發生資安事件，應留存或備份相關紀錄與日誌，確保紀錄不被竄改或刪除。



資料來源：本報告整理

圖3　111 年第 2 季通報事件發生原因比率圖

分析第 2 季通報事件發生原因，發現為使用者資安意識不足，或程式設計人員未遵循安全系統發展生命週期之原則，導致之資安事件，案例分別為某機關人員未察覺已連結至駭客偽造之頁面，並下載夾帶惡意檔案之非官方授權軟體；另一起案例則為，先偵測到網站伺服器發生對外進行異常連線或存在惡意程式，調查後發現網站因程式設計時存在 SQL Injection 漏洞，又因於上傳功能未確實檢查上傳之檔案格式，導致遭植入惡意程式。

1.3 資安防護重點

分析本季全球資安威脅現況，零時差攻擊通常會先傳出受駭者或資安事件時，廠商才開始修補程式，因此零時差攻擊常常發生在更新版本釋出前之空窗期或是遲遲未意識到資安漏洞之受駭組織。隨著內部部署產品之多樣性與隨之而來之資安風險，規劃產品資安事件應變小組，以因應零時差攻擊或產品漏洞，展現積極主動之防護作為。

國內因人員於存取時採用預設密碼或弱密碼狀況仍時有所聞，本季資安事

件中又發生人員誤於偽冒之網站下載非官方授權軟體，顯示針對一般使用者應持續加強資安意識之宣導，而對於資訊人員更應加強對資安組態基準設定與系統發展生命週期之資安要求。

綜整以上資安威脅現況，提供資安防護建議如下：

●零時差漏洞之資安管理

– 採購產品時，應依其業務用途定義產品所需之資安成熟度與細項要求，並定期監控與分析異常網路行為。

– 採用縱深防禦或多層式之資安防禦架構，增加入侵難度與阻礙。

– 以最小權限管理原則，加強資源存取時之驗證機制。

●軟體安裝之資安管理

– 訂定軟體下載與安裝之政策規範，定期更新且宣導以落實管理。

– 維護開放下載之軟體白名單，並提供或限制軟體下載來源。

– 安裝前應先檢測其安全性，並藉由建置資通安全弱點通報機制，主動監測系統更新或修補訊息。

2. 資安專題分享_零信任網路智慧信任推斷研析

零信任網路以決策引擎為核心，包含身分鑑別、設備鑑別及信任推斷 3 大關鍵技術，主體(Subject，一般指使用者)需要存取資源時，需要經過政策決策點(Policy Decision Point, PDP)決定是否授予存取權限，再由政策執行點(Policy Enforcement Point, PEP)實際執行每一次存取需求之通過或拒絕。其中，信任推斷為決策引擎最後一環，其綜合考量各項內外部參數並計算信任等級，以決定主體請求存取之資源是否被核可，因此相關研究與應用甚為重要。

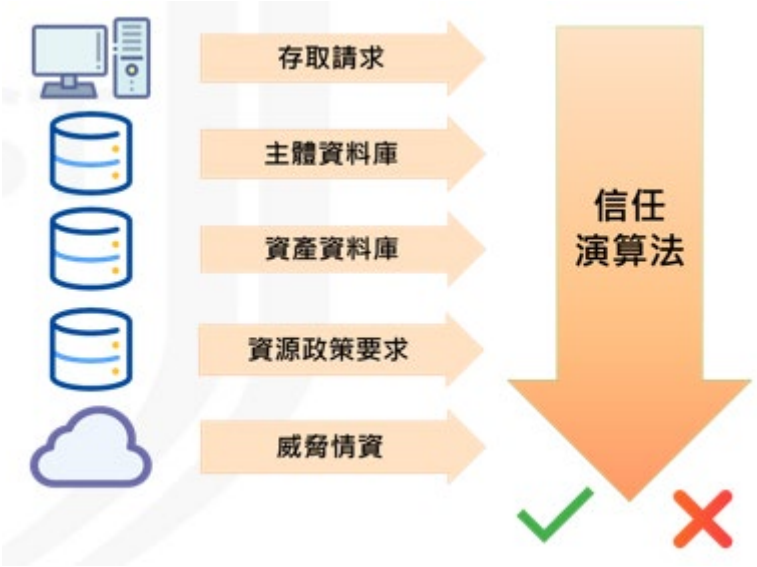
在美國國家標準暨技術研究院(National Institute of Standards and Technology, NIST)所發布之零信任框架 SP 800-207 標準文件(以下簡稱 NIST SP 800-207)中，建議之信任推斷作法主要是採取與歷史存取紀錄比對之情境原則；另美國國土安全部之網路安全暨基礎設施安全局(Cybersecurity and Infrastructure Security Agency, CISA)之零信任成熟度模型(Zero Trust Maturity Model)第 3 級最佳化(Optimal)，更進一步提出應使用機器學習即時分析使用者行為，以確認風險並提供持續保護之實作建議。

依據「國家資通安全發展方案(110 年至 113 年)」，規劃於 111 年至 113 年逐步導入零信任網路之身分鑑別、設備鑑別及信任推斷機制，此專題將概述零信任網路智慧信任推斷之研析，並經由概念性驗證，分析機器學習信任推斷結果，計算信任等級判斷存取准駁，以提升存取政策之可信賴度。

2.1 信任推斷概述

信任推斷主要為將「輸入資料」透過「信任演算法」運算，以產生決策之過程，藉由蒐集各種來源資料，做為信任演算法之輸入與運算依據，透過信任演算法將輸入資料進行運算並得到信任分數，以產生決策，如允許、拒絕、撤銷等動作。

輸入資料依 NIST SP 800-207 可分為 5 類，其中存取請求為主要情境資料之參考來源，詳見圖 4。



資料來源：NIST SP 800-207

圖4　信任演算法輸入資料

- 存取請求(Access Request)：為使用者提出存取請求之相關資訊，包含所使用之作業系統、欲存取之目標資源、設備 ID、IP 位址及應用程式更新版本(是否已在核可清單)。根據上述因素與整體資產安全樣貌，其存取可能被限制或拒絕。
- 主體資料庫(Subject Database)：為使用者相關資訊，包含個人身分 ID、經由 PEP 執行之身分驗證檢查結果及可推導其身分屬性之時間、地理位置及歷史存取行為紀錄，如登入時間、IP 位址、使用瀏覽器等。
- 資產資料庫(Asset Database)：為設備相關資訊，包含設備鑑別結果，如設備 ID、設備鑑別方式及設備健康狀態。依據資料庫中資產現行可觀察狀態(Observable Status)進行比對，再依比較結果，決定存取限制或拒絕。

- 資源請求(Resource Requirements)：定義針對資源與資料敏感性所設定之最低存取要求，包含最低鑑別保證等級(Authenticator Assurance Level, AAL)、IP 位址限制、設備健康狀態、資料機敏程度及資產組態之要求。
- 威脅情資(Threat Intelligence)：為來自外部服務平台或內部蒐集發現之威脅情資，包含惡意程式特徵與中繼站資訊等，此類資訊大部分來自於外部而非內部既有資訊。

以 Google 與 Cisco 之信任推斷方法論為例，Google 情境感知存取權(Context-Aware Access)依據使用者所處之情境，控管可存取哪些應用程式，可設定之情境(輸入資料)包含 IP 位址、地理位置、設備政策及設備作業系統等，決定情境感知存取權層級；另一服務廠商 Cisco 使用 Duo Trust Monitor，分析使用者與設備之存取行為並建立基準模型，顯示風險等級與警示資安事件等異常存取。分析之存取行為(輸入資料)，包含使用者 ID、使用者應用程式、使用者設備、身分鑑別因子、身分鑑別結果、登入時間及 IP 位址等，以決定正常使用者與設備存取行為之基準。

本報告為精進信任推斷之研究，規劃採計更多使用者行為之輸入資料，進行與歷史存取紀錄比對之機器學習信任推斷，輸入資料依資料屬性歸類，並分析資料相關性，藉由機器學習方法，研析機器學習類型與演算法進行適用性分析，以分析不同輸入資料適用之機器學習方法。

機器學習類型分別有監督式學習(Supervised Learning)、非監督式學習(Unsupervised Learning)及強化式學習(Reinforcement Learning)，此 3 種機器學習類型各有不同特性，監督式學習須事先將輸入資料標籤化，以便機器學習能有明確之依據；非監督式學習輸入資料無須事先標籤化，機器依據資料之關聯性能自動進行歸類；強化式學習則針對機器學習之輸出使用獎勵與懲罰方式回饋，讓機器認知對錯繼而強化學習。分析這 3 種機器學習類型，由於機器學習所分析使用者存取行為頻繁且相關紀錄

資料量龐大，資料事先標籤化與事後獎懲皆執行不易，因此將選定非監督式學習且已有成熟可實務運用之方法，適合對大量使用者行為進行慣性與異常分析，以下為非監督式學習演算法主要類別，詳見圖 5。

演算法類別	原理	常用演算法	適用性
異常檢測 (Outlier Detection)	基於離群程度或機率	• Local Outlier Factor (LOF) • Isolation Forest (IF) • One-Class SVM	適合分布廣泛之資料
分群 (Clustering)	分群並從各群中挑出異常	• K-Means • Gaussian Mixture Modeling (GMM) • DBSCAN	適合具群體性之資料
密度估計 (Density Estimation)	從樣本估計總體的概率密度函數	• Kernel Density Estimation (KDE)	適合種類有限之資料
降維 (Dimensionality Reduction)	降低資料維度	• PCA • Autoencoder	搭配其他類別使用，利於提高運算效能或視覺化呈現
關聯規則探勘 (Association Rule Mining)	找尋資料關聯性	• Apriori • Eclat	適合預測未來行為

資料來源：本報告整理

圖5　非監督式學習演算法

研析不同機器學習類型與演算法後，依輸入資料屬性歸類，並分析資料相關性。輸入資料類型分析，綜整現行商用服務與相關研究，將使用者行為之輸入資料依其屬性分為 3 類型，分別為時間相關，分析登入時間；另一類為位置相關，主要為 IP 位址、地理位置及時區；最後則為設備相關，依據其設備類型、OS 類型及 Browser 等進行行為分析，再分別就此 3 類型進行概念性驗證。

2.2 智慧信任推斷概念性驗證

規劃智慧信任推斷概念性驗證(Proof of Concept, PoC)前，先依輸入資料特性與相關性分析，分析適用之非監督式學習演算法，如時間相關資料(登入

時間)分布廣泛，適用異常檢測演算法；位置相關資料存在必然性，IP 位址可高度代表地理位置與時區，而 IP 位址之群體性適用分群演算法；設備類型相關資料因種類有限，若單獨進行機器學習成效不佳，規劃依相依性組合更多種類以提高機器學習成效，適用密度估計演算法，詳見圖 6。

輸入資料類型	輸入資料	特性	相關性	適用演算法
時間相關	登入時間	分布廣泛		異常檢測(Outlier Detection)
位置相關	IP位址	具群體性	存在必然性	分群(Clustering)
	地理位置	準確性不高		不採計
	時區	種類有限		密度估計(Density Estimation)
設備類型相關	設備類型	種類有限	存在相依性	密度估計(Density Estimation)
	OS	種類有限		密度估計(Density Estimation)
	Browser	種類有限		密度估計(Density Estimation)

資料來源：本報告整理

圖6　機器學習適用性分析

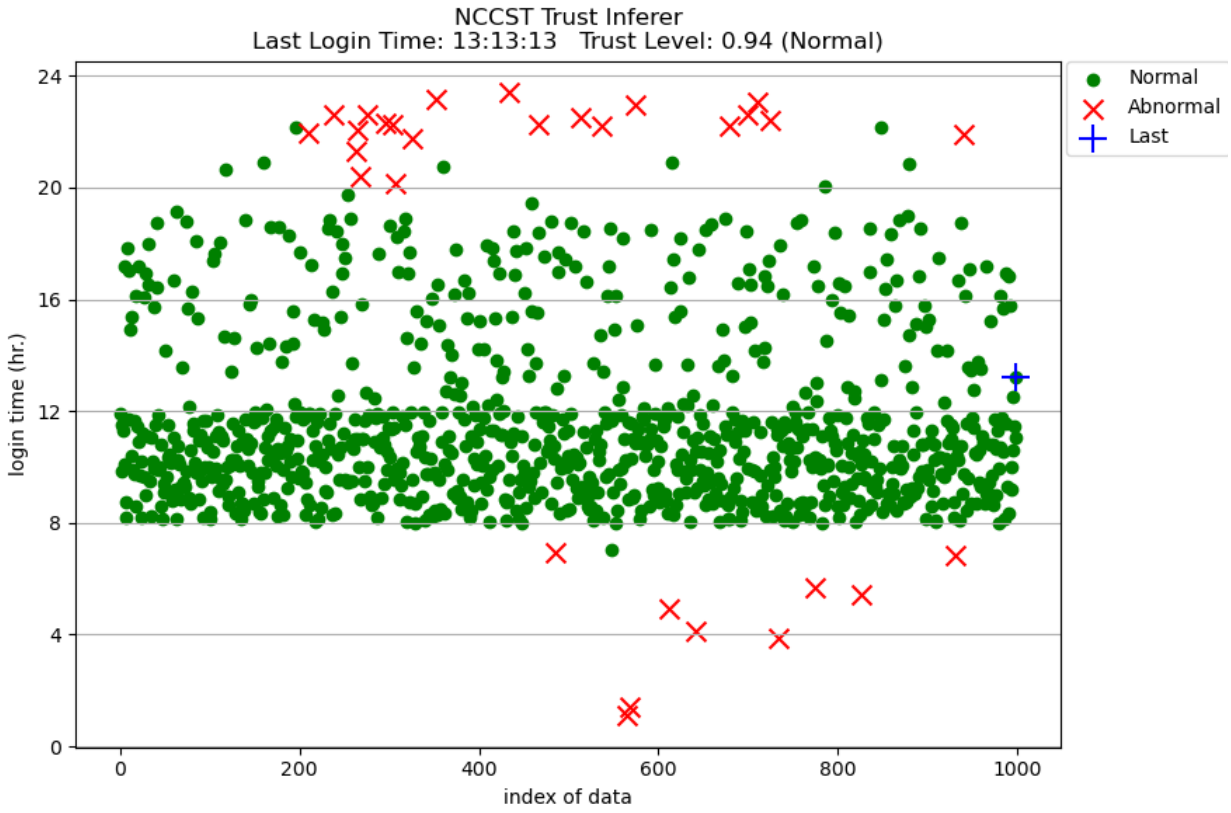
依輸入資料與機器學習之適用性分析，進行上述 3 類輸入資料之 PoC 實驗，並參考相關文獻研究，挑選適用之機器學習演算法，並針對不同情境模擬產生 PoC 資料，詳見圖 7。

輸入資料類型	輸入資料	使用演算法	PoC情境
時間相關	登入時間	異常檢測演算法 Isolation Forest	• 正常上下班類型 • 夜晚工作類型 • 隨機工作類型
位置相關	IP位址	分群演算法 Gaussian Mixture Modeling	• 98%為內網IP • 60%為內網IP
設備類型相關	OS+Browser	密度估計演算法 Kernel Density Estimation	• 98%為Windows+Chrome • 50%為Windows+IE，其餘組合平均

資料來源：本報告整理

圖7　PoC 情境

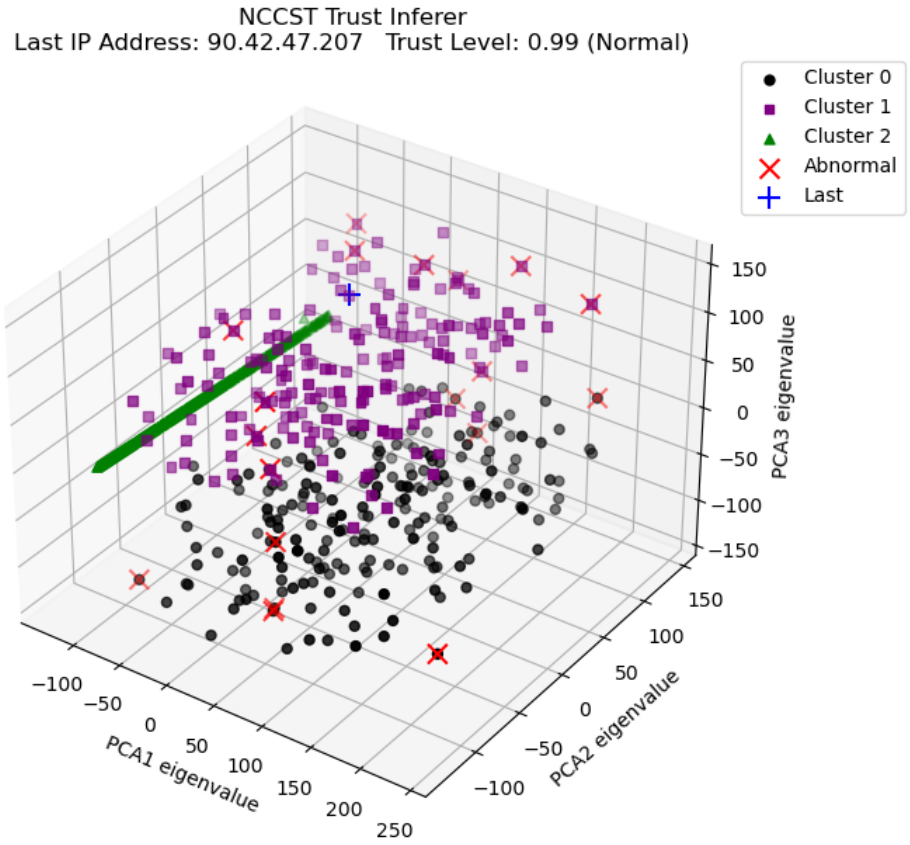
針對「登入時間」之 POC 驗證，基於登入時間(0~86399)之離群程度，使用 Isolation Forest 演算法分析離群程度，計算信任等級，針對離群程度較大者，則列入異常值判斷。以正常上下班類型情境為例，設定離群門檻為 3%，其驗證結果詳見圖 8。



資料來源：本報告整理

圖8　登入時間信任推斷之 POC 驗證結果

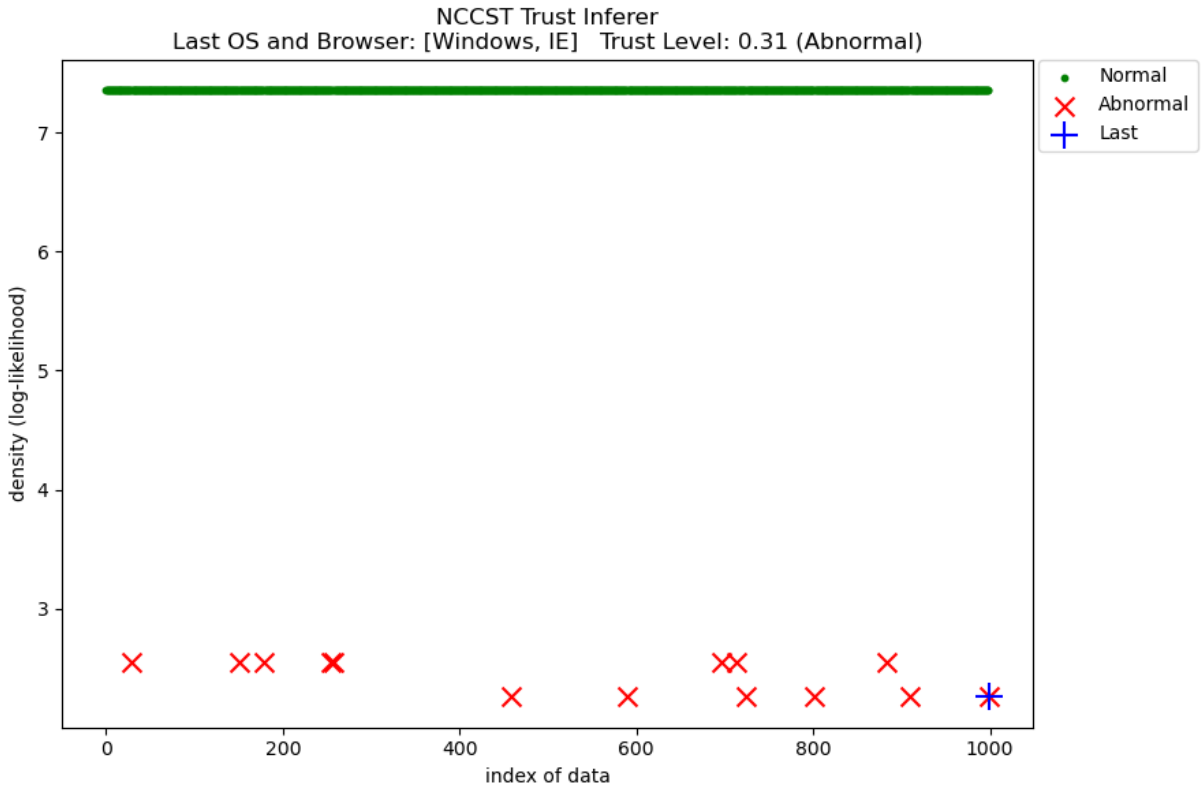
針對「IP 位址」之 POC 驗證，基於 IPv4 之 4 組位元組使用 Gaussian Mixture Modeling 演算法進行分群(Clustering)，決定最佳分群數目，逐步消除權重接近 0 之分群，再將所有 IP 分群，以估計 IP 密度。若同一群中與其他值差異較大者，則判斷為異常值。以 60%為內網 IP 情境為例，其最佳分群數為 3 群，如以 3%設定為異常密度門檻，可篩選出離群之異常 IP 並決定計算信任等級，其驗證結果詳見圖 9。



資料來源：本報告整理

圖9　IP 位址信任推斷之 POC 驗證結果

針對使用者裝置「OS+Browser」之 POC 驗證，使用 Kernel Density Estimation (KDE)演算法進行密度評估，決定異常密度門檻，密度值較低者，則判定為異常值。以 98%為 Windows+Chrome 情境為例，設定 1%為異常密度門檻並計算信任等級，其驗證結果詳見圖 10。



資料來源：本報告整理

圖10 OS+Browser 信任推斷之 POC 驗證結果

依上述研析結果進行概念性驗證，驗證顯示以機器學習進行信任推斷之結果大致上符合預期，惟過程中仍發現少數特殊案例之信任推斷尚需進行改善與調整。政府機關導入零信任網路採取逐步推動與整合過程，而非一次大規模地替換基礎架構，相關組件之部署需具備與現有系統同時混合運作之能力。後續將持續研析並完善零信任網路智慧信任推斷概念性驗證，精進信任演算法動態計算信任分數，以支援存取決策之準確性。

3.資安技術研析_Dirty Pipe 弱點研析與驗證實作

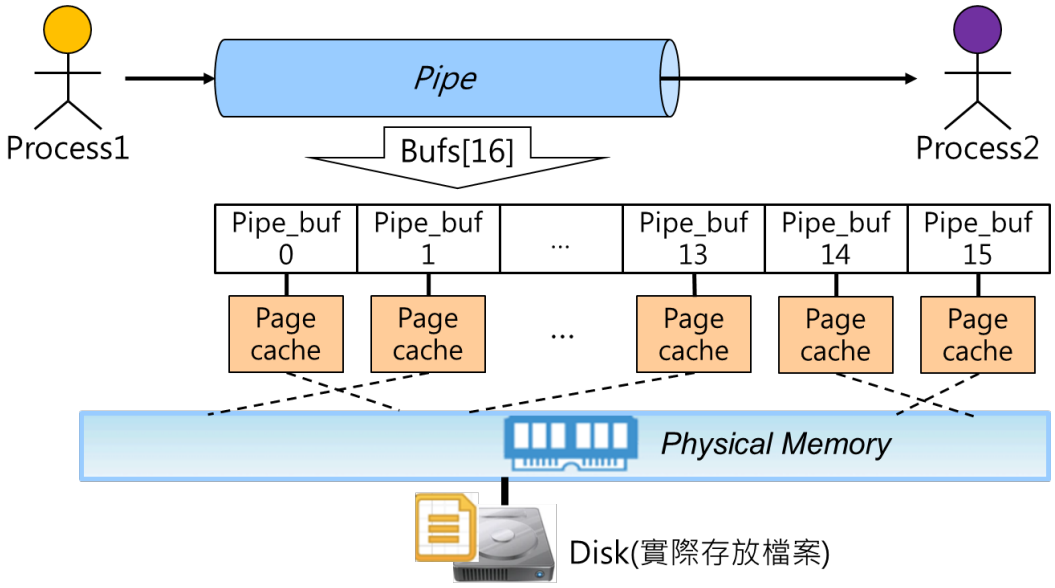
本季探討之資安技術研析為 Dirty Pipe 弱點研析與驗證實作，Dirty Pipe 弱點揭露主因為網路服務託管公司 CM4all 之軟體工程師(Max Kellermann)於處理客戶反應之日誌壓縮檔損毀問題時，發現雖可成功將日誌檔解壓縮，但 Gzip 卻出現循環冗餘校驗(Cyclic Redundancy Check, CRC)錯誤，且經過多次嘗試手動修補該文件之 CRC 後，同樣問題仍不斷發生，而在陸續測試排除硬體、應用程式及網路服務問題後，從而發現此弱點(CVE-2022-0847)。

此弱點與 Linux 核心(Kernel)相關，影響版本涵蓋 Linux Kernel 從 5.8 以上至 5.10.102/5.15.25/5.16.11 版本以下，該弱點允許駭客覆寫任何唯讀檔案，使非特權之行程可注入程式碼至具有根(Root)權限之程序(Processes)，最終擴權取得 Root 權限。弱點觸發過程中，因管線(Pipe)機制產生 Dirty Page 情形，亦即同一個檔案於快取記憶體中之內容，與硬碟中內容不一致，故又命為 Dirty Pipe 弱點。以下將概述 Dirty Pipe 弱點成因與利用方式，並進行弱點攻擊驗證實作。

3.1 Dirty Pipe 弱點成因與利用方式概述

在作業系統中，一般檔案 I/O 之流程，從檔案讀入至輸出介面會歷經數次使用者空間(User Space)與核心空間(Kernel Space)間之切換與快取記憶體(Cache)之讀寫，近年來為提升系統效能，發展出零複製(Zero Copy)相關技術，以減少 User Space 與 Kernel Space 間之切換及 Cache 之讀寫次數。Dirty Pipe 弱點是存在於 Zero Copy 類型之拼接(Splice)技術中，該技術運用 Pipe 機制，僅將檔案描述符(File Descriptor, fd)複製到 Pipe 緩充區(Buffer)，並未真實複製檔案內容，以藉此提升效能。一般而言，Pipe 可用來連接程式 A 到程式 B 兩端點程式，將程式 A 之輸出做為程式 B 之輸入使用，Pipe Buffer 則為一組環狀結構，共有 16 個 Pipe_buf，每個 Pipe_buf

各自有 1 個 Page Cache，詳見圖 11。



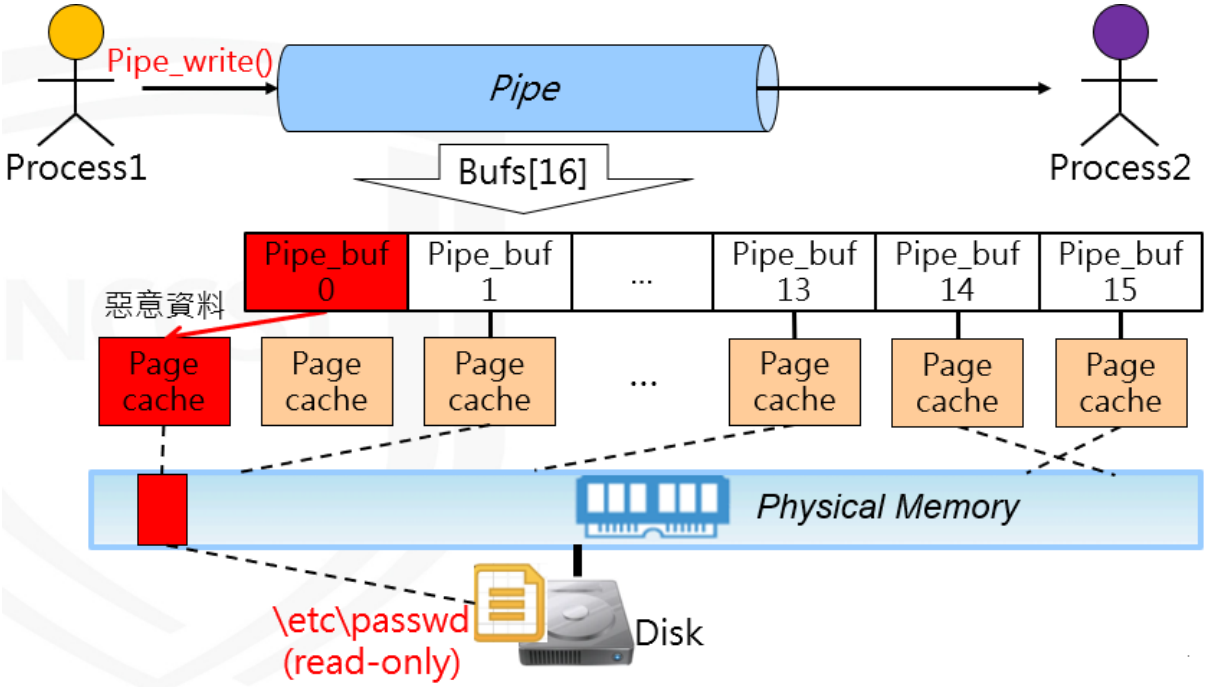
資料來源：本報告整理

圖11 Pipe_Buffer 結構示意圖

為提升 Pipe Buffer 使用效率，Pipe 可設定旗標(Flag)參數 PIPE_BUF_FLAG_CAN_MERGE，此參數之作用為當使用 Pipe_write()函數寫入資料到 Pipe_buf 時，若該 Pipe_buf 已有資料，且剩餘空間足夠容納要寫入之資料，就進行寫入(而非從下一個空的 Pipe_buf 寫入)，以充分利用空間。而本次形成 Dirty Pipe 弱點之主要根因即為 Splice 函數不當使用 PIPE_BUF_FLAG_CAN_MERGE 參數，範例簡述如下。

當使用一般 I/O 方式讀取一個唯讀(read-only)檔案(如/etc/passwd)時，系統將複製一份至 Page Cache，接續使用 Splice 函數讀取相同檔案進入 Pipe 時，Splice 函數將使用 copy_page_to_iter_pipe 函數將 Pipe_buf 指向存放該檔案之 Page Cache。檢視 copy_page_to_iter_pipe 函數原始碼，發現其複製資料前，未將 Flag 重置，使得 PIPE_BUF_FLAG_CAN_MERGE 參數仍存在。此時，若使用 Pipe_write()函數寫入惡意資料到 Pipe_buf 0 時，只要 Pipe_buf 0 指向之 Page Cache 空間足夠，即可寫入且成功竄改存放於 Page

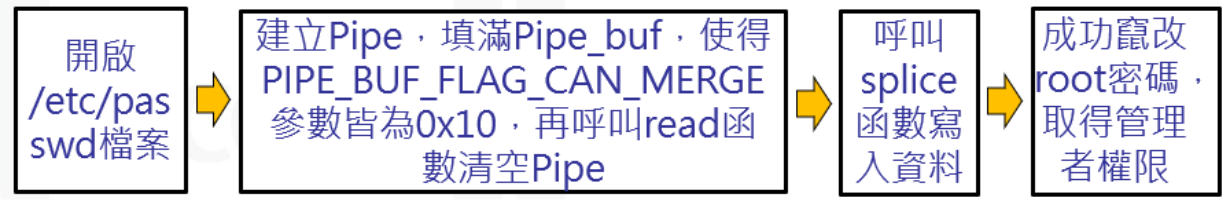
Cache 之檔案副本，且因\etc\passwd 為 read-only 格式，致惡意資料不會寫回 Disk。同時又因重新開機後即可恢復，駭客可輕易清除惡意資料，使竄改資料行為難以被發現，詳見圖 12。



資料來源：本報告整理

圖12 成功寫入且竄改存放於 Page Cache 之檔案副本

於成功竄改存放於 Page Cache 之檔案副本後，下一階段則為利用 Dirty Pipe 弱點，弱點利用流程，詳見圖 13。



資料來源：本報告整理

圖13 提權取得 Root 權限

藉由竄改 Root 密碼，成功取得管理者權限，惡意人士執行 su 指令取得 Root 權限後，即可新增帳號做為後續攻擊之用。詳見圖 14。

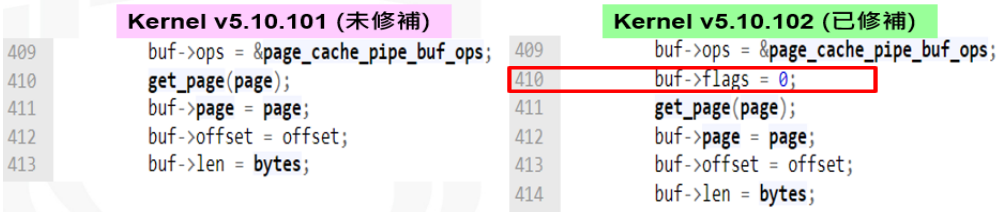
原內容	x代表密碼存在/etc/shadow root:x:0:0:root:/root:/bin/bash
竄改後內容	root:1aaron$pIwpJwMMcozsUxAtRa85w.:0:0:test:/root:/bin/sh 註： • 產生此串密碼指令為：openssl passwd -1 -salt aaron aaron • $1：代表使用MD5加密演算法 • $aaron：代表密碼明文是aaron • $pIwpJwMMcozsUxAtRa85w.：代表加密後之密碼是 pIwpJwMMcozsUxAtRa85w.
格式	使用者名稱:密碼:UID:GID:使用者資訊:HOME目錄路徑:使用者shell

資料來源：本報告整理

圖14 權限遭竄改內容比較

3.2 弱點攻擊流程與驗證實作

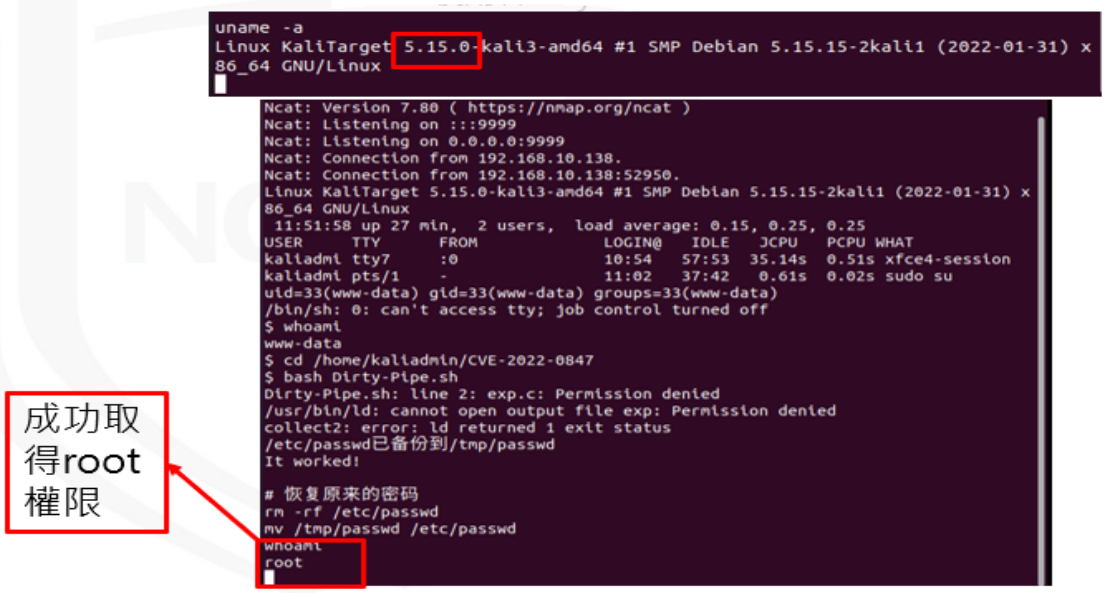
Kellermann 於 111 年 2 月確認 Dirty Pipe 是 Linux Kernal 弱點後，接續完成概念性驗證(Proof of Concept, PoC)，並向 Linux 團隊通報弱點資訊，隨即又發現 Google Pixel 6 亦存在相同弱點，再向 Android 團隊通報弱點資訊。Linux 伺服器為廣受歡迎之作業系統，若相關網站或系統因 Dirty Pipe 弱點遭駭，影響範圍與衝擊將難以評估。而 Dirty Pipe 與 105 年被揭露之 Dirty Cow 弱點為類似之惡意提權行為，沒有其他弱點減緩方式，皆只能透過核心版本升級進行更新修補。Linux 團隊已釋出弱點修補程式，在檢查程式碼後，確認 copy_page_to_iter_pipe()與 push_pipe()函式中各新增 1 行重置 flag 之程式碼(buf->flags=0)，即可成功修補此弱點，詳見圖 15。



資料來源：本報告整理

圖15 弱點成功修補示意

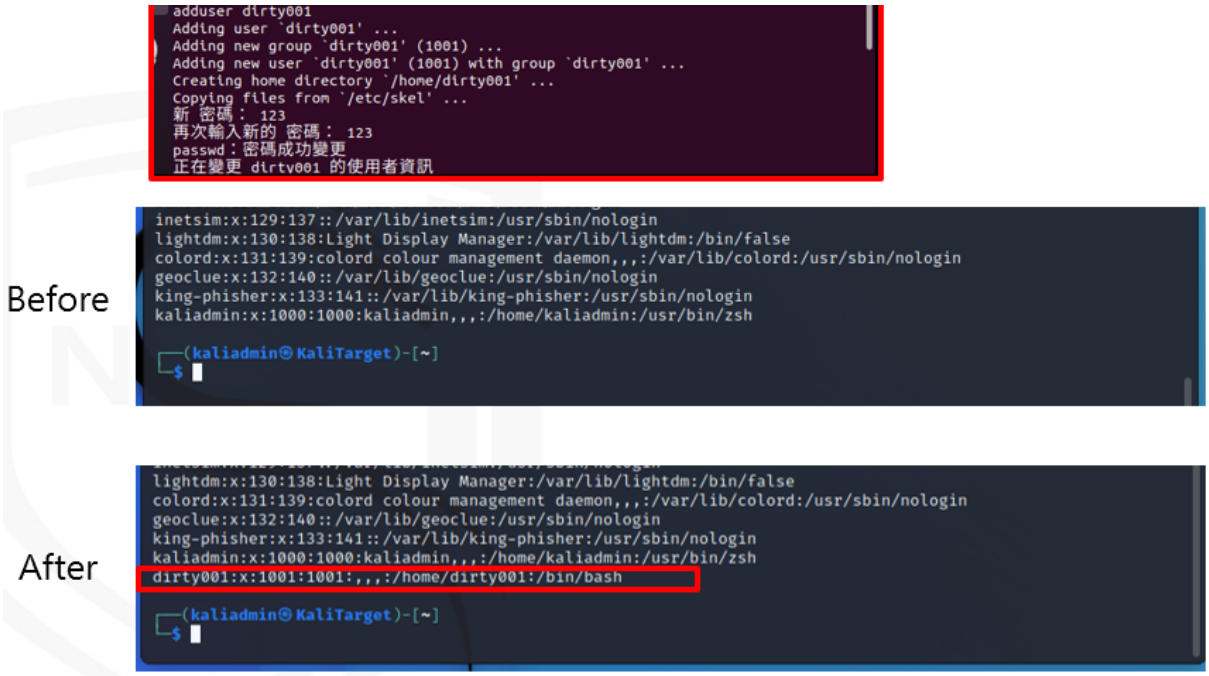
技服中心為了解此弱點與遠端程式碼執行(RCE)弱點結合運用之可行性，進行驗證實作，規劃實作環境為攻擊機與靶機各 1 台，靶機作業系統之核心版本為 Linux Kernel 5.15.0，並架設弱點安全測試之網站系統(Dema Vulnerable Web Application, DVWA)。首先，實作案例使用 DVWA 靶機內之 Php 檔，置換網站內檔案，第二步驟則模擬受駭者點選被置換之 Reverse Shell Php 檔，使靶機向攻擊機報到，接續確認使用未修補之 Linux Kernel 版本，則可執行 Dirty Pipe 弱點攻擊程式成功取得 Root 權限，詳見圖 16。



資料來源：本報告整理

圖16 執行弱點攻擊程式

驗證過程最後展示利用該管理權限，成功新增使用者 dirty001 後，並變更其密碼，詳見圖 17。



資料來源：本報告整理

圖17 駭客可成功新增使用者

本章節分析 Dirty Pipe 弱點根因分析與攻擊驗證實作，旨在提醒該弱點若在未被修補前，不僅容易遭入侵且難以主動偵測，由於影響之 Linux 與 Android 作業系統使用廣泛，受影響之 Linux Kernel 版本建議評估其風險與衝擊後儘速進行修補，並隨時留意重大弱點資訊之公布。此外，Dirty Pipe 弱點雖屬本地提權類型弱點，惟攻擊者可先利用 RCE 弱點(如 CVE-2021-41773 與 CVE-2021-42013)取得一般使用者權限，再搭配利用此弱點取得 Root 權限後進行內部橫向移動，這也揭露傳統只保護邊界之資安防護概念已不足夠，更應加強縱深防禦之層層防範措施，於內部署異常行為分析與日誌監控之管理工具，以主動發現潛在威脅。

4. 結論

本季具指標性案例為資安業者 Sonatype 發現之零時差漏洞 Spring4Shell(CVE-2022-22965)，在原廠緊急推出更新修補程式後，仍發現該漏洞遭駭客大規模用於攻擊活動中，SpringShell 漏洞遭揭露後，儼然成為駭客之新目標，如一直活躍於網路之殭屍網路程式 Mirai 藉著 SpringShell 漏洞感染 IoT 裝置展開新一波攻擊活動；另一起案例為醫院專用機器人 Tug 存在 5 項零時差漏洞，Tug 機器人因可於醫院內獨立移動之技術，使得 Cynerio 所發現之 JekyllBot:5 漏洞可能造成極大之風險，且 Cynerio 研究發現入侵此 5 項零時差漏洞，不需高超技術且無需特殊權限或任何使用者互動，就能成功運用這些漏洞。

國內部分，分析政府資安威脅現況，發現政府機關通報事件原因，以「非法入侵」類型為主，排除綜合類型「其他」外，其次分別為「設備問題」與「網頁攻擊」為主要通報類型。針對本季全球與政府所面臨之主要資安威脅，本報告就「零時差漏洞之資安管理」與「軟體安裝之資安管理」提出資安防護建議。

資安專題分享主題為零信任網路智慧信任推斷研析，依據第六期「國家資通安全發展方案」，規劃於 111 年至 113 年逐步導入零信任網路之身分鑑別、設備鑑別及信任推斷機制，專題概述零信任網路智慧信任推斷之研析，並經由概念性驗證，分析機器學習信任推斷結果，計算信任等級判斷存取准駁，以提升存取政策之可信賴度。

另外，資安技術研析主題為 Dirty Pipe 弱點研析與驗證實作，此弱點與 Linux 核心(Kernel)相關，影響版本涵蓋 Linux Kernel 從 5.8 以上至 5.10.102/5.15.25/5.16.11 版本以下，該弱點允許駭客覆寫任何唯讀檔案，使非特權之行程可注入程式碼至具有根(Root)權限之程序(Processes)，最終擴權取得 Root 權限。技術研析除說明 Dirty Pipe 弱點成因與利用方式，並進行弱點攻擊驗證實作。

資安相關活動

本季行政院資通安全處辦理之資安相關活動，說明如下。

◆ 國家層級資安聯防機制研商會議

111 年度國家層級資安聯防機制研商會議於 4 月 27 日採線上會議方式辦理，會議重點聚焦於 N-CERT、N-ISAC 及 N-SOC 之推動規劃與改版說明。

現行國家資安聯防體系以國家層級 CIS、領域 CIS 及 CI 提供者三大層級分層管理，形成資安聯防與合作網路。依據「國家資通安全發展方案(110-113 年)」，111 年起開始推動各 CI 領域交換格式調整為 STIX 2.1，自 112 年 1 月 1 日起，N-CERT、N-ISAC 及 N-SOC 均將採用新版交換格式。

新版交換格式提供視覺化模組，直接以物件描述網路觀測相關資訊，就效能上採用 JSON 格式，資料結構體積小，傳輸速度亦較快。同時，能以多個物件詳細描述攻擊手法，且與 MITRE ATT&CK 相容，透過關聯化物件，可回饋加值資訊於同一筆情資。

本次會議期透過 N-CERT、N-ISAC 及 N-SOC 之推動規劃與改版作業讓各領域落實事件通報，並持續推動資安情資、資安事件訊息分享及領域監控情資收容。