0

# 資通安全網路月報

## 一、近期資安事件分享

### 資料庫連線池耗盡導致服務效能異常事件說明

機關提供全國各級機關人員使用之共同性系統，發生服務效能異常，使用者於登入及操作時出現明顯延遲。經查，起因於該系統上線後資料量持續增長，但資料庫的搜尋語法並未隨之最佳化，導致查詢資料極度耗時且佔用資料庫連線，當較多使用者同時上線操作時，資料庫連線數(Connection Pool)被全數耗盡進而影響效能。機關立即聯繫維護廠商，調高資料庫連線數上限，並緊急安排人員修改資料庫搜尋語法與效能，始逐步降低整體服務延遲時間，恢復系統運作。

### 經驗學習(Lessons Learned)

系統於長期運作過程中，隨資料量與使用人數持續成長，若未同步檢視與調整系統效能設計，可能因資源使用效率下降而影響整體服務穩定性。建議機關於系統上線後，應建立持續性的效能監控與定期檢視機制、定期辦理容量與效能評估、將效能測試納入維運流程，以及系統變更時同步檢視效能設計：

1. 建立持續性效能監控機制，系統上線後應持續監控服務效能與資源使用情形，如登入回應時間、資料庫連線使用率及系統負載，並設定告警門

檻，以即早發現效能下降徵兆，避免問題累積影響服務運作。

2. 定期辦理容量與效能評估，隨系統使用人數與資料筆數成長，應定期評估系統承載能力與資源配置，例如檢視尖峰登入人數與資料成長趨勢，並透過壓力測試模擬較高使用量情境(如同時登入人數提升至既有規模的兩倍)，提前確認系統是否仍具備足夠處理能力，以避免於實際高使用期間發生服務壅塞。

3. 將效能測試納入維運流程，例如定期檢視執行時間過長的資料查詢並強化效能，或建立效能檢查清單作為改版前必要程序。

4. 於系統變更時同步檢視效能設計，當系統新增功能、改版或資料量增加時，應同步檢視資料存取與查詢方式，例如避免一次載入過多歷史資料、改採分頁查詢機制，或依需求建立資料庫索引以提升搜尋效率。

## 二、資通安全趨勢

### (一) 我國政府整體資安威脅趨勢

**事前聯防監控**

本月蒐整政府機關資安聯防情資共 6 萬 0,764 件(減少 1 萬 1,979 件)，分析可辨識的威脅種類，第 1 名為資訊蒐集類(54%)，主要是透過掃描、探測及社交工程等攻擊手法取得資訊；其次為入侵嘗試類(18%)，主要係嘗試入侵未經授權的主機；以及入侵攻擊類(15%)，大多是系統遭未

經授權存取或取得系統/使用者權限。統計近 1 年情資數量分布，詳見圖 1。

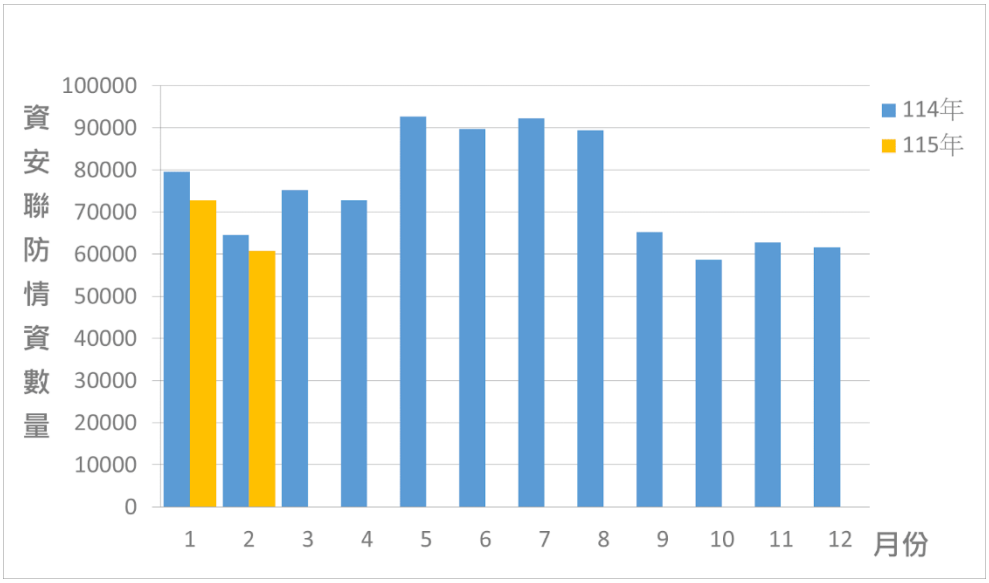


圖 1 資安聯防監控資安監控情資統計

## 駭客偽冒行政院法規會發動社交工程郵件攻擊之資安警訊

經彙整分析聯防情資資訊，發現近期駭客偽冒行政院法規會名義並以「修正就業安定基金收支保管及運用辦法第 5 條條文」為由，針對政府機關與國營企業發動社交工程電子郵件攻擊。駭客利用民間企業之域名，並偽冒行政院(executive-yuan)作為寄件者帳號，於寄件人名稱與信件內容中署名「行政院法規會」，以提升郵件可信度，誘導收件者點擊釣魚連結並下載惡意附檔，查閱所謂「條文修正內容」等相關資料，進而植入惡意後門程式(Cobalt Strike)以達成遠端控制收件者電腦之目的，相關情資已提供各機關聯防監控防護建議。

### 事中通報應變

本月資安事件通報數量共 54 件，為去年同期的 0.9 倍，通報類型以非法入侵為主，占本月通報件數 72.22%。本月除偵測到疑似駭客利用路由器散佈 PeerBlight 惡意程式情形外，亦持續發現多個機關因安裝冒牌軟體而遭植入惡意程式之情事，占總通報件數 25.93%。近 1 年資安事件通報統計詳見圖 2。

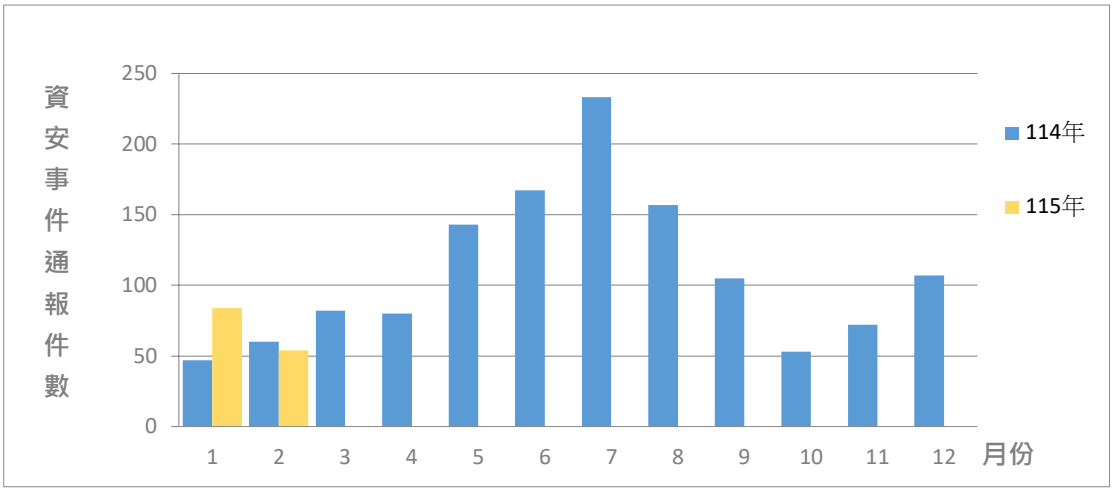


圖 2 資安事件通報統計

## (二) 重要漏洞警訊

| 警訊 | 類別 | 內容說明 |
|---|---|---|
| 漏洞警訊 | 電子目錄服務系統<br>葳橋資訊單一簽入暨<br>電子目錄服務系統<br>嚴重程度：CVSS 8.8 | ● 研究人員發現葳橋資訊單一簽入暨電子目錄服務系統存在作業系統指令注入(OS Command Injection)漏洞(CVE-2026-1427 與 CVE-2026-1428)。 |

| 警訊 | 類別 | 內容說明 |
| --- | --- | --- |
| | (CVE-2026-1427 與 CVE-2026-1428) | ● 已通過身分鑑別之遠端攻擊者可注入任意作業系統指令並於設備上執行，請更新至電子目錄服務系統(V4)至 IFTOP_P4_181(含)以後版本。<br>● 請使用者儘速連繫葳橋資訊技術支援團隊，取得適用之修正版本，並完成系統升級。 |
| | 電子郵件系統<br>C&Cm@il 郵件協同系統<br>嚴重程度：<br>(CVE-2026-2234 : CVSS 9.1)、(CVE-2026-2235 : CVSS 6.5 )及( CVE-2026-2236 : CVSS 7.5 ) | ● 研究人員發現桓基科技 C&Cm@il 存在 3 個高風險安全漏洞(CVE-2026-2234、CVE-2026-2235 及 CVE-2026-2236)。<br>● 類型包含缺乏身分鑑別(Missing Authentication)與 SQL 注入(SQL Injection)，最嚴重可使未經身分鑑別之遠端攻擊者讀取與修改任意使用者信件內容。<br>● 官方已提供安全公告，請參考官方說明儘速確認並採取相關緩解措施。 |
| | 流程管理系統<br>AgentFlow | ● 研究人員發現華苓科技開發的 Agentflow 存在多項安全漏洞（CVE-2026-2095 ~ |

| 警訊 | 類別 | 內容說明 |
| --- | --- | --- |
| | 嚴重程度：<br>( CVE-2026-2095：CVSS 9.8 )、( CVE-2026-2096：CVSS 9.8 )、( CVE-2026-2097：CVSS 8.8 )、( CVE-2026-2098：CVSS 6.1 )、( CVE-2026-2099：CVSS 5.4 ) | 2099 )。<br>● 類型包含身分鑑別繞過與不安全的反序列化，遠端未經身分鑑別之攻擊者可藉此登入系統或執行任意程式碼 (RCE)，威脅等級評定為極高 (CVSS 9.8)。<br>● 請使用者儘速連繫華苓科技技術支援團隊，取得適用之修正版本，完成系統更新或採取應對緩解措施。 |
| 已知遭駭客利用之漏洞 | 通訊設備<br>Cisco Catalyst SD-WAN<br>嚴重程度：CVSS 10.0<br>(CVE-2026-20127) | ● 研究人員發現 Cisco Catalyst SD-WAN Controller and Manager 軟體存在極嚴重之身分驗證繞過漏洞。<br>● 未經身分鑑別之遠端攻擊者可發送特製請求，繞過驗證程序並取得管理權限，進而完全控制設備。<br>● 官方已提供安全建議，請參考官方說明進行軟體版本更新。 |

| 警訊 | 類別 | 內容說明 |
| --- | --- | --- |
| | 文書處理軟體<br>Microsoft Office<br>嚴重程度：CVSS 7.8<br>(CVE-2026-21509) | ● 研究人員發現 Microsoft Office 存在安全功能繞過(Security Feature Bypass)漏洞(CVE-2026-21509)。<br>● 未經身分鑑別之攻擊者可透過發送惡意 Office 文件並誘使用戶開啟，進而繞過元件物件模型(Component Object Model, COM)與物件連結與嵌入(Object Linking and Embedding, OLE)防護機制，使原本應該被阻擋之 COM/OLE 控制元件仍能執行。<br>● 官方已針對漏洞釋出修復更新，請參考官方說明進行更新 |
| | 網頁瀏覽器<br>Chromium 為基礎之瀏覽器<br>嚴重程度：CVSS 8.8<br>(CVE-2026-2441) | ● 研究人員發現 Google Chrome、Microsoft Edge、Vivaldi、Brave 及 Opera 等以 Chromium 為基礎之瀏覽器存在使用釋放後記憶體(Use After Free)漏洞(CVE-2026-2441)。<br>● 未經身分鑑別之遠端攻擊者可利用特製 |

| 警訊 | 類別 | 內容說明 |
| --- | --- | --- |
| | | HTML 頁面觸發記憶體錯誤，進而於瀏覽器沙箱環境執行任意程式碼。<br>● 建議管理人員儘速針對受影響服務進行安全更新。 |
| | 網路安全設備<br>Fortinet 多項產品<br>嚴重程度：9.8<br>(CVE-2026-24858) | ● 研究人員發現 Fortinet 多項產品存在身分鑑別繞過(Authentication Bypass)漏洞(CVE-2026-24858)。<br>● 設備啟用 FortiCloud SSO 之情況下，擁有 FortiCloud 帳號且已註冊設備之遠端攻擊者可登入任意他人帳號註冊之設備，請儘速確認並進行修補。<br>● 官方已針對漏洞釋出修復更新，請參考官方說明進行更新。 |

警訊說明：

「漏洞警訊」：為已驗證漏洞但尚未遭攻擊者大量利用，修補速度建議儘快安排更新。

「已知遭駭客利用之漏洞」：已知有漏洞成功攻擊情形，建議即刻評估修補

## 三、國際資安新聞

### 攻擊者透過偽造 PDF 誘餌竊取 Dropbox 登入訊息

(資料來源：Dark Reading)

根據 Forcepoint 的研究報告指出，近期針對企業的網路釣魚攻擊活動呈現上升趨勢。攻擊者採用複雜的多階段混淆技術，試圖誘騙受害者輸入 Dropbox 帳號憑證並加以竊取。在此攻擊活動中，攻擊者會利用偽造或遭入侵的內部電子郵件帳號發送郵件，誘導目標使用者查看一份偽造的「訂單請求」。郵件內附帶一個連結至 PDF 文件的連結。當使用者點擊後，會先被導向一個託管於合法雲端服務平台 Vercel 的模糊化 PDF 文件，接著再被重新導向至一個外觀與官方頁面極為相似的偽造 Dropbox 登入頁面。在該頁面中，受害者會被要求輸入其工作帳號與密碼。實際上，這些憑證在頁面顯示「使用者名稱或密碼錯誤」提示之前就已被攻擊者竊取。隨後，竊得的憑證與相關使用者資訊會透過 Telegram 機器人即時傳送給攻擊者，使其能夠進一步進行帳戶接管、內部系統存取，甚至發動後續詐欺行為。為降低此類攻擊風險，建議使用者遵循反釣魚安全最佳實務，例如對來源不明的電子郵件與 PDF 附件保持警覺，並在開啟或點擊連結前仔細確認其真實性。

## 微軟：Windows Admin Center 嚴重漏洞導致權限提升

**(資料來源：Tech Republic)**

微軟警告，Windows Admin Center（WAC） 存在一項高風險安全漏洞 CVE-2026-26119（CVSS 評分：8.8），可能在企業環境中被利用以進行

權限提升攻擊。該漏洞源於身分驗證機制處理不當，使具備合法存取權限的攻擊者在無需使用者互動的情況下，即可透過網路提升其權限。若成功利用此漏洞，攻擊者可能取得管理員層級控制權，進而修改系統設定、建立或變更特權帳戶、停用安全防護機制、存取敏感資料，甚至在企業網路中進行橫向移動。由於 Windows Admin Center 為集中式伺服器與基礎架構管理平台，一旦遭到利用，可能影響多台受管理主機，進一步放大整體安全風險。目前該漏洞影響 Windows Admin Center 2.6.4 版本。截至目前為止，尚未有公開資訊顯示此漏洞已遭到實際利用。組織應透過以下方式降低風險：修補到最新版本、強制執行最小權限原則、實施多因素身份驗證、限制網路暴露、加強主機系統、啟用增強日誌紀錄以及測試事件應變計畫，以降低風險。