115 年 1 月資訊安全宣導

中製 APP 資安風險高
資安院提醒民眾慎選使用，避免個資外洩

隨著行動裝置普及，民眾日常生活高度依賴各類行動應用程式（以下簡稱 APP），然而部分中國製 APP 存在多項資安高風險行為，可能危害使用者個人資料與行動裝置安全。國家資通安全研究院特此提出警示，呼籲民眾提高資安意識，下載或使用 APP 時，密切注意 APP 對資料蒐集與權限要求的合理性。

我國國安局、法務部調查局及警政署刑事局，依數發部發布之「行動應用 APP 基本資安檢測基準 v4.0」指標，對小紅書、微博、抖音、微信及百度雲盤等中國 APP 進行檢測，發現皆出現多項高風險行為，類型包含「蒐集敏感性資訊」、「讀取儲存空間」、「逾越 APP 使用功能之權限」、「擷取系統資訊」、「掌握生物特徵」以及「數據回傳與分享」等 6 大面向，顯示中製 APP 在資安防護上仍有重大疑慮。

依國安局的檢測結果，本院分析上述 APP 可能的資安風險與影響如下：

一、蒐集敏感性資訊

風險行為：APP 會蒐集手機或行動裝置所在位置、通訊錄、通訊對象、剪貼簿內容與截圖。

可能影響：例如民眾在家中查詢附近醫療院所資訊時，APP 可能會記錄其所在地與搜尋內容，了解其健康狀況；此外，使用者在複製信用卡號準備付款時，剪貼簿內容也可能遭 APP 擷取。

二、讀取儲存內容

風險行為：APP 可存取手機或行動裝置內部照片、文件等私人資料，造成隱私外洩。

可能影響：例如個人手機中的家庭合照、工作簡報、甚至病歷報告與財務報告，被 APP 讀取並回傳至遠端伺服器進行分析與利用。

三、逾越 APP 使用功能之權限

風險行為：APP 過度要求使用者填寫個資、要求不必要權限、強迫同意不合理條款及未保障個資權利。

可能影響：例如民眾下載 APP 僅欲觀看影片、星象算命等等，卻被要求提

供生日、身分證號、住址、手機、電子郵件等資訊，導致個資暴露於不明風險中。

四、擷取系統資訊

風險行為：APP 可取得並分析使用者手機安裝程式清單與設備參數資訊，進而建立使用習慣檔案。

可能影響：例如民眾手機安裝之銀行 APP、VPN 工具及健康追蹤器等軟體資訊，可能被 APP 讀取並分析，進而推測使用者的財務狀況、健康狀態、個人喜好與網路使用行為。

五、掌握生物特徵

風險行為：臉部資訊屬高度敏感資料，外洩後恐遭偽造身分或進行詐騙。

可能影響：例如個人臉部資料、指紋、聲紋可能被儲存並傳送至境外，未來被用於製作假身分或深偽影音，造成身分盜用與社會信任危機。

六、回傳數據與分享

風險行為：APP 可能於運作時，將手機資料、使用者個資等等，回傳至中國境內伺服器，或分享資料給予第三方。

可能影響：例如 APP 可能在使用者不知情之情況下，自動將聯絡人、位置資訊、裝置參數、使用者登錄各網路平台預存各種個資、帳號密碼等資訊傳送至中國境外伺服器，恐有提供予中國國安、公安或情資部門，使國人個資遭中國政府進一步運用。

上述資安風險與影響可能導致的結果無法預估，假設個人的手機或行動裝置成為資安漏洞，成為中國駭客入侵政府資料庫的中繼站，後果將不堪設想。以美國為例，美國聯邦調查局在 2025 年 6 月向國會提交的報告指出，中國涉嫌偽造大量美國駕照運入美國，可能藉此申請假郵寄選票操縱 2020 年總統大選，這些個資也可能來自資安事件導致的個資外洩，例如 Equifax 2017、T-Mobile(Experian)等事件，遭竊的個資包含姓名、地址、生日、社會安全號碼、駕照號碼等等。此外，美國政府也針對 Equifax 2017 事件，起訴四名中國軍方人員。

基於網路資安與個資安全，資安院建議民眾：

1. 安裝 APP 前，**詳閱權限要求與隱私條款**。
2. 定期檢查手機 APP 權限設定，**關閉不必要的權限**。
3. 優先選用來源可信之 APP，**避免安裝來路不明程式**。

4. **使用資安防護工具**，監控資料傳輸與異常行為。

5. APP 要求提供機敏資訊前，應**評估其合理性與必要性**。

不過，即便 APP 在安裝時並未提示權限要求與隱私條款，但在下列狀況下，也非常不安全：

1. 惡意 APP：某些 APP 在設計上包含惡意程式碼，可能會利用系統漏洞，例如 root、越獄環境等等，進一步存取未授權的資料。

2. 第三方軟體開發套件（SDK）濫用：有些 APP 雖然表面上用途單純，但內部可能使用了來自其他公司的廣告或追蹤模組（又稱軟體開發套件，SDK），這些模組會在使用時偷偷收集裝置 ID、已安裝的 APP 清單等資訊。

3. APP 內建後門或間接推論技術：有些 APP 即使沒有直接存取敏感資料，仍可能透過其他方式推測使用者的行為或個資。例如：APP 不讀通話記錄，但根據民眾使用 APP 的時間、麥克風聲音變化等訊號，間接判斷是否正在通話。

有鑑於此，資安院再次呼籲民眾，面對日益複雜的資安威脅，唯有提高警覺並落實防護，方可有效守護自身資訊安全。請民眾慎選 APP 來源，定期檢查權限設定，避免自身隱私資料洩露造成不必要之風險，也防止國人個資遭到中國政府不當運用。

資料來源：國家資通安全研究院