jamf

Security 360：

年度趨勢報告

行動裝置

目錄

前言

Jamf 的 Security 360 報告深入回顧持續演變的威脅情勢，其內容基於客戶環境中發現的真實事件、資安研究團隊的創新發現，以及來自全球、國家與產業活動的觀察結果。本報告版本聚焦於探討行動裝置威脅情勢，凸顯組織所面臨的各項風險。

本報告探討攻擊者用於取得存取權、橫向移動，並最終竊取或破壞資料，乃至造成損害的各類具影響力之攻擊向量。攻擊者會利用裝置與軟體漏洞、在 App 及網頁通訊中植入惡意程式碼，並威脅組織防禦體系中最薄弱的環節——使用者，以此達成其攻擊目標。

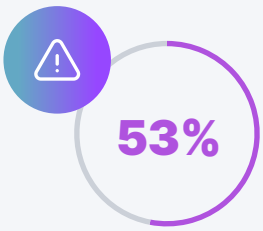
除分析這些威脅趨勢外，本報告亦收錄 Jamf 資安長 (CISO) 的觀點，為負責防護行動裝置群組的資安主管與 IT 從業人員提供實務洞察。

研究方法

為了解並量化本報告所識別之資安趨勢的真實影響，我們匿名分析了客戶環境中超過 170 萬台 iOS 與 Android 裝置樣本。本分析於 2025 年底執行，回顧過去 12 個月的數據，涵蓋全球多個國家與地區。

為在資料蒐集與處理過程中保護隱私並維持最高標準，本研究分析的中繼資料取自彙整後的紀錄檔，當中不含任何個人或組織識別資訊。

關鍵發現



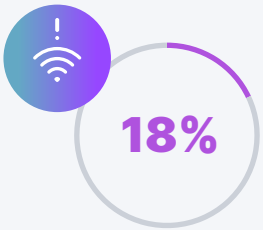
至少有 1 台裝置作業系統嚴重過期的組織比例

過時的作業系統代表存在未修補且可被利用的漏洞。自動化與強制更新是保護裝置的重要手段。

每 850 台中有 1 台

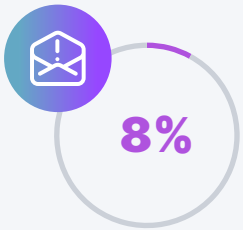
用於工作且已越獄的裝置數量

Jamf 已偵測到這類裝置，情境感知存取政策已阻止其存取公司資源。



有員工連接高風險熱點的組織比例

高風險熱點易導致惡意存取點或中間人攻擊等基礎架構威脅，若裝置未針對此風險進行組態，風險將更為凸顯。



使用者點擊釣魚連結的裝置比例

釣魚攻擊仍是攻擊者入侵帳戶的常用手段，年度變化不大。若缺乏適當防護，後果可能相當嚴重。

零點擊與瀏覽器攻擊

仍是常見且有效的攻擊手法

作業系統與軟體持續出現漏洞，此類漏洞已成為攻擊者透過多種間諜軟體家族竊取敏感資訊的關鍵途徑。本報告強調針對行動裝置進行策略性風險控管的重要性。

企業環境的核心趨勢

行動裝置協助員工在任何地點保持工作效率。行動裝置的管理與使用方式，以及其面臨的威脅，決定了相應的防護策略。

組織每天都在努力縮小攻擊面。您已部署各項控制措施與政策，並在技術堆疊中導入頂尖的安全軟體，但攻擊者仍在持續演進與攻擊。

攻擊面由多個環節組成。本報告將探討組織難以控制、且攻擊者經常利用的主要風險，以及如何避免慘重後果。

1. 軟體與裝置漏洞是營運中無法避免的一環。

儘管行動裝置作業系統的開發過程相當謹慎，但完美無瑕仍是不可能達成的目標。2025 年發布的 CVE 漏洞紀錄超過 48,000 筆。這代表需要識別與修補的漏洞數量極為龐大。

但開發商深知這一點，因此會發布資安修補程式。這正是您的團隊需要介入的環節。您是否有套用這些修補程式？是否持續將作業系統更新至最新版本？是否遵循資安最佳實務？裝置的組態方式至關重要。

攻擊者會利用這些漏洞，導致攻擊面持續擴大。

2. 行動 App 可能是助力，也可能是隱患。

App 是行動工作不可或缺的一環。您的公司可能在裝置群組中部署了數十甚至數百款 App。每款 App 都有其獨特風險。行動惡意軟體相對少見，但隱私、供應鏈及資料處理仍是潛在風險點。

您的 App 也需保持最新版本，其開發商同樣在修補漏洞。App 生命週期管理至關重要，同時也需確保在員工的資安與隱私之間取得平衡。

App 會倍增潛在風險，導致攻擊面擴大。

3. 即使是防護最完備的裝置，也面臨網路與網頁風險的威脅。

無論資料處於靜態儲存或動態傳輸狀態，資料防護都是基本要求。要實現此目標，必須了解網路基礎架構與使用者行為。員工經常連接未受保護的熱點，這類熱點易成為中間人攻擊 (AitM) 的目標。若未經適當組態，您的資料將面臨暴露風險。

釣魚攻擊及其他網頁風險持續猖獗。攻擊者會仿冒多類線上內容的熱門網站，涵蓋娛樂、商務、公用工具及金融領域。使用者每日皆會上當受騙，尤其是生成式 AI 協助攻擊者精進攻擊技術之時。

使用者操作失誤與外部網路帶來不受控的入侵點，導致攻擊面擴大。

4. 風險會相互疊加，進而衍生出進階威脅。

裝置漏洞、App、網路基礎架構及使用者行為，都可能成為資安防禦體系的破口。攻擊面越大，防護難度越高，而這三類風險常被用於目標式攻擊。

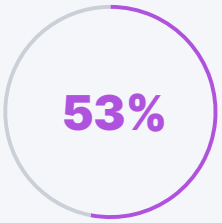
這些風險的擴散可能引發更具危害性的攻擊，例如進階持續性威脅 (APT) 與間諜軟體。2025 年，Jamf Threat Labs 觀察到零點擊與一點擊攻擊的漏洞利用情形仍在持續。高階主管、政治人物、社運人士及記者是重點攻擊目標。

我們調查了 2025 年部分最惡劣的零點擊與一點擊攻擊事件。這類攻擊旨在竊取敏感情報，並利用裝置的多個元件發動攻擊。本報告後續將詳述相關調查結果。

裝置漏洞

行動作業系統是安全防護的基礎，無論其本身是否安全。

裝置作業系統的程式碼庫龐大且複雜。而人非聖賢，漏洞難免會滲入程式碼中。人類同樣聰明——攻擊者總在尋找可被利用的潛在漏洞。



的**組織**至少有一台裝置的
作業系統嚴重過期

何謂 CVE?

常見漏洞和暴露 (CVE) 計畫是由資安社群建立的漏洞資料庫。每筆 CVE 記錄均會標註受影響的軟體或程式庫、提供嚴重性評分，並說明潛在的漏洞利用方式。

以下列舉 2025 年兩個重大案例，兩者均已被確認在真實環境中遭到濫用。這些 CVE 漏洞已在 iOS 18.4.1 中完成修補。

CVE-2025-31200

嚴重性評分：9.8（重大）

處理惡意構造的媒體檔案中的音訊串流，可能導致程式碼執行。

CVE-2025-31201

嚴重性評分：9.8（重大）

具備任意讀寫能力的攻擊者，可能繞過指標驗證機制。

攻擊者可串聯這類漏洞，竊取您的資料並部署間諜軟體。試想以下（大幅簡化的）情境：

高知名度目標收到精心構造的訊息，內含惡意音訊檔案。

行動裝置無需使用者互動，即會處理音訊訊息以進行預覽。

處理過程中的記憶體損毀，使攻擊者獲得任意讀寫能力。

繞過指標驗證機制，使攻擊者能偽造有效的程式碼指標。

攻擊者將程式碼執行導向惡意酬載。

裝置遭到入侵，監控行動隨即展開。

這意味著什麼？

- **這是一場零點擊的目標式攻擊：** 使用者無需點擊任何內容，裝置即可能遭到入侵。攻擊目標通常是記者、政治人物或高階主管等高知名度人士。
- **漏洞會相互疊加：**攻擊者正仔細尋找可利用的漏洞，並且他們善於此道。
- **修補至關重要：**這些漏洞已在 iOS 18.4.1 中修復。若您的裝置未更新，資料將無法獲得保護。

希望這能凸顯保持裝置更新的重要性。但這並不意味著執行起來毫無難度。使用者不願更新裝置的原因有很多：

- 不願使用的新功能/介面
- App 與新版作業系統不相容
- 工作流程中斷/資源限制

如前所述，過期軟體相當普遍，而保持更新是一個持續變動的目標。落實更新期限與最低作業系統版本要求，可保護您的裝置群組免於受到重大漏洞的影響，例如 Jamf Threat Labs 在 2025 年分析的這些案例。

攻擊者利用漏洞，透過圖片與音訊檔案解析、瀏覽器一點擊攻擊等方式，實現零點擊攻擊向量。 儘管供應商已發布資安修補程式並付出努力，攻擊者仍能找到並利用新的漏洞開發攻擊工具，因此定期更新行動裝置，對於保護所有使用者免於漏洞威脅至關重要。 以下回顧 2025 年最具影響力的漏洞。

2025 年值得關注的 iOS 漏洞

CVE-2025-24201 | 嚴重性：10.0（重大）	CVE-2025-43300 | 嚴重性：10.0（重大）	CVE-2025-31201 | 嚴重性：9.8（重大）
描述：		
惡意偽造的網頁內容可能突破網頁內容沙盒限制。	處理惡意圖片檔案可能導致記憶體損毀。	具備任意讀寫能力的攻擊者，可能繞過指標驗證機制。
衝擊：		
此漏洞可在目標緩衝區的結尾之後或開頭之前進行資料越界寫入。這可能導致記憶體損毀，或讓攻擊者修改資料以執行未預期的程式碼。	此漏洞同樣可在目標緩衝區的結尾之後或開頭之前進行資料越界寫入。	此漏洞包含不當的存取控制，允許未經授權存取資安敏感元件。因此，攻擊者可修改與讀取記憶體，並執行未經授權的程式碼。
已修補的作業系統：		
iOS 18.3.2 和 iPadOS 18.3.2	iOS 18.6.2 與 iPadOS 18.6.2	iOS 18.4.1 與 iPadOS 18.4.1

以下表格列出我們確認在 2025 年遭到濫用的其他漏洞。

iOS

已修補的 iOS 版本	日期	漏洞評分	元件
18.3.1	2025 年 2 月	CVE-2025-24200 CVSS 評分：6.1 | 嚴重性：中等	輔助使用
18.3.1	2025 年 2 月	CVE-2025-43200 CVSS 評分：4.2 | 嚴重性：中等	訊息
18.4.1	2025 年 4 月	CVE-2025-31200 CVSS 評分：9.8 | 嚴重性：重大	CoreAudio
26.2	2025 年 12 月	CVE-2025-43529 CVSS 評分：8.8 | 嚴重性：高	WebKit
26.2	2025 年 12 月	CVE-2025-14174 CVSS 評分：8.8 | 嚴重性：高	WebKit

2025 年值得關注的 Android 漏洞

CVE-2025-10585 | 嚴重性：9.8（重大）

描述：

Google Chrome V8 引擎中的類型混淆問題，允許遠端攻擊者透過惡意構造的 HTML 頁面，潛在利用堆積損毀漏洞發動攻擊。

衝擊：

指標或其他資源被宣告為特定類型，但日後存取的是不相容類型的資源。這可能導致記憶體重寫、程式崩潰，甚至可能被用於執行程式碼。

已修補的作業系統：

Chrome 140.0.7339.155

CVE-2025-48543 | 嚴重性：8.8（高）

描述：

因釋放後使用問題，Chrome 沙盒存在多處可能被突破的路徑，以攻擊 Android system_server。這可能導致本機權限提升，且無需額外的執行權限。漏洞利用過程無需使用者互動。

衝擊：

使用已釋放的記憶體可能損毀有效資料。若攻擊者在記憶體合併前植入惡意資料，可能得以執行任意程式碼。

已修補的作業系統：

Android 13、14、15、16

CVE-2024-53104 | 嚴重性：7.8（高）

描述：

媒體：uvcvideo：在 uvc_parse_format 中跳過 UVC_VS_UNDEFINED 類型的畫框解析。由於在 uvc_parse_streaming 計算畫框緩衝區大小時，未將此類型畫框納入考量，可能導致越界寫入。

衝擊：

在目標緩衝區的結尾之後或開頭之前進行資料越界寫入，可能導致記憶體損毀，或讓攻擊者修改資料以執行未預期的程式碼。

已修補的作業系統：

上游 Linux 核心，2025 年 2 月

Android

已修補的 ANDROID 版本	日期	漏洞評分	元件
12、12L、13、14、15	2025 年 3 月	CVE-2024-43093 CVSS 評分：7.3 | 嚴重性：高	架構
安全公告*	2025 年 3 月	CVE-2024-50302 CVSS 評分：5.5 | 嚴重性：中等	核心
安全公告	2025 年 9 月	CVE-2025-38352 CVSS 評分：7.4 | 嚴重性：高	核心

*Android 不為核心更新發布作業系統版本。如需詳情，請參閱對應的 Android 安全公告。

Chrome

已修補的 CHROME 版本	日期	漏洞評分
136.0.7103.125	2025 年 5 月	CVE-2025-4664 CVSS 評分：4.3 | 嚴重性：中等
137.0.7151.72	2025 年 6 月	CVE-2025-5419 CVSS 評分：8.8 | 嚴重性：高
138.0.7204.63	2025 年 6 月	CVE-2025-6554 CVSS 評分：8.1 | 嚴重性：高
138.0.7204.157	2025 年 7 月	CVE-2025-6558 CVSS 評分：8.8 | 嚴重性：高
142.0.7444.175*	2025 年 12 月	CVE-2025-13223 CVSS 評分：8.8 | 嚴重性：高
143.0.7499.109	2025 年 12 月	CVE-2025-14174 CVSS 評分：8.8 | 嚴重性：高

* 標註版本對應桌面版 Chrome。

裝置的組態方式至關重要。

現代行動作業系統具備眾多強大功能，其中部分在五年前仍是難以想像的。俗話說得好，能力越大，責任越大……

（希望）您已將裝置註冊至行動裝置管理 (MDM) 系統，以確保其組態恰當。裝置需在可用性/生產力、資安與使用者隱私之間取得平衡——因此合適的資安並非總是顯而易見。

儘管這會因組織的風險屬性與產業而異，但部分標準功能與設定會帶來高風險，因此應加以限制：

- 越獄裝置會規避 Apple 的資安限制，允許使用者以不安全或不穩定的方式修改裝置。每台越獄裝置都可能成為攻擊者入侵您系統的潛在後門。
- 替代 App Marketplace 允許使用者在 App Store 或 Google Play 以外的管道安裝 App。替代 App Marketplace 不受相同的資安與隱私要求約束，增加了惡意或有問題 App 的風險。

然而，儘管存在這些風險，JAMF THREAT LABS 仍發現：

每 850 台中有 1 台
用於工作的裝置已越獄

2%
的組織擁有安裝替代 App Marketplace 的裝置。

資安長 (CISO) 的觀點

以下整體解決方案可緩解行動裝置面臨的最常見威脅，包括間諜軟體、遭入侵或惡意的應用程式，以及未修補的應用程式——這些威脅都可能在使用者不知情的情況下，暗中暴露敏感的公司資料。

- **確保所有行動裝置均已註冊至 MDM**，執行經核可的作業系統版本與更新，並符合資安基準。任何不符合規範的裝置，應自動隔離於公司資源之外，直至問題得到修復。建立穩健的架構來管理裝置及其使用者，對於防患於未然、遏止惡意軟體爆發至關重要。
- **部署基於代理程式的資安解決方案**，監控越獄行為、惡意行為及作業系統層級威脅。確保遙測數據持續傳送至您的 SIEM，使資安營運中心 (SOC) 能一併掌握行動威脅與其餘環境狀況。
- **啟用 DNS 過濾與釣魚防護功能**，覆蓋所有裝置上的所有 App，而非僅限電子郵件。這應包括惡意 Wi-Fi 與中間人攻擊的偵測。

應用程式風險

行動 App 是員工完成工作的重要工具。您的組織部署了多少款行動 App？這些 App 無論是第三方開發或內部自製，都是敏感資料的入口。

<1%

的組織受**行動惡意軟體影響。**

行動惡意軟體並不常見。它確實存在，但規模不及電腦端。這主要歸功於主流行動作業系統採用的現代架構，其中沙盒機制與受管控的 App Marketplace 降低了惡意內容進入裝置的風險。

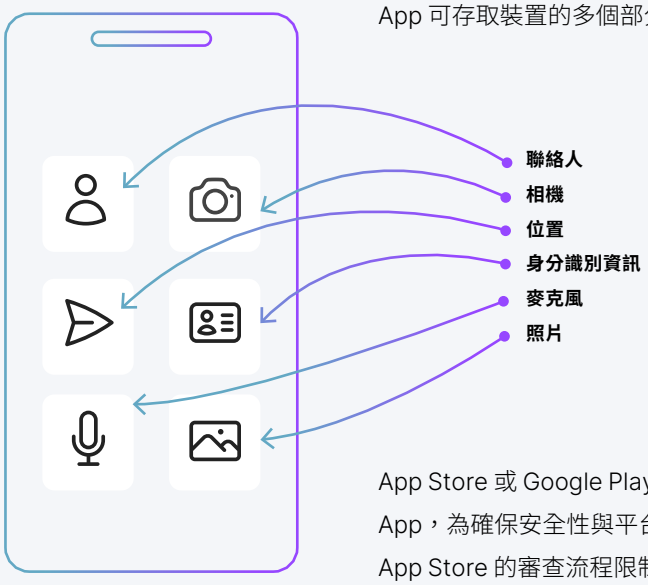
儘管如此，App 仍會擴大您的攻擊面。需考量：

- **App 如何處理資料儲存與傳輸**
- **App 收集哪些資料及其隱私政策內容**
- **供應鏈考量，例如 App 所依賴的程式庫**

惡意行為者利用 App 漏洞部署進階持續性威脅 (APT) 與間諜軟體，因此深入了解您的 App 至關重要。此外，App 透過網路傳輸資料的方式也可能帶來風險——後續將詳述。

App 的隱私政策決定了資料處理方式。

App 可存取裝置的多個部分，其中部分較為敏感：



App Store 或 Google Play 上的 App 必須揭露所收集的所有資料。所有替代市集與散佈的 App，為確保安全性與平台完整性，均需經過 Apple 的公證流程，但其核准流程相較於官方 App Store 的審查流程限制較少。

資安與隱私以兼顧。

無論您是提供行動裝置給員工，還是允許他們自帶裝置 (BYOD)，授予其存取公司資源與資料的權限時，都需優先考量資安與隱私。重視資安，是因為您需要保護資料。重視隱私，是因為您需要保護使用者。

取得兩者的平衡可能是一項挑戰。例如：

- 您的**資料外洩防護 (DLP)** 措施可能違反隱私規範。
- 為了資安而**鎖定裝置**可能會影響生產力。
- **不當的政策**可能導致影子 IT 的產生，即使用者為執行特定工作職能而下載未經核可的 App。

為解決這些問題，您的組織可採取以下措施：

- 要求必須註冊至 **MDM** 才能存取公司資源
- 在 BYOD 裝置上透過強化容器或分割區分離個人與公司資料，落實資料外洩防護 (DLP) 政策——透過禁止存取個人資料保護使用者隱私
- 透過加密通道傳送公司網路流量，確保機密性與資料完整性
- 向使用者宣導資安最佳實務與相關政策

補充：
App 資安分析

Jamf 與 NowSecure 合作，針對行動 App 風險展開深入分析，尤其是在企業廣泛部署的 App 方面。我們以 OWASP 標準作為行動 App 風險的基礎評估依據，分析了 135 款最熱門且廣泛散佈的商務與個人行動 App。

所有受分析的 App 均為 2025 年 12 月 31 日時的最新版本，反映了企業在真實環境中面臨的現有 App 風險。

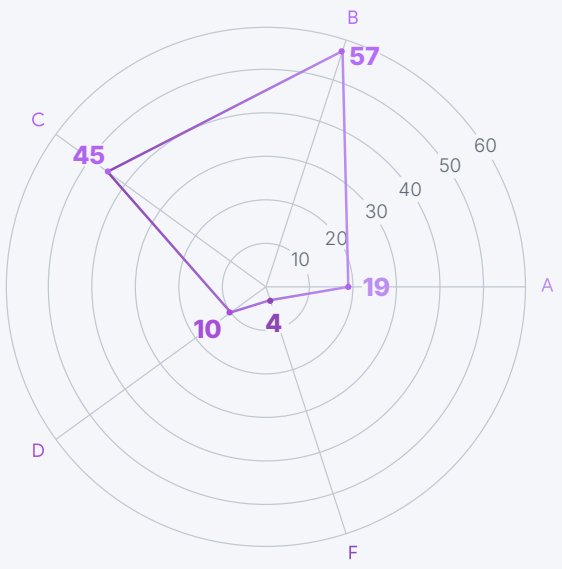
NowSecure 協助組織防範行動 App漏洞與資料外洩，避免其演變成資安、隱私或合規事件。透過持續分析自有及第三方行動 App，並將分析結果納入資安、IT 風險管理流程，NowSecure 為團隊提供大規模管理行動風險所需的能見度、證據與治理能力。

進一步了解 NowSecure。

App 資安評分

NowSecure 提供 0 至 100 分的行動 App 資安評分（評分越高越好），以及 **A**-**F** 的風險等級（**A** = 極低風險，**F** = 重大風險）。這些評分基於自動化測試得出，評估項目包括漏洞、資料外洩、不安全的編碼實務、加密弱點及網路缺陷。

熱門 APP 的資安評分

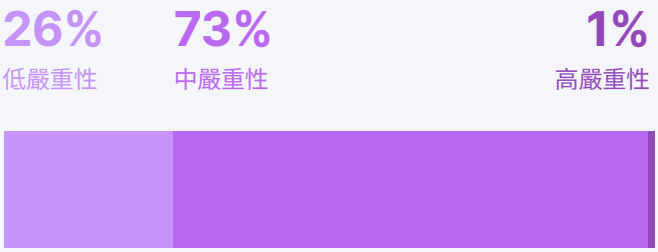


A — F

極低風險 — 顯著風險

在 135 款受分析的 App 中，約 **86%** 存在已知資安漏洞，僅 **14%** 被視為具有極低風險。這意味著風險在日常使用的最常見商務與個人 App 中相當普遍，即使是最新版本亦不例外。

漏洞分佈



在分析中發現的所有漏洞中，大多數屬於中等嚴重性等級。如後續所見，漏洞數量超過受分析的 App 數量——這意味著部分 App 被發現存在多個漏洞。

App 漏洞評估

評估多個漏洞對單一 App 帶來的風險影響至關重要。評估時，**95%** 的 App 至少包含一個中等嚴重性漏洞，而 135 款 App 中有 **2%** 存在高嚴重性漏洞——使其成為攻擊者的理想目標。

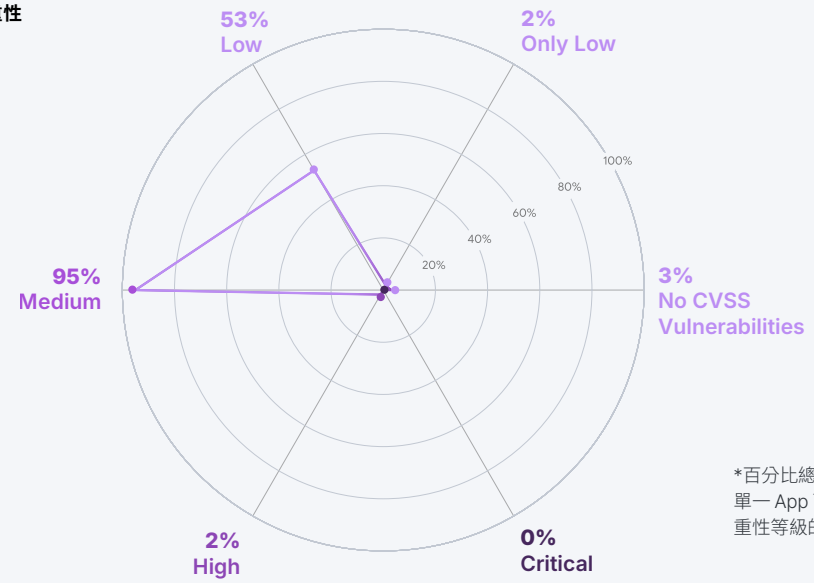
雖然軟體製造商必須修復其應用程式中的漏洞，但企業有責任了解自身面臨的風險，並確保及時更新。關於修補時程，存在不同的建議標準（例如，CISA 建議在首次偵測到重大嚴重性漏洞後 15 個日曆日內修復，高嚴重性漏洞則在首次偵測後 30 個日曆日內修復），但這些數據表明，所有組織都應制定相應計畫，確保 App 保持更新。

如前所述，NowSecure 針對 App 的現行版本進行評估。儘管如此，大多數 App 仍存在多個漏洞。App 風險管理是一項持續且不斷演進的工作，需要持續監控與執行。

但透過以下方式，即可實現有效管理：

1. 持續識別漏洞與隱私問題
2. 根據業務影響優先處理修復工作
3. 透過行動裝置管理控制措施落實政策
4. 長期監控第三方 App 行為

漏洞嚴重性

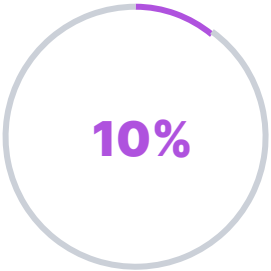


*百分比總和可能超過 100%，原因是單一 App 可能同時存在多個不同嚴重性等級的漏洞。

供應鏈

行動 App 經常依賴第三方 SDK 與程式庫，這些元件可能帶來隱藏風險。

您的 App 可能具備可接受的資料收集與隱私政策，但所使用的第三方軟體開發套件 (SDK) 或程式庫可能存在重大缺陷。由於企業仍需為資料外洩和合規失敗負責，因此他們必須能夠掌握軟體供應鏈的風險。

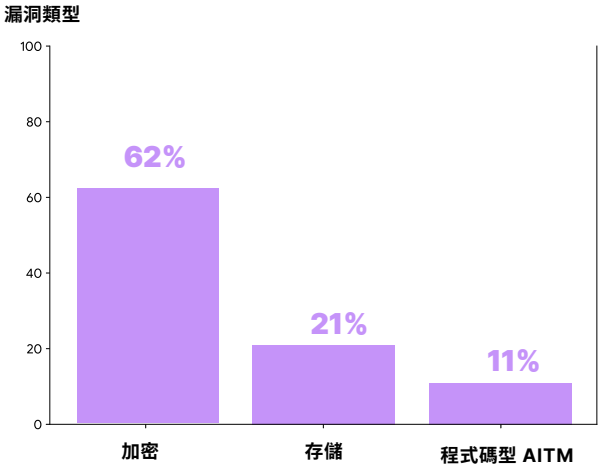


的 **App** 曾使用
含漏洞的程式庫

資料安全

資料可能透過多種方式從 App 中洩露。

- **加密相關問題：**對 App 開發商而言，確保資料安全、保護通訊及驗證使用者身分相當具有挑戰性。許多開發商依賴第三方程式庫。在分析的所有 App 中，NowSecure 發現有兩個已知存在漏洞的程式庫被廣泛使用：OpenSSL 與 libpng。
- **不安全的儲存：**靜態資料的管理方式，會直接決定資料的機密性、完整性與可用性。薄弱的儲存防護會增加資料外洩的風險。
- **中間人攻擊 (AitM) 風險：**App 處理動態傳輸資料的方式也同樣重要。例如，若通訊未經適當加密，攻擊者可能攔截或篡改傳輸中的敏感資訊。
- **資料存取：** 行動 App 可存取攻擊者覬覦的雲端與企業資料。無論透過何種方式存取，資料外洩就是資料外洩。



AI 應用

AI（尤其是生成式 AI）仍是現今的熱門話題。根據德勤 2026 年 1 月發布的報告，員工對經核可 AI 工具的存取權在一年內成長 50%，60% 的員工會在工作中使用 AI 工具。

這不難理解，因為裝置本機 AI 與雲端 AI 均具備眾多便捷功能。例如，行動 App 越來越多地同時整合兩者：

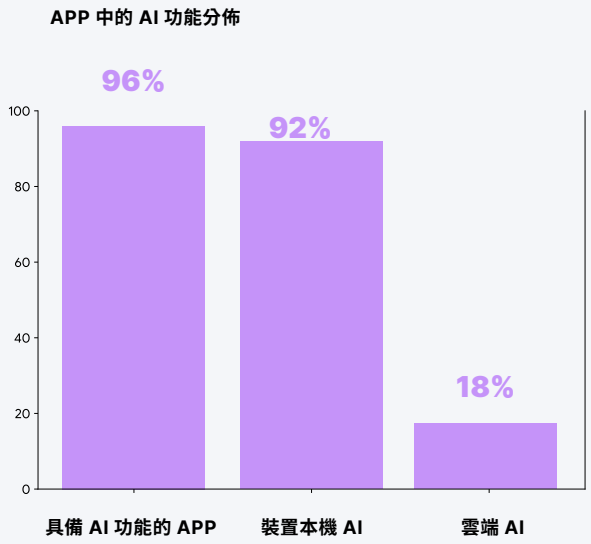
- **裝置本機 AI：**大型語言模型 (LLM) 使應用程式能執行自然語言處理任務（如文字生成與預測輸入），而機器學習模型則用於圖像辨識、即時物體偵測、條碼掃描及擴增實境等功能。
- **雲端 AI：依賴外部基礎架構進行處理與運算，可執行各種進階任務。**

使用者與組織迅速導入生成式 AI，但隨著技術的快速演進，相關風險也在同步攀升。

需考量以下風險：

- 使用者可能使用影子 AI（未經核可且不受管控的 AI 存取），這可能涉及**敏感公司資料**，並違反相關政策。雲端AI依賴外部基礎架構，意味著您的組織可能無法掌握**潛在風險**（包括**資料外洩**）。
- 使用者可能會利用 AI 代理程式**執行自主行動**，從而繞過預期的控制機制。

事實證明，許多常見 App 都在使用 AI，但企業往往缺乏明確的能見度。



隱私

我們隨時隨地攜帶行動裝置。這些裝置儲存大量關於我們個人與工作生活的資訊，包括照片、聯絡人、敏感資料、財務文件、專有資訊等。

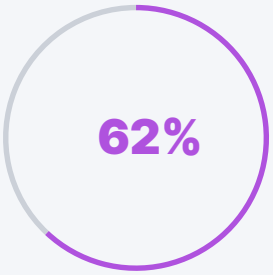
因此，使用者與雇主皆優先重視隱私，此外，您可能需遵守相關隱私法規。

然而，無論是出於開發商的意圖或疏忽，這一點並未總是在應用程式中體現。應用程式可能請求危險權限以收集敏感資料，例如存取：

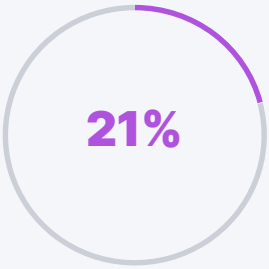
- 裝置位置
- 麥克風
- 相機
- 聯絡人

除了請求資訊外，App 如何處理這些資訊？部分資料的收集是因為 App 執行功能所需。而其他資料的收集則非必要。部分 App 功能會損害隱私，帶來以下影響隱私的問題：

- 追蹤與使用者畫像建立
- 與第三方共用資料
- 收集聯絡人/定向廣告



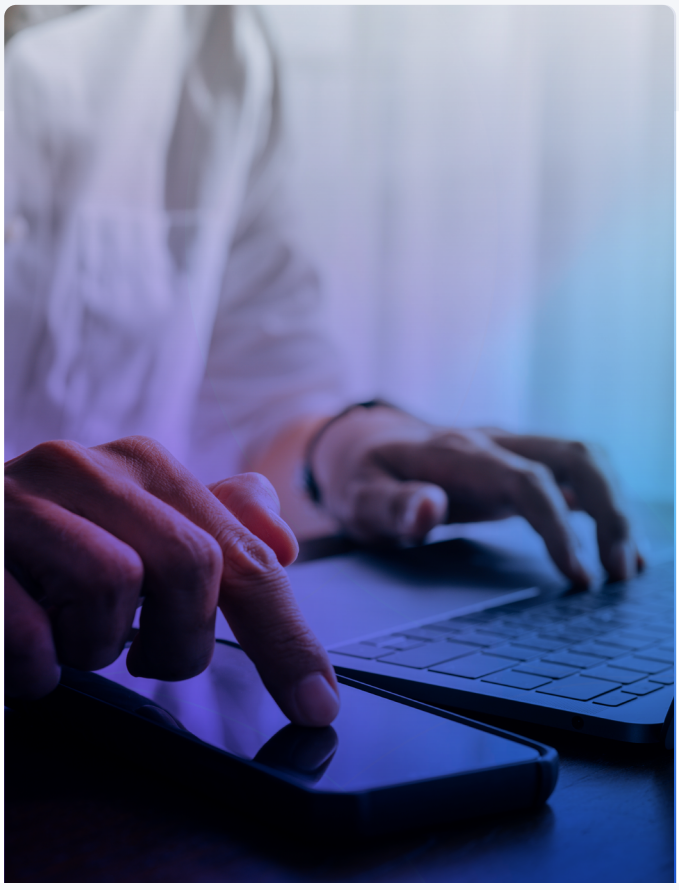
的 **App** 曾請求
高風險權限



的 **App** 存在
影響隱私的行為

資安長 (CISO) 的觀點

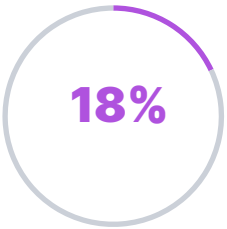
行動 App 是公司敏感資料的第一道門戶。為管理此風險，組織需控制裝置上可安裝的 App、保護跨網路傳輸的資料，並對裝置機群中的 App 漏洞保持能見度。在 BYOD 場景中，核心目標是分離。將公司資料置於容器中加以保護，同時不侵犯個人隱私。最終形成平衡的解決方案：資安團隊擁有所需的管控措施，員工也能確信其個人資料保持私密。



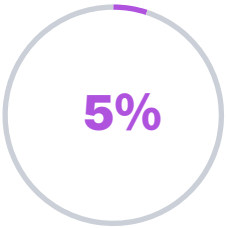
網路與網頁風險

如同死亡與稅收，確定無疑的是，攻擊者將持續利用我們資安防禦中最薄弱的環節：人。攻擊者的攻擊手法日益精進，運用生成式 AI 打造越來越具說服力的攻擊內容。使用者會點擊釣魚連結、連接高風險 Wi-Fi 網路與熱點，或在其他方面忽視資安衛生。

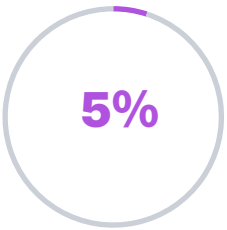
並非所有漏洞皆存在於裝置本身；即使是組態理想、防護完備的裝置，仍易遭受攔截傳輸中資料的威脅。網路是攻擊者常用的入侵途徑。這可能透過多種方式呈現：



的**組織**有使用者連接
高風險熱點



的**組織**有使用者成為
基礎架構型中間人攻擊
的受害者



的**組織**有裝置
受加密劫持影響

網路基礎架構

您可以掌控自身網路的組態，但無法管控使用者離開公司範圍時所連接的所有第三方網路（包括行動網路）。希望您已在落實條件式存取、網路分段及 Zero Trust 網路存取政策。

若未落實，您的資料將面臨風險。若使用者連接未受保護的公共 Wi-Fi 網路（可能加密薄弱或無身分驗證），攻擊者可透過竊取工作階段 Cookie、繞過憑證驗證或其他技術加以利用。

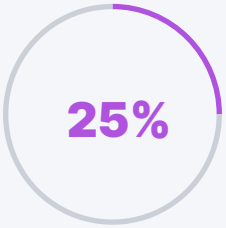
網頁通訊協定規範裝置、瀏覽器與伺服器之間的資訊交換方式。它們是資料安全的關鍵組成部分。攻擊者可將這些通訊協定降級至較舊、安全性較低的版本，從而更容易解密並竊取傳輸中的資料。這會使您的組織面臨中間人攻擊的風險。

這類中間人攻擊利用的是網路基礎架構中的漏洞，而非作業系統或 App 內的程式碼漏洞。

網頁風險

即便處於安全連線環境，上網瀏覽也無法確保絕對安全。裝置未必要遭到入侵才會出現安全問題。點擊惡意連結/廣告或造訪有問題的網站，可能導致加密劫持，或是透過網路釣魚進行的憑證竊取。加密劫持是指攻擊者利用裝置的運算與記憶體資源進行加密貨幣挖礦，這可能會導致裝置效能嚴重下降，甚至完全癱瘓。

說到釣魚攻擊，可謂是我們始終存在的老對手。生成式 AI 讓打造具說服力的網路釣魚訊息變得比以往更輕鬆。使用者再也無法憑藉錯字或其他傳統跡象，判斷訊息是否為惡意釣魚內容。



的**組織**曾有使用者誤點**網路釣魚連結而受害。**

釣魚攻擊中最常被濫用的前 30 大品牌

惡意攻擊者偏好仿冒知名品牌。使用者更傾向點擊自己熟悉且常用服務的連結，而攻擊者正是利用了使用者對日常使用機構的信任。攻擊者特別偏愛攻擊銀行與金融服務業，因為遭入侵的帳戶通常同時包含金錢與敏感資訊。

需注意的是，這些品牌本身並無惡意行為；攻擊者僅是利用其可信賴的聲譽，引誘毫無防備的使用者落入釣魚陷阱。

娛樂/社群網路	商務	公用事業	銀行/金融服務
Netflix	Microsoft	Optus	Allegro
Facebook	Apple	AT&T	U.S. Internal Revenue Service
Steam	Adobe	Amazon	Rakuten
eBay, Inc.		DHL	Coinbase
WhatsApp		British Telcom	PayPal
		Orange	AEON Card
		Comcast	Sumitomo Mitsui Banking Corporation
		East Japan Railway Company	Navy Federal Credit Union
			Bradesco
			Bank of America Corporation
			HSBC Group
			Raiffeisen Bank
			American Express
			ING Direct

資安長 (CISO) 的觀點

除技術管控措施外，透過資安意識宣導、訓練與測試，讓員工主動具備辨識與通報網路釣魚及其他社交工程威脅的能力，也至關重要。釣魚模擬測試應運用 AI，依據使用者能力客製化測試內容，並配合新型態、多樣化的威脅更新測試場景。

風險擴散：進階持續性威脅

截至目前，我們已探討的相關風險包括：

- 裝置作業系統與組態
- 行動 App
- 網路與網頁瀏覽

任何單一風險（例如作業系統漏洞、資料處理不當的行動 App，或使用者連接公共 Wi-Fi），都可能對資料安全造成重大影響。
但實際影響與否，取決於組織的組態政策與使用者訓練成效。

但當這些風險不斷累積，就會構成嚴重問題。進階威脅團體會串聯多個漏洞，打造複雜的漏洞利用程式。過去，發動這類進階攻擊的威脅者向來僅鎖定高價值目標，但如今他們的攻擊工具逐漸廣泛流傳，普通大眾也可能面臨風險。

了解這類進階威脅，是防禦此類攻擊的關鍵。Jamf Threat Labs 針對目標監控行動中使用的多種漏洞利用傳遞機制（包括零點擊與一點擊攻擊）及作戰部署模式進行了評估，這類攻擊主要用於從記者、企業高階主管、政治人物、社運人士等高風險使用者身上蒐集情報。分析內容涵蓋作業系統與第三方應用程式漏洞、供應商回應等主題。 以下是他們的研究發現。

零點擊攻擊仍具高度相關性

2025 年，針對 Apple 與 Android 裝置的零點擊攻擊仍是活躍的威脅途徑，其中記者與企業高階主管是主要攻擊目標。透過圖片解析漏洞
(CVE-2025-43300) 攻擊 WhatsApp 使用者的案例被揭露**，進一步印證了這類攻擊的威脅性。**

該揭露表明，攻擊者仍能在無需使用者任何互動的情況下實現程式碼執行，規避傳統基於資安意識的防禦措施。這類攻擊通常與目標監控或情報蒐集行動相關。

在野零點擊漏洞的持續出現，證實具動機的攻擊者仍具備投入高成本開發漏洞利用程式的能力與意願。

如何保護您的組織：
落實漏洞利用後偵測、行為遙測與異常式監控，而非僅依賴使用者互動式管控措施。

瀏覽器攻擊持續存在，包括透過廣告進行的隱匿式傳遞。

全年來，Apple 與 Google 發布了眾多瀏覽器資安修補程式。Chrome 共收到 250 個資安修補程式，Safari 則超過 75 個，這表明透過惡意構造的網頁內容可觸發的記憶體安全問題仍在持續被發現。

這類漏洞備受攻擊者青睞，因其可透過惡意網站或廣告中的 JavaScript 程式碼武器化，從而降低攻擊者的作戰成本。威脅情報報告顯示，商業間諜軟體供應商仍依賴一點擊漏洞利用鏈，結合已揭露漏洞與沙盒逃脫技術，實現對裝置的完全入侵。

Intellexa 運作模式的揭露表明，這類漏洞利用程式正被情報機構積極使用，且可**透過廣告網路以零點擊攻擊的形式傳遞**。

如何保護您的組織：

在受管理的行動環境中，透過網路流量檢查、漏洞利用行為偵測及強制快速更新作業系統/瀏覽器，強化您的資安防禦體系。

被攻擊的企業積極展開反擊，但防禦覆蓋範圍仍不足。

2025 年，平台供應商與大型科技公司明顯加大了對抗目標式間諜軟體行動的力道，包括採取法律、技術與架構層面的多項措施。諸如 **Meta 對 NSO 集團提起訴訟**等備受矚目的法律行動，顯示防禦已從單純技術防禦升級為持續性法律威懾。

與此同時，Apple 持續投入平台層級防護措施的研發，包括**記憶體標籤擴充 (MTE)**技術及強化鎖定模式。儘管採取這些措施，成功的漏洞利用鏈仍持續存在。

進階攻擊者持續調整其工具與技術，以在新型防護措施內部或周邊運作。例如，近期一場非公開會議上展示了一種可能的繞過方法。

如何保護您的組織：

以獨立偵測、鑑識能見度及針對目標式攻擊場景客製化的事件回應能力，彌補供應商層級防護的不足。

需警惕的間諜軟體

Predator | 開發商： Intellexa

Predator 主要依賴基於網頁的一點擊漏洞利用，通常透過惡意連結、網頁內容（包括廣告）進行傳遞。該軟體大量濫用 WebKit 漏洞，這從 Apple 多次發布修補程式即可證明。這種攻擊模式可擴充性更強，但對修補程式發布的延遲更為敏感。Predator 的案例表明，一點擊攻擊在實際運作中仍具備有效性。

Graphite | 開發商： Paragon

Graphite 是一款商業間諜軟體平台，與進階 iOS 漏洞利用相關，經評估可支援零點擊與一點擊兩種攻擊傳遞方式。2025 年，**針對已安裝所有修補程式的 iPhone 發動的零點擊 iMessage 漏洞利用成功得手，體現了 Graphite 無需使用者互動即可入侵裝置的能力。**多起感染事件可歸因於同一運營者基礎架構，證實攻擊為協調性、蓄意性目標式攻擊，而非機會主義行為。儘管供應商面臨越來越大的監管與法律壓力，這些發現仍確認 Graphite 已成為間諜軟體市場中具備實戰能力的後起之秀。

Landfall | 開發商：無資料

Landfall 是一款此前未被發現的商業級 Android 間諜軟體家族，用於針對三星 Galaxy 裝置的目標式行動間諜活動。攻擊者**利用三星圖像處理庫中的一個重大零日漏洞**，透過惡意構造的圖像檔案傳遞該間諜軟體，這些檔案顯然是透過 WhatsApp 等即時通訊應用程式散佈。

該攻擊行動至少從 2024 年年中活躍至 2025 年 4 月三星修補該漏洞為止，為攻擊者提供了全面的監控能力，包括錄音、定位追蹤，以及蒐集聯絡人、照片與通話記錄。從防禦角度來看，Landfall 證明具備零日漏洞利用能力的 Android 間諜軟體行動仍在公眾視野之外持續演進，凸顯了主動修補管理、異常偵測及跨行動平台長期裝置遙測的必要性。

Pegasus | 開發商：NSO Group

Pegasus 是一款高階 iOS 與 Android 間諜軟體平台，與零點擊及有限的一點擊漏洞利用鏈相關，可實現**對裝置的完全入侵**。該軟體僅鎖定少數高價值個人，並針對隱匿性與持續性進行最佳化。2025 年，NSO 集團的業務受到出口限制與法律責任的影響。該公司其後**被一組投資者收購**，但預計其技術仍會被情報機構使用，可能會以其他品牌名義運作。

Dante | 開發商： Memento Labs

Memento Labs 是一家義大利監控技術廠商，前身即為備受爭議的 Hacking Team，於 2019 年被收購後正式更名。2025 年，與 Memento Labs 相關的工具被用於一場名為「ForumTroll 行動」的**進階網路間諜活動**，該行動利用了一個 Chrome 沙盒逃脫零日漏洞 (CVE-2025-2783)。 據其執行長表示，該公司已停止支援 Windows 相關解決方案，並將重心轉向行動平台，因此該惡意軟體家族及漏洞預計將出現在 Android 裝置上。

Spyrtacus | 開發商： SIO

Spyrtacus 是一款商業監控型間諜軟體家族，據報導於 2025 年積極針對 Android 裝置發動攻擊。該軟體透過惡意連結及應用層社交工程手法傳遞。一旦駐留於裝置上，Spyrtacus 會展現典型間諜軟體功能，包括**資料外洩、定位追蹤，以及訊息與聯絡人蒐集**。

不同於 Pegasus 或 Graphite 等零點擊間諜軟體，Spyrtacus 通常需要使用者一定程度的互動或透過社交工程，才能啟動安裝。Spyrtacus 於真實攻擊行動中的出現，凸顯並非所有目標式行動間諜軟體都依賴零日漏洞利用；相反，攻擊者可將社交工程與現成間諜軟體框架結合，以達成類似目標。

資安長 (CISO) 的觀點

儘管供應商已實施重大的平台層級防護與資安強化措施，2025 年的攻擊者仍持續發現並利用重大漏洞，尤其是
在瀏覽器（Chrome、Safari）及即時通訊應用程式等高價值元件中。這些元件因其複雜性、頻繁暴露於不可信內容，以及在使用者日常工作流程中的核心地位，仍是攻擊者青睞的目標。

成功目標式攻擊的持續存在，凸顯沒有任何防禦策略能完全消除風險，尤其是對抗資源充足的對手時。因此，嚴格的裝置管理與強制更新，仍是組織可運用的最有效且可管控的防護措施之一。

這進一步證實，行動裝置管理並非輔助性功能，而是核心資安控制措施。確保快速部署安全更新、執行資安基準、維持裝置能見度及縮短風險暴露期，是限制新發現漏洞影響範圍的關鍵因素。

風險雖大，但並非無法克服。

應對這些風險需要縝密的架構設計。安全裝置的核心支柱為：

裝置管理：
用於套用限制、設定組態及執行政策

端點安全：
監控裝置健康狀態與行為，以應對潛在入侵風險

安全遠端存取：
管控哪些使用者及裝置可存取公司資源

這些支柱協同運作，確保只有符合規範的裝置與經授權的使用者才能存取您的敏感資料。

根據**裝置是否為公司所有**，具體實施方式可能略有不同。

裝置的組態可能成為風險，也可能成為資安防禦的資產。自動化升級、應用程式審核與行為分析，加上依據合規狀態執行存取政策，將協助您有效保護資料安全。

閱讀 Jamf Threat Labs 最新行動裝置研究報告

Predator 間諜軟體如何規避 iOS 錄音指示功能

2026 年 2 月

Predator 間諜軟體運用一種複雜技術，利用 Objective-C 的空訊息 (nil messaging) 機制，規避 iOS 的錄音指示功能。該惡意軟體鉤取負責處理所有感應器活動更新的 SpringBoard 方法，然後將自身指標設為 NULL，導致指示功能的更新被靜默忽略，而非向使用者顯示。此方法比以往技術更隱匿，因為裝置會正常運作，卻不提供任何監控正在進行的視覺警告，使完全被入侵的裝置能被祕密存取相機與麥克風。

OpenClaw：看似實用的 AI，可能成為您最大的內部威脅

2026 年 2 月

OpenClaw 是一個開源框架，用於建構自主 AI 代理程式，此類代理程式可執行殼層指令、存取檔案並與應用程式互動，且無內建安全邊界，對企業資安構成重大風險。該框架因具備無限制系統存取權、資料外洩風險，且易受間接提示注入攻擊（惡意指令嵌入合法商務內容）影響，而具有高度危險性。近期資安通告顯示，攻擊者可利用多種漏洞透過該框架取得持續存取權，使 OpenClaw 部署成為高風險內部威脅，企業環境中需透過全面偵測、防範與治理策略，才能安全管理。

Predator 的技能切換：iOS 間諜軟體中未公開的反分析技術

2026 年 1 月

Predator 間諜軟體具備複雜的反分析能力，遠超以往記載，包括一套錯誤碼系統，可為運營者提供部署失敗原因的精確診斷資訊。該惡意軟體可偵測開發者模式、越獄工具、資安應用程式與地理限制，並實施進階反鑑識技術，向受害者隱藏錄音指示。

這些機制顯示，當目標攻擊失敗時，運營者會收到詳細回饋，以進行問題排查與策略調整，證明商業間諜軟體供應商不僅致力於規避資安產品，更投入大量精力偵測研究人員。

Jamf Threat Labs 揭露行動 遊戲 App 外洩玩家憑證

2025 年 11 月

下載量超過 1000 萬次的熱門行動遊戲《戰艦世界：閃擊戰》(World of Warships Blitz)，被發現於登入與註冊過程中，透過未加密的 HTTP 連線外洩玩家憑證與工作階段權杖。儘管憑證經過混淆處理，但此次外洩仍促成重放攻擊——攻擊者可擷取並重新傳送驗證請求，以劫持帳戶。在進行負責任的揭露後，開發商積極配合，於 8.4.0 版本中修復了此問題。

這項調查強調，即便熱門應用程式也可能存在重大漏洞，因此多層資安防禦以及使用者密碼安全衛生教育至關重要。

Jamf Threat Labs 發現外洩憑證的 App

2025 年 9 月

兩款行動應用程式被發現透過未加密 HTTP 連線外洩使用者憑證與個人識別資訊（PII）——分別為服務 1500 萬使用者的馬來西亞醫療管理 App，以及印度珠寶公司的「儲蓄」App。兩款應用程式均以明文傳輸敏感資料，使使用者面臨憑證竊取、身份詐欺及未授權帳戶存取風險，尤其在公共網路環境下風險更高。

此發現強調組織迫切需要導入安全資料傳輸機制，且使用者亦應善用行動威脅防禦解決方案、零信任網路存取 (ZTNA) 與內容過濾功能，以阻擋高風險 App。

Flekst0re：第三方 App 商店資安評估

2025 年 8 月

Flekst0re 等第三方 iOS 應用程式商店確實存在嚴重資安風險，經由一款概念驗證的修改版 WhatsApp 可獲得證明：該版本看似合法，卻會祕密錄製通話內容並傳送至遠端伺服器。此類平台透過企業憑證重新簽署應用程式，規避 Apple 安全審查流程；Flekst0re 的自訂來源功能亦允許使用者下載未經驗證的應用程式，這些程式可能含間諜軟體或惡意軟體。

雖第三方商店提供便利性與修改版應用程式的存取權，卻從根本上削弱 iOS 的資安防護機制，使所有使用銀行、通訊或電子郵件等敏感 App 的使用者面臨極大風險。

jamf

歡迎聯絡我們，深入了解行動裝置威脅情勢。

www.jamf.com/zh-tw/