

臉書第三方小遊戲可能洩露

1.2 億用戶資訊

一家名為 Nametest.com 開發的姓名遊戲測試被發現含有漏洞，研究人員發現只要連結 Nametest.com 的網站就能拿到訪客的資訊，如姓名、性別、生日、地點、臉書貼文、友人資訊等等，廣告商可藉此發送精準廣告，歹徒可窺探用戶隱私，伺機勒索。

文/[林妍濤](#) | 2018-06-29 發表

臉書才因一個心理測驗遊戲導致 8,700 萬筆用戶資料遭濫用的劍橋分析醜聞，安全研究人員又發現另一個姓名測驗遊戲 app 有漏洞，洩露 1.2 億名用戶資訊，時間長達一年。所幸漏洞已經修補。

問題出在一家名為 Nametest.com 開發的姓名遊戲測試「Which Disney Princess Are you」。當使用者載入這個遊戲時，它會收集大量用戶資訊，包括姓名、性別、生日、地點等，並且顯示在其公司網頁上。一般情況下，其他網站應無法存取這些資訊，但是這個網站將訊息包在 Javascript 中。而 Javascript 的特性是可以和其他網站共享，因此只要其他網站發出呼叫，用戶的資訊就會分享出去。

研究人員 Inti De Ceukelaire 首先發現這項漏洞，同時設立了能連結 Nametest.com 的網站，就拿到了後者訪客的資訊。雪上加霜的是 Namestest.com 還提供存取憑證，視權限不同可用以存取訪客的臉書貼文、相片和友人資訊。使用者只要造訪 Namestest.com 網站一次，駭客就能拿到他 2 個月的個資。更糟的是，即使用戶刪掉 app，Namestest.com 還是能取得資料。唯一解決就是手動刪除儲存在裝置上的 cookies。

經由這個漏洞，廣告商能利用用戶臉書貼文和親友資訊發送精準廣告，歹徒則可蒐集用戶上網習慣、甚至藉機勒索。研究人員分析網頁存檔，顯示這項漏洞至少在 2016 年底就已存在，雖然 Namestests.com 網站表示他們是在 2017 年 1 月底才加上這個 Javascript。

所幸這個漏洞已經修補。De Ceukelaire 於 4 月通報臉書，而 Namestests.com 網站已在 6 月修補這項漏洞。

3 月間爆發劍橋分析洩露 8,700 萬名用戶資料的事件後，臉書 4 月公佈臉書資料濫用類抓漏獎勵方案。本研究就獲得本方案的 4,000 美元獎金。隨後研究人員將獎金捐出，由臉書加碼一倍捐給了公益團體。

資料來源：iThome