# 瀏覽器擴充漏洞可能導致資料外洩或用戶曝光，Firefox、Chrome 與 Safari 都受影響

研究人員利用特定的列舉攻擊手法，繞過主要瀏覽器的防護機制，取得使用者的擴充程式資訊，可能使得 Tor、VPN 用戶身份曝光。

文/林妍溱 | 2017-08-29 發表

研究人員發現 Firefox、Safari 及 Chrome 擴充程式機制出現漏洞，可能導致使用者的擴充程式被看光，致使以 Tor 或 VPN 匿名的用戶身份曝光。

西班牙德烏斯托大學研究人員 Iskander Sanchez-Rola 指出，擴充程式和瀏覽器的密切關係使其成為明顯的攻擊目標，用來竊取資訊與密碼、瀏覽上網活動記錄等等。雖然瀏覽器也加入了防護方式，像是存取控制設定及隨機 URI(URI Randomization)機制，但 Sanchez-Rola 及其同僚進行的一項研究顯示，透過特定列舉攻擊（enumeration attack）手法，可繞過主要瀏覽器的防護功能，致使資訊曝光。

針對這些機制研究人員設計了破解方法。首先研究人員對瀏覽器存取控制設定發動計時旁路攻擊（timing side-channel），成功取得了瀏覽器中安裝的完整擴充程式，而這種技倆可以繞過所有主要瀏覽器

的防護，包括Safari、Chrominum系列的瀏覽器如Chrome、Opera、Yandex、Comodo Dragon 及舊版 Firefox 等。

第二種攻擊法則是針對 Safari 的隨機 URI(URI Randomization)保護機制而來。這個機制能確保使用者上的網站 URL 不會外洩。研究人員透過名為 URI 外洩（URI leakage）的手法，對 Safari 擴充程式進行程式碼靜態分析，藉此曝露出數百個擴充程式，包括 Tor 或 VPN 的隨機 URI，進而讓駭客或情治機關得以辨識出使用者。他們的測試顯示甚至能抓出 40.5%的擴充程式 URL。

事實上，本篇文章公佈時，這些漏洞都還未修補。研究人員表示希望能藉由揭露瀏覽器的弱點，促使瀏覽器及擴充程式開發商討論以及早催生防制措施。

資料來源：iThome