

行政院國家資通安全會報技術服務中心

漏洞/資安訊息警訊

發布編號	NCCST-ANA-2019-0073	發布時間	Thu Jun 20 15:39:22 CST 2019
事件類型	漏洞預警	發現時間	Thu Jun 20 00:00:00 CST 2019
警訊名稱	Firefox 瀏覽器存在安全漏洞(CVE-2019-11707)，允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新		
內容說明	Google Project Zero 研究人員發現 Firefox 瀏覽器使用 Array.pop 函數處理 JavaScript 物件時，可能引發類型混淆(Type confusion)的安全漏洞(CVE-2019-11707)，攻擊者可透過誘騙受害者點擊惡意連結，進而造成遠端執行任意程式碼。		
影響平台	Firefox 67.0.3 以前版本 Firefox ESR 60.7.1 以前版本		
影響等級	高		
建議措施	<p>1.請確認瀏覽器版本，點擊瀏覽器選單按鈕，點選「說明」-->「關於 Firefox」，可查看當前使用的 Mozilla Firefox 瀏覽器是否為受影響之版本。</p> <p>2.更新方式如下：</p> <p>(1)開啟瀏覽器，點擊選單按鈕，點選「說明」-->「關於 Firefox」，瀏覽器將執行版本檢查與更新。</p> <p>(2)點擊「重新啟動以更新 Firefox」完成更新。</p> <p>3.保持良好使用習慣，請勿點擊來路不明的網址連結。</p>		
參考資料	<p>1. https://www.mozilla.org/en-US/security/advisories/mfsa2019-18/</p> <p>2. https://thehackernews.com/2019/06/mozilla-firefox-patch-update.html</p> <p>3. https://www.tenable.com/blog/cve-2019-11707-critical-type-confusion-zero-day-in-mozilla-firefox-exploited-in-the-wild</p> <p>4. https://www.jpccert.or.jp/at/2019/at190027.html</p>		

此類通告發送對象為通報應變網站登記之資安人員。若貴單位之資安人員有變更，可逕自登入通報應變網站（<https://www.ncert.nat.gov.tw>）進行修改。若您仍為貴單位之資安人員但非本事件之處理人員，請協助將此通告告知相關處理人員。

如果您對此通告的內容有疑問或有關於此事件的建議，請勿直接回覆此信件，請以下述聯絡資訊與我們連絡。

地 址： 台北市富陽街 116 號

聯絡電話： 02-27339922

傳真電話： 02-27331655

電子郵件信箱： service@nccst.nat.gov.tw