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-2020-0034	發布時間	Tue Apr 07 10:05:25 CST 2020
事件類型	漏洞預警	發現時間	Mon Apr 06 00:00:00 CST 2020
警訊名稱	Firefox 瀏覽器存在安全漏洞(CVE-2020-6819 與 CVE-2020-6820)，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	研究人員發現 Firefox 瀏覽器在運行 nsDocShell 解構函式或處理 ReadableStream 類型的物件時，會因資源競爭(Race Condition)問題，導致使用釋放後記憶體(use-after-free)的安全漏洞(CVE-2020-6819 與 CVE-2020-6820)。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 74(含)以前版本 Firefox ESR 68.6(含)以前版本		
影響等級	高		
建議措施	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。 2.更新方式如下： (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。 (2)點擊「重新啟動以更新 Firefox」完成更新，並確認更新後的版本為 Firefox 74.0.1 或 Firefox ESR 68.6.1 以後版本。 3.保持良好使用習慣，請勿點擊來路不明的網址連結。		
參考資料	1. https://www.mozilla.org/en-US/security/advisories/mfsa2020-11/ 2. https://threatpost.com/firefox-zero-day-flaws-exploited-in-the-wild-get-patched/154466/		

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