

張貼日期：2022/05/27

# 【資安漏洞預警】Firefox修補惡意JavaScript執行的重大漏洞【CVE-2022-1802】【CVE-2022-1529】

- 主旨說明【Firefox修補惡意JavaScript執行的重大漏洞】【CVE-2022-1802】【CVE-2022-1529】

- 內容說明：

- 轉發 科學園區資安資訊分享與分析中心 SPISAC-ANA-202205-0011
- Mozilla上周釋出安全更新公告，以修補桌機、手機版瀏覽器及郵件軟體Thunderbird中2個可執行惡意JavaScript重大風險漏洞。
- 兩個漏洞中【CVE-2022-1802】為Top-Level Await實作中的原型鏈污染【prototype pollution】漏洞。如果攻擊者可透過原型鏈污染破壞JavaScript中Array物件的方法【methods】就能取得權限執行程式碼【CVE-2022-1529】則允許攻擊者傳送方法訊息到主行程查詢JavaScript物件索引，導致原型鏈污染，結果是攻擊者控制的JavaScript可以在具權限的主行程中執行。

- 影響平台：

- Firefox 100.0.2以前版本
- Firefox ESR 91.9.1以前版本
- Firefox for Android 100.3以前版本
- Thunderbird 91.9.1以前版本

- 建議措施：

請更新至以下版本：

- Firefox 100.0.2版
- Firefox ESR 91.9.1版
- Firefox for Android 100.3版
- Thunderbird 91.9.1版

- 參考資料：

1. <https://www.ithome.com.tw/news/151086>
2. <https://www.mozilla.org/en-US/security/advisories/mfsa2022-19/>

計算機與通訊中心  
網路系統組 敬啟

From:  
<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:  
[https://net.nthu.edu.tw/netsys/mailing:announcement:20220527\\_01](https://net.nthu.edu.tw/netsys/mailing:announcement:20220527_01)

Last update: 2022/05/27 11:00