張貼日期：2026/07/27

【漏洞預警WordPress存在兩項高風險安全漏洞(CVE-2026-60137與CVE-2026-63030)請儘速確認並進行修補

- 主旨說明:【漏洞預警WordPress存在兩項高風險安全漏洞(CVE-2026-60137與CVE-2026-63030)請儘速確認並進行修補

- 內容說明:
  - 轉發 國家資安資訊分享與分析中心 資安訊息警訊 NISAC-200-202607-00000006
  - 研究人員發現WordPress存在兩項高風險安全漏洞(CVE-2026-60137與CVE-2026-63030)類型分別為SQL注入(SQL Injection)與REST API批次端點路由判讀錯誤問題。其中CVE-2026-60137已遭駭客利用，請儘速確認並進行修補。
  - CVE-2026-60137當外掛程式或佈景主題將未受信任之輸入傳入受影響功能時，可能導致SQL注入。
  - CVE-2026-63030未經身分鑑別之遠端攻擊者可利用REST API批次端點路由判讀錯誤問題，並結合CVE-2026-60137執行SQL注入，進而於受影響系統上執行任意程式碼。
- 影響平台:
  - WordPress 6.8.0至6.8.5版本
  - WordPress 6.9.0至6.9.4版本
  - WordPress 7.0.0至7.0.1版本
- 建議措施:
  - 官方已針對漏洞釋出修復更新，請升級至以下版本，並參考官方說明進行更新：https://wordpress.org/news/2026/07/wordpress-7-0-2-release/
- 參考資料:
  1. https://nvd.nist.gov/vuln/detail/CVE-2026-60137
  2. https://nvd.nist.gov/vuln/detail/CVE-2026-63030
  3. https://wordpress.org/news/2026/07/wordpress-7-0-2-release/

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:20260727_22

Last update: **2026/07/27 14:38**