國立成功大學 National Cheng Kung University

ANA事件單通知:TACERT-ANA-2025120502124747【漏洞預警】WordPress擴充程式與網頁主題存在6個安全漏洞(CVE-2025-13536) (CVE-2025-13538) (CVE-2025-13539) (CVE-2025-13540) (CVE-2025-13615) (CVE-2025-13675)，請儘速確認並進行修補

教育機構ANA通報平台

發佈編號	TACERT-ANA-2025120502124747	發佈時間	2025-12-05 14:06:48
事故類型	ANA-漏洞預警	發現時間	2025-12-05 14:06:48
影響等級	中		

[主旨說明:]【漏洞預警】WordPress擴充程式與網頁主題存在6個安全漏洞(CVE-2025-13536) (CVE-2025-13538) (CVE-2025-13539) (CVE-2025-13540) (CVE-2025-13615) (CVE-2025-13675)，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-200-202512-00000041

研究人員發現WordPress擴充程式與網頁主題存在6個高風險安全漏洞，請儘速確認並進行修補。

1. Blubrry PowerPress擴充程式存在任意檔案上傳(Arbitrary File Upload)漏洞(CVE-2025-13536)，取得一般權限之遠端攻擊者可於受影響網頁伺服器上傳並執行網頁後門程式，進而達成遠端執行任意程式碼。

2. FindAll Listing與Tiare Membership擴充程式及Tiger網頁主題存在權限提升(Privilege Escalation)漏洞(CVE-2025-13538、CVE-2025-13540及CVE-2025-13675)，未經身分鑑別之遠端攻擊可於註冊時指定管理者角色，進而利用漏洞取得網站管理員權限。

3. FindAll Membership擴充程式存在身分鑑別繞過(Authentication Bypass)漏洞(CVE-2025-13539)，未經身分鑑別之遠端攻擊者於取得一般使用者帳號且能存取管理員電子郵件之情況下，以管理員身分登入系統。

4. StreamTube Core擴充程式存在任意使用者密碼變更(Arbitrary User Password Change)漏洞(CVE-2025-13615)，未經身分鑑別之遠端攻擊者可任意變更網站使用者密碼，進而接管管理員帳號。

WordPress為常見網站架設系統，由於其擴充程式與網頁布景主題數量眾多，因此偶有出現嚴重漏洞情況，如本次警訊所列之幾項漏洞。

建議若有使用WordPress系統時，除留意WordPres本身核心程式之更新資訊外，針對擴充程式網頁布景主題亦須關注，適時更新修補，此外亦建議評估所用之擴充程式網頁布景主題之必要性，如無需求，建議移除。

情資分享等級: WHITE(情資內容為可公開揭露之資訊)

此訊息僅發送到「區縣市網路中心」，煩請貴單位協助轉發與通知轄下各單位知悉

[影響平台:]

Blubrry PowerPress 11.15.2(含)以前版本

FindAll Listing 1.0.5(含)以前版本

FindAll Membership 1.0.4(含)以前版本

Tiare Membership 1.2(含)以前版本

StreamTube Core 4.78(含)以前版本

Tiger網頁主題 101.2.1(含)以前版本

[建議措施:]

更新Blubrry PowerPress至11.15.3(含)以後版本

更新FindAll Listing至1.1(含)以後版本

更新FindAll Membership至1.1(含)以後版本

更新Tiare Membership至1.3(含)以後版本

更新StreamTube Core至4.79(含)以前後版本

Tiger網頁主題請參考官方說明採取必要措施，網址如下： https://wwwwordfence.com/threat-intel/vulnerabilities/wordpress-themes/tiger-2/tiger-10121-unauthenticated-privilege-escalation

[參考資料:]
1. https://nvd.nist.gov/vuln/detail/CVE-2025-13536
2. https://nvd.nist.gov/vuln/detail/CVE-2025-13538
3. https://nvd.nist.gov/vuln/detail/CVE-2025-13539
4. https://nvd.nist.gov/vuln/detail/CVE-2025-13540
5. https://nvd.nist.gov/vuln/detail/CVE-2025-13615
6. https://nvd.nist.gov/vuln/detail/CVE-2025-13675

(此通報僅在於告知相關資訊，並非為資安事件)，如果您對此通報的內容有疑問或有關於此事件的建議，歡迎與我們連絡。

教育機構資安通報應變小組
網址：https://info.cert.tanet.edu.tw/
專線電話：07-5250211
網路電話：98400000
E-Mail：service@cert.tanet.edu.tw