張貼日期：2025/09/04

【漏洞預警】FreePBX存在高風險安全漏洞(CVE-2025-57819)，請儘速確認並進行修補

- 主旨說明:【漏洞預警】FreePBX存在高風險安全漏洞(CVE-2025-57819)，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 NISAC-200-202509-00000006
  - 研究人員發現FreePBX此用於管理Asterisk系統之Web管理介面工具，存在驗證繞過(Authentication Bypass)漏洞(CVE-2025-57819)，未經身分鑑別之遠端攻擊者可直接存取管理者功能，進而控制資料庫與執行任意程式碼。該漏洞已遭駭客利用，請儘速確認並進行修補。
  - 備註：Asterisk為開放原始碼之使用者交換機(PBX)系統軟體，包含網路電話(VoIP)功能，除運作一般電腦外，亦可運作於OpenWRT之類的嵌入式系統上。
- 影響平台:
  - FreePBX 15至15.0.66(不含)版本
  - FreePBX 16至16.0.89(不含)版本
  - FreePBX 17至17.0.3(不含)版本
- 建議措施:
  - 官方已針對漏洞釋出修復更新，請參考官方說明，網址如下：
    https://github.com/FreePBX/security-reporting/security/advisories/GHSA-m42g-xg4c-5f3h
- 參考資料:
  1. https://nvd.nist.gov/vuln/detail/CVE-2025-57819
  2. https://github.com/FreePBX/security-reporting/security/advisories/GHSA-m42g-xg4c-5f3h

---

計算機與通訊中心
網路系統組 敬啟