教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2025090310095858	發佈時間	2025-09-03 10:22:01
事故類型	ANA-漏洞預警	發現時間	2025-09-03 10:22:01
影響等級	中		

[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。

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:]

- 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