張貼日期：2025/10/22

【漏洞預警】Fortinet FortiPAM與FortiSwitchManager存在高風險安全漏洞(CVE-2025-49201)，請儘速確認並進行修補

- 主旨說明：【漏洞預警】Fortinet FortiPAM與FortiSwitchManager存在高風險安全漏洞(CVE-2025-49201)，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-200-202510-00000158
  - 研究人員發現Fortinet FortiPAM與FortiSwitchManager之GUI存在驗證機制不足(Weak Authentication)漏洞(CVE-2025-49201)，未經身分鑑別之遠端攻擊者可透過暴力破解繞過驗證流程並登入系統，進而執行未經授權之指令，請儘速確認並進行修補。
- 影響平台：
  - FortiPAM 1.5.0版本
  - FortiPAM 1.4.0至1.4.2版本
  - FortiPAM 1.3所有版本
  - FortiPAM 1.2所有版本
  - FortiPAM 1.1所有版本
  - FortiPAM 1.0所有版本
  - FortiSwitchManager 7.2.0至7.2.4版本
- 建議措施：
  - 官方已針對漏洞釋出修復更新，請參考官方說明進行更新，網址如下：https://fortiguard.fortinet.com/psirt/FG-IR-25-010
- 參考資料：
  1. https://nvd.nist.gov/vuln/detail/CVE-2025-49201
  2. https://fortiguard.fortinet.com/psirt/FG-IR-25-010

計算機與通訊中心
網路系統組 敬啟