張貼日期：2025/08/04

【漏洞預警□HPE之Networking Instant On無線基地台存在高風險安全漏洞(CVE-2025-37102與CVE-2025-37103)□請儘速確認並進行修補

- 主旨說明:【漏洞預警□HPE之Networking Instant On無線基地台存在高風險安全漏洞(CVE-2025-37102與CVE-2025-37103)□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-200-202507-00000230
  - 研究人員發現HPE之Networking Instant On無線基地台存在2項高風險安全漏洞(CVE-2025-37102與CVE-2025-37103)□類型分別為作業系統命令注入(OS Command Injection)與使用硬刻之帳號通行碼(Use of Hard-coded Credentials)□前者可使已取得管理權限之遠端攻擊者注入任意作業系統指令並於設備上執行，後者可使未經身分鑑別之遠端攻擊者利用固定帳號通行碼以管理員權限登入系統，請儘速確認並進行修補。
- 影響平台:
  - HPE之Networking Instant On無線基地台軟體版本3.20.1(含)以下
- 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://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04894en_us&docLocale=en_US
- 參考資料:
  1. https://nvd.nist.gov/vuln/detail/CVE-2025-37102
  2. https://nvd.nist.gov/vuln/detail/CVE-2025-37103
  3. https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04894en_us&docLocale=en_US

計算機與通訊中心
網路系統組 敬啟