張貼日期：2024/04/16

【漏洞預警D-Link NAS存在高風險安全漏洞(CVE-2024-3272與CVE-2024-3273)請儘速確認並進行修補！

- 主旨說明D-Link NAS存在高風險安全漏洞(CVE-2024-3272與CVE-2024-3273)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-200-202404-00000053
  - 研究人員發現部分舊款D-Link NAS存在使用Hard-coded帳號通行碼漏洞(Use of Hard-Coded Credentials)(CVE-2024-3272)與作業系統指令注入漏洞(OS Command Injection)(CVE-2024-3273)未經身分鑑別之遠端攻擊者可利用CVE-2024-3272提升至系統權限，或利用CVE-2024-3273執行任意程式碼。受影響之型號皆已停止支援，請儘速確認並進行汰換。
- 影響平台:
  - DNS-320L
  - DNS-325
  - DNS-327L
  - DNS-340L
- 建議措施:
  - 官方已宣布不再支援更新受影響之型號，請儘速確認並進行汰換。
- 參考資料:
  1. https://nvd.nist.gov/vuln/detail/CVE-2024-3272
  2. https://nvd.nist.gov/vuln/detail/CVE-2024-3273
  3. https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383

計算機與通訊中心
網路系統組 敬啟