

張貼日期：2026/02/25

# 【漏洞預警】Dell RecoverPoint for Virtual Machines存在高風險安全漏洞(CVE-2026-22769)請儘速確認並進行修補

- 主旨說明: 【漏洞預警】Dell RecoverPoint for Virtual Machines存在高風險安全漏洞(CVE-2026-22769)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 資安訊息警訊 NISAC-200-202602-00000093
  - 研究人員發現Dell RecoverPoint for Virtual Machines存在使用硬刻之帳號通行碼(Use of Hard-coded Credentials)漏洞(CVE-2026-22769)未經身分鑑別之遠端攻擊者可使用硬刻之帳號通行碼取得底層作業系統之root權限。
  - 該漏洞已遭駭客利用，請儘速確認並進行修補。
- 影響平台:
  - RecoverPoint for Virtual Machines 5.3 SP4 P1(含)以前版本 6.0 6.0 SP1 6.0 SP1 P1 6.0 SP1 P2 6.0 SP2 6.0 SP2 P1 6.0 SP3及6.0 SP3 P1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://www.dell.com/support/kbdoc/zh-tw/000426773/dsa-2026-079>
- 參考資料:
  1. <https://nvd.nist.gov/vuln/detail/CVE-2026-22769>
  2. <https://www.dell.com/support/kbdoc/zh-tw/000426773/dsa-2026-079>

計算機與通訊中心  
網路系統組 敬啟

From:  
<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:  
[https://net.nthu.edu.tw/netsys/mailling:announcement:20260225\\_23](https://net.nthu.edu.tw/netsys/mailling:announcement:20260225_23)



Last update: 2026/02/25 15:24