Date Posted: 2026/02/25

[Vulnerability Alert] High-Risk Security Vulnerability Found in Dell RecoverPoint for Virtual Machines (CVE-2026-22769), Please Confirm and Patch Immediately

- Subject Explanation: [Vulnerability Alert] High-Risk Security Vulnerability Found in Dell RecoverPoint for Virtual Machines (CVE-2026-22769), Please Confirm and Patch Immediately

- Content Description:
  - Forwarding National Information Security Analysis and Sharing Center (NISAC) Alert NISAC-200-202602-00000093
  - Researchers have discovered a Use of Hard-coded Credentials vulnerability (CVE-2026-22769) in Dell RecoverPoint for Virtual Machines. An unauthenticated remote attacker could use hard-coded credentials to gain root access to the underlying operating system.
  - This vulnerability has already been exploited by hackers; please confirm and patch immediately.
- Impacted Platforms:
  - RecoverPoint for Virtual Machines 5.3 SP4 P1 and earlier versions, 6.0, 6.0 SP1, 6.0 SP1 P1, 6.0 SP1 P2, 6.0 SP2, 6.0 SP2 P1, 6.0 SP3, and 6.0 SP3 P1 versions
- Suggested Measures:
  - The official vendor has released a repair update for the vulnerability; please refer to the official instructions to update. The URL is as follows: https://www.dell.com/support/kbdoc/zh-tw/000426773/dsa-2026-079
- References:
  1. https://nvd.nist.gov/vuln/detail/CVE-2026-22769
  2. https://www.dell.com/support/kbdoc/zh-tw/000426773/dsa-2026-079

Computer and Communication Center
Network Systems Division

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

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20260225_23

Last update: **2026/02/25 15:27**