

ADV2026_094 Dell Security Advisory – Update 1 (February 18th, 2025)

Dell has published a security advisory highlighting vulnerabilities in the following products on February 17th, 2026. It is recommended that you take the necessary precautions by ensuring your products are always updated.

- RecoverPoint for Virtual Machines – versions prior to 5.3 SP4 P1
- RecoverPoint for Virtual Machines – 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
- Open-source reporting has indicated that CVE-2026-22769 is being exploited in the wild.

Update 1

Cybersecurity and Infrastructure Security Agency (CISA) added CVE-2026-22769 to their Known Exploited Vulnerabilities (KEV) Database on February 18, 2026.

For more information on these updates, you can follow this URL:

- [DSA-2026-079: Security Update for RecoverPoint for Virtual Machines Hardcoded Credential Vulnerability](#)
- [Dell Security advisories and notices](#)
- [CISA KEV: CVE-2026-22769](#)

The Guyana National CIRT recommends that users and administrators review these updates and apply them where necessary.

References

- Dell security advisory. (February 18, 2026). Retrieved from Canadian Centre for Cyber Security. <https://www.cyber.gc.ca/en/alerts-advisories/dell-security-advisory-av26-138>
- Dell Advisories, Notices and Resources. (n.d.). Retrieved from Dell. <https://www.dell.com/support/security/en-ca>
- CISA KEV: CVE-2026-22769. (n.d.). Retrieved from CISA. https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-22769



- DSA-2026-079: Security Update for RecoverPoint for Virtual Machines Hardcoded Credential Vulnerability. (February 17, 2026). Retrieved from Dell.
<https://www.dell.com/support/kbdoc/en-us/000426773/dsa-2026-079>