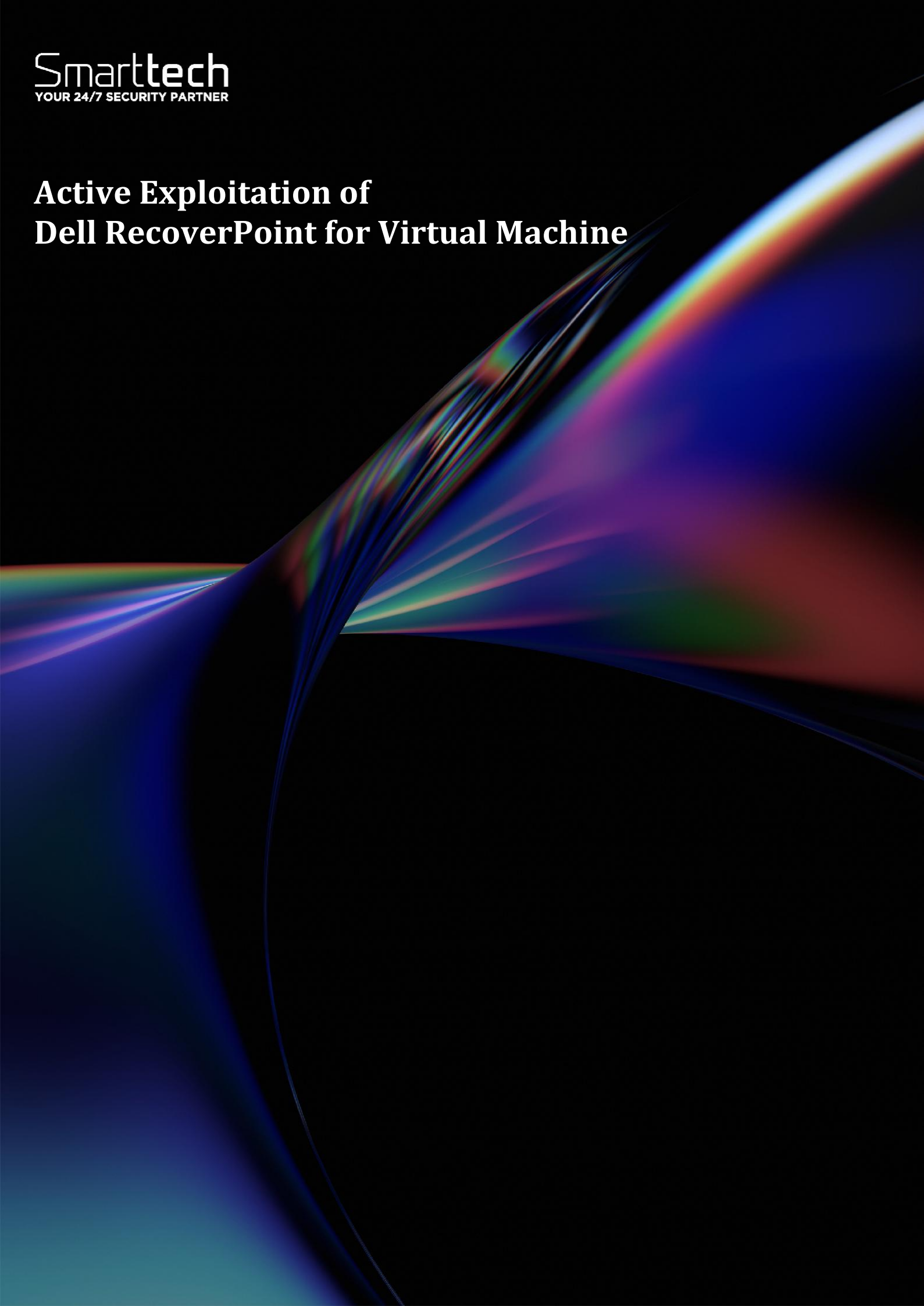
Smarttech
YOUR 24/7 SECURITY PARTNER

Active Exploitation of Dell RecoverPoint for Virtual Machine



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	26
Authors	Alex Ciuta < alexandru.ciuta@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-02-19
Issue Date	2026-02-19

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released. Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview:

Dell has confirmed active exploitation of a zero-day vulnerability in Dell RecoverPoint for Virtual Machines. Successful exploitation by an unauthenticated remote attacker with knowledge of the hardcoded credential could potentially exploit this vulnerability, leading to unauthorized access to the underlying operating system and root-level persistence.

Technical summary

The vulnerability (CVE-2026-22769) is caused by the presence of hard-coded administrator credentials within Dell RecoverPoint for Virtual Machines, which results in a security decision being made based on untrusted, built-in authentication data. This flaw allows an unauthenticated remote attacker to gain full administrative access to the affected system. To exploit it, an attacker only needs to connect to the exposed management interface where these credentials are accepted automatically.

Proprietary Code CVEs	**Description**	**CVSS Base Score**
CVE-2026-22769	Dell RecoverPoint for Virtual Machines, versions prior to 6.0.3.1 HF1, contain a hardcoded credential vulnerability. This is considered critical as an unauthenticated remote attacker with knowledge of the hardcoded credential could potentially exploit this vulnerability leading to unauthorized access to the underlying operating system and root-level persistence. Dell recommends that customers upgrade or apply one of the remediations as soon as possible.	10.0

Mitigation

- Upgrade to the fixed software version that removes the hard-coded credentials and closes the authentication bypass.
- Apply the security patch as soon as possible, since the vulnerability is known to be actively exploited.
- No temporary workarounds are available—patching is the only effective remediation path.

Affected Products & Remediation

Product	Affected Versions	Remediated Versions
RecoverPoint for Virtual Machines	Version 5.3 SP4 P1	Follow the steps below in order: 1. Migrate from RecoverPoint for Virtual Machines 5.3 SP4 P1 to 6.0 SP3 (Instructions) 2. Upgrade to 6.0.3.1 HF1 OR 1. Follow the instructions in the Knowledge Base article to run the remediation script: RecoverPoint for Virtual Machines: Apply the remediation script for DSA-2026-079
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	1. Upgrade to 6.0.3.1 HF1 OR 2. Follow the instructions in the Knowledge Base article to run the remediation script: RecoverPoint for Virtual Machines: Apply the remediation script for DSA-2026-079

Versions 5.3 SP4, 5.3 SP3, 5.3 SP2, and potentially earlier versions of RecoverPoint for Virtual Machines are also impacted by CVE-2026-22769. Dell recommends that customers upgrade to version 5.3 SP4 P1 or a 6.x version then apply the remediation steps outlined above. Supported versions of RecoverPoint for Virtual Machines and related End of Service dates can be found on the RecoverPoint for Virtual Machines Support Overview page.

References

https://www.dell.com/support/kbdoc/en-us/000426773/dsa-2026-079
https://thehackernews.com/2026/02/dell-recoverpoint-for-vms-zero-day-cve.html
https://www.cve.org/CVERecord?id=CVE-2026-22769

CVE

CVE-2026-22769

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com