Critical Vulnerability in Dell RecoverPoint Allows Remote System Takeover

TL;DR

CVE-2026-22769 (CVSS 10.0) is a hardcoded credential vulnerability in Dell RecoverPoint for Virtual Machines that allows unauthenticated remote attackers to gain root-level access.

Dell confirmed limited active exploitation. If you are running affected versions, patch or apply the remediation script immediately.

Overview

There is a hardcoded credential vulnerability (CVE-2026-22769, CVSS 10) affecting Dell's RecoverPoint for Virtual Machines. The issue allows a remote attacker with knowledge of the embedded credential to authenticate to the system without valid user credentials.

Affected Products

- Dell RecoverPoint for Virtual Machines prior to 6.0.3.1 HF1
- Versions 6.0, 6.0 SP1, 6.0 SP1 P1, 6.0 SP1 P2, 6.0 SP2, 6.0 SP2 P1, 6.0 SP3, 6.0 SP3 P1
- Version 5.3 SP4 P1 (requires upgrade path)
- Versions 5.3 SP4, 5.3 SP3, as5.3 SP2, and potentially earlier builds

Note: RecoverPoint Classic (physical and virtual appliances) is not affected.

Researchers observed attackers accessing the Apache Tomcat Manager interface, deploying malicious WAR files, and executing commands as root. Once inside the appliance, attackers moved into VMware environments and deployed additional tooling for persistence and lateral movement.

RecoverPoint appliances are typically deployed inside trusted internal networks and connect directly to virtualized workloads. If compromised, they can provide attackers with direct access into core infrastructure. Dell confirmed limited active exploitation. Aspire recommends patching immediately.

Aspire Protects

- **Patch** – Upgrade immediately to 6.0.3.1 HF1
  - If upgrade cannot be performed immediately, apply Dell's remediation script. See Dell's advisory for further information.
- Restrict management interfaces to trusted internal networks

- Review Tomcat Manager logs for unauthorized deployments
- Inspect VMware environments for suspicious virtual network adapters

TTPs to Watch

Initial Access

- Valid Accounts [T1078] – The attacker may have authenticated using hardcoded credentials embedded in the appliance.

Persistence

- Server Software Component: Web Shell [T1505.003] – The attacker may have deployed a malicious WAR file to maintain access.

Execution

- Command and Scripting Interpreter [T1059] – The attacker may have executed system commands through the deployed web shell.

Lateral Movement

- Remote Services [T1021] – The attacker may have pivoted from the compromised appliance into VMware infrastructure.

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

RecoverPoint for Virtual Machines is widely used in enterprise VMware environments. Organizations operating virtualized infrastructure should assess exposure immediately.

- Finance
- Government
- Education
- Energy
- Healthcare
- Retail
- Technology
- Manufacturing

Aspire's Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

DSA-2026-079: Security Update for RecoverPoint for Virtual Machines Hardcoded Credential Vulnerability | Dell US