EnCyb

Severity: Critical

Advisory Type: Vulnerability

Ghost NIC Persistence in Dell Zero-Day Exploitation

Advisory Report

TLP: WHITE

SECURITY THREAT ADVISORY COUNCIL (STAC)

Empowering organizations with cutting-edge cybersecurity strategies to combat emerging digital threats effectively.

EXECUTIVE SUMMARY

China-linked threat actors (UNC6201) have been exploiting a critical Dell RecoverPoint for Virtual Machines zero-day (CVE-2026-22769) since mid-2024. The vulnerability involves hardcoded credentials that enable unauthenticated root-level access and the deployment of persistent backdoors. Attackers transitioned from the Brickstorm malware to the more advanced Grimbolt implant and used hidden VMware ESXi "Ghost NICs" for stealthy lateral movement. The campaign targets organizations using VMware environments across sectors such as legal, technology, and manufacturing, with the full extent of impact still under investigation.

- CVE: CVE-2026-22769
- CVSS: 10.0
- Active Region: Global
- Affected Sector: Critical infrastructure, legal, technology, manufacturing, and enterprises operating VMware environments
- Affected Product: Dell RecoverPoint for Virtual Machines
- Severity: Critical
- Published Date: February 17, 2026

TECHNICAL DETAILS

- **Target:** Dell RecoverPoint for Virtual Machines appliances deployed in VMware environments, particularly infrastructure appliances that often lack traditional endpoint detection and response (EDR) visibility.
- **Root Cause:** A hardcoded credential vulnerability (CVE-2026-22769) that allows an unauthenticated remote attacker with knowledge of the credential to gain unauthorized access and achieve root-level persistence on the underlying operating system.
- **Prerequisite For Exploitation:** Attackers require network-level access to the vulnerable appliance and knowledge of the hardcoded credential. The management interface must be reachable (internet-exposed or accessible from a compromised internal host).

IMPACT

- Unauthenticated remote compromise of affected appliances.
- Root-level persistence on affected systems
- Deployment of backdoors (Brickstorm / Grimbolt)
- Stealthy lateral movement via “Ghost NICs”
- Long-term undetected espionage and data access
- Potential compromise of broader VMware virtual infrastructure

RECOMMENDATIONS

- Apply the vendor security update immediately (upgrade to **RecoverPoint for VMs 6.0.3.1 HF1** or later)
- Restrict and segment access to the management interface; ensure it is **not internet-exposed** and accessible only from trusted networks.
- Rotate all credentials associated with the appliance and connected VMware infrastructure (including service, admin, and API credentials).

REFERENCE

- https://www.bleepingcomputer.com/news/security/chinese-hackers-exploiting-dell-zero-day-flaw-since-mid-2024/

SECURE, SCALE, SUCCEED WITH CONFIDENCE

EnCyb

www.encyb.com/contact-us/ EnCyb soc@encyb.com

www.encyb.com