Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

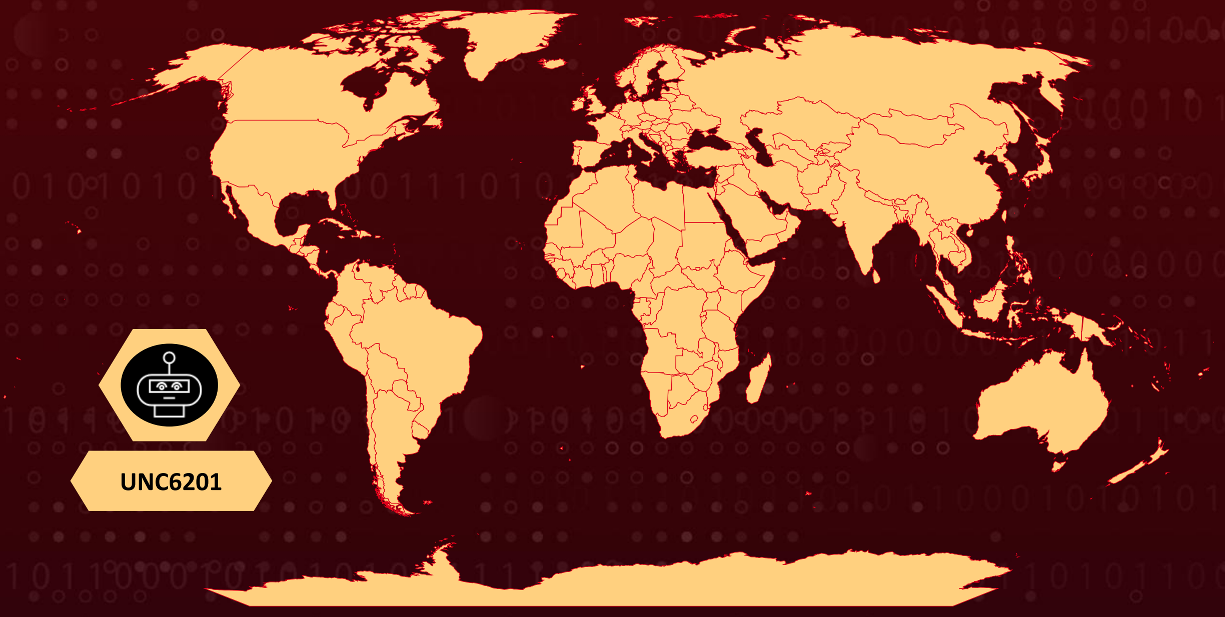
CVE-2026-22769: UNC6201 Exploiting Dell RecoverPoint Zero-Day

Date of Publication	Admiralty Code	TA Number
February 19, 2026	A1	TA2026049

Summary

First Seen: Mid - 2024
Targeted Regions: Worldwide
Targeted Platforms: Linux, VMware ESXi/vCenter
Targeted Products: Dell RecoverPoint for Virtual Machines
Threat Actor: UNC6201
Malware: BRICKSTORM, GRIMBOLT, SLAYSTYLE
Attack: UNC6201 has been exploiting a critical zero-day (CVE-2026-22769) in Dell Technologies RecoverPoint for Virtual Machines since at least mid-2024, enabling unauthenticated root-level access to trusted infrastructure appliances. The activity shows overlaps with UNC5221 (also reported as Silk Typhoon) and is assessed as part of a broader PRC-aligned intelligence collection effort. Post-exploitation involved deployment of SLAYSTYLE, BRICKSTORM, and the newer GRIMBOLT backdoor, reflecting sustained capability development and stealth-focused tradecraft. The campaign persisted undetected for over a year, highlighting monitoring gaps in internal infrastructure and the need for urgent patching, forensic validation, and threat hunting.

Attack Regions



🟨 Targeted 🟥 Non-Targeted

Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-22769	Dell RecoverPoint for Virtual Machines (RP4VMs) Use of Hard-coded Credentials Vulnerability	Dell RecoverPoint for Virtual Machines	✓	✓	✓

Attack Details

#1 The China-nexus threat cluster UNC6201 has been actively exploiting a critical zero-day vulnerability in Dell Technologies RecoverPoint for Virtual Machines since at least mid-2024. Notable overlaps exist between UNC6201 and UNC5221 (aka Silk Typhoon), a group previously linked to campaigns targeting government agencies with custom malware and known for embedding itself within critical U.S. infrastructure networks. However, the clusters are not currently assessed as identical. This activity is assessed to form part of a broader PRC-aligned intelligence collection effort.

#2 The vulnerability (CVE-2026-22769), rated CVSS 10.0, stems from hard-coded default credentials for the administrative account in the embedded Apache Tomcat Manager component, enabling unauthorized remote access. Successful exploitation allows attackers to upload malicious payloads and achieve root-level command execution on the appliance, which typically resides in trusted and sensitive network segments, increasing its value for follow-on operations.

#3 Following initial access, UNC6201 deployed the SLAYSTYLE Java web shell to establish persistence and deliver additional payloads. Earlier intrusions leveraged the BRICKSTORM backdoor, while more recent activity introduced GRIMBOLT, a backdoor written in C# and compiled using Native AOT to remove intermediate language metadata commonly leveraged in static analysis. GRIMBOLT is further packed with UPX and communicates over WebSocket with the same command-and-control infrastructure used by BRICKSTORM, suggesting iterative capability development and sustained operational investment.

#4 UNC6201 demonstrated disciplined tradecraft in persistence and lateral movement. The group modified the legitimate boot-time script convert_hosts.sh, executed via rc.local, to ensure malware execution upon reboot. It also created temporary virtual network adapters, referred to as “Ghost NICs”, on existing virtual machines running on ESXi hosts to pivot into internal networks and SaaS environments while minimizing forensic artifacts. On compromised vCenter appliances, iptables-based single packet authorization was implemented to restrict backdoor access on port 10443 to pre-authenticated source IPs within a limited time window, effectively evading scanning and network monitoring controls.

#5 The campaign operated undetected for over a year, underscoring persistent monitoring gaps around internal infrastructure appliances. Dell has since issued patches and security advisories. Organizations should conduct thorough forensic reviews, inspect Tomcat Manager logs for unauthorized deployments, validate the integrity of startup scripts, and monitor for indicators of compromise associated with SLAYSTYLE, BRICKSTORM, and GRIMBOLT to ensure complete remediation.

Recommendations

Patch and Harden Dell RecoverPoint Appliances: Apply the remediation provided in the official Dell security advisory for CVE-2026-22769 immediately. Change all default and hard-coded credentials on the appliance, disable or restrict access to the Tomcat Manager interface, and ensure the appliance is running the latest supported firmware version.

Conduct Forensic Review of Existing Deployments: Inspect all Dell RecoverPoint for Virtual Machines instances for signs of compromise. Review Tomcat Manager audit logs at /home/kos/auditlog/fapi_cl_audit_log.log for unauthorized deployment requests, check for unexpected WAR files in /var/lib/tomcat9 and compiled artifacts in /var/cache/tomcat9/Catalina, and verify the integrity of /home/kos/kbox/src/installation/distribution/convert_hosts.sh for unauthorized modifications.

Monitor VMware Virtual Infrastructure: Audit ESXi and vCenter environments for unauthorized changes to virtual machine network configurations, including the creation of unexpected virtual network adapters. Review vCenter appliance iptables rules for anomalous NAT or traffic redirection entries, particularly rules referencing non-standard ports such as 10443.

Restrict Network Access to Management Interfaces: Ensure that management interfaces for Dell RecoverPoint, Tomcat Manager, vCenter, and ESXi are not exposed to broad network segments. Apply strict network segmentation and firewall rules to limit access to authorized administrative hosts only.

Deploy Detection Rules and Hunt for IOCs: Incorporate the published YARA rules for GRIMBOLT, BRICKSTORM, and SLAYSTYLE into endpoint detection workflows. Sweep environments for known file hashes and network indicators, including WebSocket-based C2 communications to identified infrastructure. Monitor for DNS-over-HTTPS activity from unexpected endpoints.

Review Startup and Boot Persistence Mechanisms: Audit rc.local and associated boot-time scripts across all Linux-based appliances in the environment. Establish baseline integrity checks for these files and alert on any unauthorized modifications.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
	T1078: Valid Accounts	T1078.001: Default Accounts
Execution	T1059: Command and Scripting Interpreter	
Persistence	T1037: Boot or Logon Initialization Scripts	T1037.004: RC Scripts
	T1505: Server Software Component	T1505.003: Web Shell
Defense Evasion	T1027: Obfuscated Files or Information	T1027.002: Software Packing
	T1205: Traffic Signaling	T1205.001: Port Knocking
Lateral Movement	T1021: Remote Services	
	T1599: Network Boundary Bridging	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1572: Protocol Tunneling	
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
Resource Development	T1587: Develop Capabilities	T1587.001: Malware
	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	24a11a26a2586f4fba7bfe89df2e21a0809ad85069e442da98c37c4add369a0c, dfb37247d12351ef9708cb6631ce2d7017897503657c6b882a711c0da8a9a591, 92fb4ad6dee9362d0596fda7bbcfe1ba353f812ea801d1870e37bfc6376e624a, aa688682d44f0c6b0ed7f30b981a609100107f2d414a3a6e5808671b112d1878, 2388ed7aee0b6b392778e8f9e98871c06499f476c9e7eae6ca0916f827fe65df, 320a0b5d4900697e125cebb5ff03dee7368f8f087db1c1570b0b62f5a986d759, 90b760ed1d0dcb3ef0f2b6d6195c9d852bcb65eca293578982a8c4b64f51b035, 45313a6745803a7f57ff35f5397fdf117eaec008a76417e6e2ac8a6280f7d830
IPv4	149[.]248[.]11[.]71
File Path	/home/kos/kbox/src/installation/distribution/convert_hosts.sh, /home/kos/tomcat9/tomcat-users.xml

Patch Link

https://www.dell.com/support/kbdoc/en-in/000426773/dsa-2026-079

References

https://www.dell.com/support/kbdoc/en-in/000426773/dsa-2026-079

https://cloud.google.com/blog/topics/threat-intelligence/unc6201-exploiting-dell-recoverpoint-zero-day/

https://hivepro.com/threat-advisory/brickstorm-breaks-in-chinas-quiet-grip-on-us-virtual-stack/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.

Contextualize
Uni5 Threat Exposure Management
Resolve
Prioritize

REPORT GENERATED ON

February 19, 2026 ● 06:00 AM

More at www.hivepro.com