AUTORITETI KOMBËTAR
PËR SIGURINË KIBERNETIKE

Dobësi e shfrytëzuar në mënyrë aktive në Dell RecoverPoint për Makinat Virtuale

Data: 19/02/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive 2
Informacione Teknike 2
Rekomandime 3

Përmbledhje Ekzekutive

Një dobësi kritike zero-day është shfrytëzuar në mënyrë aktive kundër Dell RecoverPoint për Virtual Machines (RP4VM), një pajisje për backup dhe disaster recovery e përqendruar në VMware.

Informacione Teknike

Një dobësi kritike zero-day, CVE-2026-22769 (CVSS 10.0), është shfrytëzuar në mënyrë aktive kundër Dell RecoverPoint for Virtual Machines (RP4VM), një pajisje e përqendruar në VMware për backup dhe rikuperim nga fatkeqësitë.

• CVE-2026-22769
• Rezultati CVSS: 10.0 (Kritik)
• Produkti i prekur: Dell RecoverPoint for Virtual Machines (para 6.0.3.1 HF1) Dobësia, e cila i atribuohet një dobësie të koduar në kredenciale, u mundëson sulmuesve të paautorizuar në distancë të fitojnë akses në nivelin root në pajisjet e prekura. Aktiviteti i kërcënimit është lidhur me UNC6201, me shfrytëzim të vërejtur që nga mesi i vitit 2024.

Aktiviteti pas shfrytëzimit përfshin:
• Vendosjen e familjeve të programeve keqdashëse të personalizuara BRICKSTORM dhe GRIMBOLT
• Implementimin e shell-it të uebit (SLAYSTYLE)
• Lëvizjen anësore të VMware ESXi nëpërmjet teknikës "Ghost NIC"
• Qëndrueshmërinë dhe ndryshimin e mundshëm të SaaS

Produkti	Versioni i afektuar	Mitigimit
RecoverPoint for Virtual Machines	Version 5.3 SP4 P1	Migrate from RecoverPoint for Virtual Machines 5.3 SP4 P1 to 6.0 SP3 Përditëso në 6.0.3.1 HF1
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	Përditëso në 6.0.3.1 HF1

Rekomandime

AKSK rekomandon të përditësoni menjëherë Dell RecoverPoint për Makinat Virtuale në versionin e përditësuar.