مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-Dell Data Protection Central

Tracking #:432318728

Date:06-04-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Dell has released security updates addressing multiple critical vulnerabilities in Data Protection Central (DPC) and Integrated Data Protection Appliance (IDPA) environments.

TECHNICAL DETAILS:

Dell has released security updates addressing multiple critical vulnerabilities in Data Protection Central (DPC) and Integrated Data Protection Appliance (IDPA) environments. The vulnerabilities originate primarily from the underlying SUSE Linux Enterprise Server 12 SP5 (SLES 12 SP5) third-party components. Successful exploitation could allow attackers to compromise affected systems, potentially leading to remote code execution, privilege escalation, denial of service, or data exposure.

Details:

Critical Vulnerability Highlights (Selective)

Below are representative critical/high-impact CVEs relevant to exploitation risk:

- CVE-2026-23004
  - Type: Kernel-level vulnerability
  - Impact: Privilege escalation / potential full system compromise
- CVE-2026-23083 / CVE-2026-23084 / CVE-2026-23085 / CVE-2026-23086
  - Type: Memory handling flaws in core components
  - Impact: Remote code execution (RCE) or denial of service
- CVE-2026-22998 / CVE-2026-22999
  - Type: Improper input validation
  - Impact: Unauthorized access / execution
- CVE-2026-23105 / CVE-2026-23112
  - Type: Privilege boundary bypass
  - Impact: Escalation to root-level access
- CVE-2025-40055 / CVE-2025-40064
  - Type: Kernel vulnerabilities
  - Impact: Arbitrary code execution
- CVE-2024-26935
  - Type: Linux kernel flaw
  - Impact: Potential local privilege escalation

Note: The advisory aggregates a large vulnerability set across multiple years, increasing cumulative risk due to attack chaining.

Affected Products:

- Dell Data Protection Central
  - Versions: 19.9.x, 19.10.x, 19.11.x, 19.12.x
- PowerProtect DP Series (IDPA)
  - Versions: Prior to 2.7.9

Fixed Versions:

- DPC: Versions 19.9–19.12 with latest OS update
- IDPA: Version 2.7.9 with updated OS

RECOMMENDATIONS:

- Patch Immediately: Deploy the latest OS update across all affected systems.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.dell.com/support/kbdoc/en-us/000449107/dsa-2026-173-security-update-for-dell-data-protection-central-multiple-third-party-component-vulnerabilities