



Search Dell or identify your p

Create and access a list of your products

Your Dell.com Carts

- Products
- Solutions
- Services
- Support
- < Back
- Support Home
- Support Library
- Support Videos
- Support Services & Warranty
- Drivers & Downloads
- Manuals & Documentation
- PC Diagnostics
- Self-Repair & Parts
- Service Requests & Dispatch Status
- Order Support
- Contact Technical Support
- Community
- Contact Us

- Sign In
- Create an Account
- Premier Sign In
- Dell Financial Services
- Partner Program Sign In

US/EN >

< Back

Home / Support Home / Knowledge Base Article

Print Email Alert English

DSA-2026-158: Security Update Dell PowerProtect Data Manager for Multiple Security Vulnerabilities

Summary: Dell PowerProtect Data Manager remediation is available for multiple security vulnerabilities that could be exploited by malicious users to compromise the affected system.

Detailed Article ^

- Impact
- Details
- Affected Products & Remediation
- Revision History
- Related Info

Legal Disclaimer

Affected Products

Provide Feedback

Please select a product to check article relevancy X Identify Your Product v

Impact

Critical


Details

Third-party Component	CVEs	More Information
PPDM Core: Logback	CVE-2025-11226, CVE-2024-12801, CVE-2024-12798	https://nvd.nist.gov/vuln/search 🔗
Apache Tomcat	CVE-2025-61795	https://nvd.nist.gov/vuln/search 🔗
Spring Framework	CVE-2025-22235, CVE-2025-41249, CVE-2025-22233	https://nvd.nist.gov/vuln/search 🔗
Spring Security	CVE-2025-22228	https://nvd.nist.gov/vuln/search 🔗
Apache Commons FileUpload	CVE-2025-48976	https://nvd.nist.gov/vuln/search 🔗
json-smart	CVE-2024-57699	https://nvd.nist.gov/vuln/search 🔗
reactor-netty	CVE-2025-22227	https://nvd.nist.gov/vuln/search 🔗
Apache Log4j	CVE-2025-68161	https://nvd.nist.gov/vuln/search 🔗
AssertJ - Fluent Assertions for Java	CVE-2026-24400	https://nvd.nist.gov/vuln/search 🔗
PPDM Reporting: Infinispan	CVE-2025-5731	https://nvd.nist.gov/vuln/search 🔗
Logback	CVE-2025-11226	https://nvd.nist.gov/vuln/search 🔗

Third-party Component	CVEs	More Information
Netty Project	CVE-2025-59419	https://nvd.nist.gov/vuln/search 🔗
OpenSSH	CVE-2016-20012, CVE-2020-14145, CVE-2021-28041, CVE-2021-36368, CVE-2023-38408, CVE-2023-48795, CVE-2025-26465	https://nvd.nist.gov/vuln/search 🔗
Spring Framework	CVE-2025-41254	https://nvd.nist.gov/vuln/search 🔗
XMLUnit	CVE-2024-31573	https://nvd.nist.gov/vuln/search 🔗
Angular	CVE-2025-59052	https://nvd.nist.gov/vuln/search 🔗
brace-expansion	CVE-2025-5889	https://nvd.nist.gov/vuln/search 🔗
crypto/tls	CVE-2025-68121	https://nvd.nist.gov/vuln/search 🔗
Operating System (OS)	CVE-2026-0672, CVE-2026-0865, CVE-2026-0861, CVE-2026-0915, CVE-2026-22695, CVE-2026-22801, CVE-2026-25646, CVE-2026-24882, CVE-2026-22795, CVE-2026-22796, CVE-2025-11187, CVE-2025-15467, CVE-2025-15468, CVE-2025-15469, CVE-2025-66199, CVE-2025-68160, CVE-2025-69418, CVE-2025-69419, CVE-2025-69420, CVE-2025-69421, CVE-2026-26157, CVE-2026-26158, CVE-2026-23490, CVE-2026-21925, CVE-2026-21932, CVE-2026-21933, CVE-2026-21945, CVE-2025-40257, CVE-2025-40259, CVE-2025-68284, CVE-2025-68285, CVE-2025-68775, CVE-2025-68813, CVE-2025-71085, CVE-2026-22999, CVE-2026-23001, CVE-2026-23010	https://nvd.nist.gov/vuln/search 🔗

Proprietary Code CVEs	Description	CVSS Base Score	CVSS Vector String
CVE-2026-28266	Dell PowerProtect Agent Service, version(s) prior to 20.1, contain(s) a Weak Encoding for Password vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Unauthorized access.	7.1	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N ☐
CVE-2026-28264	Dell PowerProtect Agent Service, version(s) prior to 20.1, contain(s) an Incorrect Permission Assignment for Critical Resource vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information exposure.	3.3	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N ☐

Proprietary Code CVEs	Description	CVSS Base Score	CVSS Vector String
CVE-2026-28266	Dell PowerProtect Agent Service, version(s) prior to 20.1, contain(s) a Weak Encoding for Password vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Unauthorized access.	7.1	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N ☐
CVE-2026-28264	Dell PowerProtect Agent Service, version(s) prior to 20.1, contain(s) an Incorrect Permission Assignment for Critical Resource vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information exposure.	3.3	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N ☐

 Dell Technologies recommends all customers consider both the CVSS base score and any relevant temporal and environmental scores that may impact the potential severity associated with a particular security vulnerability.

Affected Products & Remediation

Product	Affected Versions	Remediated Versions	Link
Dell PowerProtect Data Manager	Versions prior to 20.1.0.0	Version 20.1.0.0 or later	PPDM 20.1.0.0 drivers and downloads

Product	Affected Versions	Remediated Versions	Link
Dell PowerProtect Data Manager	Versions prior to 20.1.0.0	Version 20.1.0.0 or later	PPDM 20.1.0.0 drivers and downloads

Revision History

Revision	Date	Description
1.0	2026-04-01	Initial Release
2.0	2026-04-04	Updated for enhanced presentation
3.0	2026-04-07	Updated the Third Party Components section to include CVE-2025-68121
4.0	2026-04-14	Updated the Proprietary Code section to included CVE-2026-28266

Related Information

[Dell Security Advisories and Notices](#)

[Dell Vulnerability Response Policy](#)

[CVSS Scoring Guide](#)

Legal Disclaimer

Affected Products

PowerProtect Data Manager Appliance, PowerProtect Data Manager, PowerProtect Data Manager Essentials, PowerProtect Data Manager Software

Article Properties

Article Number: 000447277

Article Type: Dell Security Advisory

Last Modified: 14 Apr 2026

Find answers to your questions from other Dell users

[Visit Community](#)

Support Services

Check if your device is covered by Support Services.

[Check Support Status](#)

US/EN	Account	Support	Connect with Us	Site Map
Site Map	My Account	Support Home	Community	US/EN
	Order Status	Contact Technical Support	Contact Us	
	Profile Settings	Returns	X (Twitter)	
	My Products		LinkedIn	
	Make a Payment		Instagram	
	Dell Rewards Balance		YouTube	
Our Offerings	Our Company	Our Partners	Resources	
Artificial Intelligence	Who We Are	Find a Partner	Blog	
Products	Careers	Find a Reseller	Dell Rewards	
Solutions	Dell Technologies Capital	OEM Solutions	Events	
Services	Investors	Partner Program	Email Sign-Up	
Deals	Newsroom		Specialty Product Collections	
	Recycling		Privacy Center	
	Corporate Impact		Security & Trust Center	
	Customer Stories		Trial Software Downloads	
Dell Technologies	Dell Premier for Business	Dell Financial Services		
Copyright © 2026 Dell Inc.	Terms of Sale	Privacy Statement	Do Not Sell or Share My Personal Information	
Cookies, Ads & Emails	Legal & Regulatory	Accessibility	Anti-Slavery, Human Trafficking & Child Labor	