



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

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









Identify Your Product


## Impact


Critical


## Details

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

Third-party Component	CVEs	More Information
Netty Project	CVE-2025-59419	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
OpenSSH	CVE-2016-20012, CVE-2020-14145, CVE-2021-28041, CVE-2021-36368, CVE-2023-38408, CVE-2023-48795, CVE-2025-26465	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
Spring Framework	CVE-2025-41254	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
XMLUnit	CVE-2024-31573	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
Angular	CVE-2025-59052	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
brace-expansion	CVE-2025-5889	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
crypto/tls	CVE-2025-68121	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
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	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 

Proprietary Code CVEs	Description	CVSS Base Score	CVSS Vector String
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	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N</a> 

Proprietary Code CVEs	Description	CVSS Base Score	CVSS Vector String
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	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N</a> 

 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	<a href="#">PPDM 20.1.0.0 drivers and downloads</a>

Product	Affected Versions	Remediated Versions	Link
Dell PowerProtect Data Manager	Versions prior to 20.1.0.0	Version 20.1.0.0 or later	<a href="#">PPDM 20.1.0.0 drivers and downloads</a>

## 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 CVE Identifier, Third Party Components sections to include CVE-2025-68121

## Related Information

[Dell Security Advisories and Notices](#)

[Dell Vulnerability Response Policy](#)

[CVSS Scoring Guide](#)

## Legal Disclaimer

The information in this Dell Technologies Security Advisory should be read and used to assist in avoiding situations that may arise from the problems described herein. Dell Technologies distributes Security Advisories to bring important security information to the attention of users of the affected product(s). Dell Technologies assesses the risk based on an average of risks across a diverse set of installed systems and may not represent the actual risk to your local installation and individual environment. It is recommended that all users determine the applicability of this information to their individual environments and take appropriate actions. The information set forth herein is provided "as is" without warranty of any kind. Dell Technologies expressly disclaims all warranties, either express or implied, including the warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Dell Technologies, its affiliates or suppliers, be liable for any damages whatsoever arising from or related to the information contained herein or actions that you decide to take based thereon, including any direct, indirect, incidental, consequential, loss of business profits or special damages, even if Dell Technologies, its affiliates or suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages, so the foregoing limitation shall apply to the extent permissible under law.

## 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:** 08 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](#)

<a href="#">US/EN</a>	<b>Account</b> Account	<b>Support</b> Support	<b>Connect with Us</b> Connect with Us	Site Map
<a href="#">Site Map</a>	<a href="#">My Account</a>	<a href="#">Support Home</a>	<a href="#">Community</a>	<a href="#">US/EN</a>
<a href="#">Order Status</a>	<a href="#">Profile Settings</a>	<a href="#">Contact Technical Support</a>	<a href="#">Contact Us</a>	
<a href="#">My Products</a>	<a href="#">Make a Payment</a>	<a href="#">Returns</a>	<a href="#">X (Twitter)</a>	
<a href="#">Dell Rewards Balance</a>			<a href="#">LinkedIn</a>	
			<a href="#">Instagram</a>	
			<a href="#">YouTube</a>	
<b>Our Offerings</b> Our Offerings	<b>Our Company</b> Our Company	<b>Our Partners</b> Our Partners	<b>Resources</b> Resources	
<a href="#">Artificial Intelligence</a>	<a href="#">Who We Are</a>	<a href="#">Find a Partner</a>	<a href="#">Blog</a>	
<a href="#">Products</a>	<a href="#">Careers</a>	<a href="#">Find a Reseller</a>	<a href="#">Dell Rewards</a>	
<a href="#">Solutions</a>	<a href="#">Dell Technologies Capital</a>	<a href="#">OEM Solutions</a>	<a href="#">Events</a>	

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
<b>Dell Technologies</b>	<b>Dell Premier for Business</b>	<b>Dell Financial Services</b>	
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