



Search Dell or identify your p

- 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

Your Dell.com Carts

US/EN >

< Back

Home / Support Home / Knowledge Base Article

Print Email Alert English

## DSA-2025-347: Security Update for Dell PowerScale OneFS Multiple Vulnerabilities

Summary: Dell PowerScale OneFS 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

Medium

### Details

Proprietary Code CVEs	Description	CVSS Base Score	CVSS Vector String
CVE-2025-43937	Dell PowerScale OneFS, versions prior to 9.12.0.0, contains an insertion of sensitive information into log file vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable application with privileges of the compromised account.	6.6	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:H</a> ☐
CVE-2025-43935	Dell PowerScale OneFS, versions prior to 9.12.0.0, contains an improper resource shutdown or release vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to denial of service.	4.4	<a href="#">CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H</a> ☐
CVE-2025-43724	Dell PowerScale OneFS, versions prior to 9.12.0.0, contains an authorization bypass through user-controlled key vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability to gain unauthorized access to NFSv4 or SMB shares.	4.2	<a href="#">CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L</a> ☐
CVE-2025-43883	Dell PowerScale OneFS, versions prior to 9.12.0.0, contains an improper check for unusual or exceptional conditions vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to denial of service.	4.1	<a href="#">CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H</a> ☐

Proprietary Code CVEs	Description	CVSS Base Score	CVSS Vector String
CVE-2025-43937	Dell PowerScale OneFS, versions prior to 9.12.0.0, contains an insertion of sensitive information into log file vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable application with privileges of the compromised account.	6.6	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:H</a> ☐
CVE-2025-43935	Dell PowerScale OneFS, versions prior to 9.12.0.0, contains an improper resource shutdown or release vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to denial of service.	4.4	<a href="#">CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H</a> ☐
CVE-2025-43724	Dell PowerScale OneFS, versions prior to 9.12.0.0, contains an authorization bypass through user-controlled key vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability to gain unauthorized access to NFSv4 or SMB shares.	4.2	<a href="#">CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L</a> ☐

CVE-2025-43883	Dell PowerScale OneFS, versions prior to 9.12.0.0, contains an improper check for unusual or exceptional conditions vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to denial of service.	4.1	<a href="#">CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H</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
PowerScale OneFS	Versions 9.5.0.0 through 9.10.1.2	Versions 9.10.1.3 or later	<a href="#">PowerScale OneFS Downloads Area</a>
PowerScale OneFS	Versions prior to 9.12.0.0	Versions 9.12.0.0 or later	<a href="#">PowerScale OneFS Downloads Area</a>
PowerScale OneFS	Versions 9.7.0.0 through 9.7.1.9	Versions 9.7.1.10 or later	<a href="#">PowerScale OneFS Downloads Area</a>
PowerScale OneFS	Versions 9.5.0.0 through 9.5.1.4	Versions 9.5.1.5 or later	<a href="#">PowerScale OneFS Downloads Area</a>

Product	Affected Versions	Remediated Versions	Link
PowerScale OneFS	Versions 9.5.0.0 through 9.10.1.2	Versions 9.10.1.3 or later	<a href="#">PowerScale OneFS Downloads Area</a>
PowerScale OneFS	Versions prior to 9.12.0.0	Versions 9.12.0.0 or later	<a href="#">PowerScale OneFS Downloads Area</a>
PowerScale OneFS	Versions 9.7.0.0 through 9.7.1.9	Versions 9.7.1.10 or later	<a href="#">PowerScale OneFS Downloads Area</a>
PowerScale OneFS	Versions 9.5.0.0 through 9.5.1.4	Versions 9.5.1.5 or later	<a href="#">PowerScale OneFS Downloads Area</a>

### Notes:

1. We encourage all customers to adopt the Long-Term Support (LTS) 2025 version which is 9.10.1.x code line, with the latest maintenance release.
2. For more information on LTS code lines, see [Dell Infrastructure Solutions Group \(ISG\) LTS Release Support Customer Summary](#) and [Security Update Release Schedule for Supported Versions of Dell PowerScale OneFS](#).

## Revision History

Revision	Date	Description
1.0	2025-10-01	Initial Release
1.0	2025-10-08	Minor formatting adjustments

## 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

PowerScale OneFS

### Article Properties

**Article Number:** 000376214

**Article Type:** Dell Security Advisory

**Last Modified:** 08 Oct 2025

### 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](#)

## Provide Feedback

Accurate



Useful



Easy to Understand



Was this article helpful?

Yes No radio buttons

Additional Information (optional)

0/3000 characters

Text input field for additional information

Letters, numbers and any special characters except < > ( ) \

Submit Feedback button

<a href="#">US/EN</a>	<a href="#">Account</a>	<a href="#">Support</a>	<a href="#">Connect with Us</a>	<a href="#">Site Map</a>
<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="#">Contact Technical Support</a>	<a href="#">Contact Us</a>	
<a href="#">Profile Settings</a>		<a href="#">Returns</a>	<a href="#">X (Twitter)</a>	
<a href="#">My Products</a>			<a href="#">LinkedIn</a>	
<a href="#">Make a Payment</a>			<a href="#">Instagram</a>	
<a href="#">Dell Rewards Balance</a>			<a href="#">YouTube</a>	
<a href="#">Our Offerings</a>	<a href="#">Our Company</a>	<a href="#">Our Partners</a>	<a href="#">Resources</a>	
<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>	
<a href="#">Services</a>	<a href="#">Investors</a>	<a href="#">Partner Program</a>	<a href="#">Email Sign-Up</a>	
<a href="#">Deals</a>	<a href="#">Newsroom</a>		<a href="#">Specialty Product Collections</a>	
	<a href="#">Recycling</a>		<a href="#">Privacy Center</a>	
	<a href="#">Corporate Impact</a>		<a href="#">Security &amp; Trust Center</a>	
	<a href="#">Customer Stories</a>		<a href="#">Trial Software Downloads</a>	
<a href="#">Dell Technologies</a>	<a href="#">Dell Premier for Business</a>	<a href="#">Dell Financial Services</a>		
<a href="#">Copyright © 2026 Dell Inc.</a>	<a href="#">Terms of Sale</a>	<a href="#">Privacy Statement</a>	<a href="#">Do Not Sell or Share My Personal Information</a>	
<a href="#">Cookies, Ads &amp; Emails</a>	<a href="#">Legal &amp; Regulatory</a>	<a href="#">Accessibility</a>	<a href="#">Anti-Slavery, Human Trafficking &amp; Child Labor</a>	