



Search Dell or identify your p

- Enjoy members-only rewards and discounts
- 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
- Partner Program Sign In

SG/EN >

< Back

Some article numbers may have changed. If this isn't what you're looking for, try searching all articles. [Search articles](#)

Home / Support Home / Knowledge Base Article

Print Email Alert English

## DSA-2026-038: 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.

|                                 |   |
|---------------------------------|---|
| <b>Detailed Article</b>         | ^ |
| Impact                          |   |
| Details                         |   |
| Affected Products & Remediation |   |
| Workarounds & Mitigations       |   |
| 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-2026-21421        | Dell PowerScale OneFS, versions prior to 9.10.1.6 and versions 9.11.0.0 through 9.12.0.1, contains an execution with unnecessary privileges vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to elevation of privileges.  | 6.7             | <a href="#">CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H</a><br>☑ |
| CVE-2026-22270        | Dell PowerScale OneFS, versions prior to 9.10.1.6 and versions 9.11.0.0 through 9.12.0.1, contains an uncontrolled search path element vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to denial of service, elevation of privileges, and information disclosure.              | 6.7             | <a href="#">CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H</a><br>☑ |
| CVE-2026-21423        | Dell PowerScale OneFS, versions prior to 9.10.1.6 and versions 9.11.0.0 through 9.12.0.1, contains an incorrect default permissions vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to code execution, denial of service, elevation of privileges, and information disclosure. | 6.7             | <a href="#">CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H</a><br>☑ |
| CVE-2026-21424        | Dell PowerScale OneFS, versions prior to 9.10.1.6 and versions 9.11.0.0 through 9.12.0.1, contains an execution with unnecessary privileges vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.  | 6.7             | <a href="#">CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H</a><br>☑ |
| CVE-2026-21425        | Dell PowerScale OneFS, versions prior to 9.10.1.6 and versions 9.11.0.0 through 9.12.0.1, contains an incorrect privilege assignment vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.  | 6.7             | <a href="#">CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H</a><br>☑ |
| CVE-2026-21426        | Dell PowerScale OneFS, versions prior to 9.10.1.6 and versions 9.11.0.0 through 9.12.0.1, contains an execution with unnecessary privileges vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to denial of service, elevation of privileges, and information disclosure.         | 6.7             | <a href="#">CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H</a><br>☑ |
| CVE-2026-21422        | Dell PowerScale OneFS, versions 9.10.0.0 through 9.13.1.0, contains an external control of system or configuration setting vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to protection mechanism bypass.   | 3.4             | <a href="#">CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:L</a><br>☑ |

| Proprietary Code CVEs | Description  | CVSS Base Score | CVSS Vector String  |
|-----------------------|--|-----------------|---|
| CVE-2026-21421        | Dell PowerScale OneFS, versions prior to 9.10.1.6 and versions 9.11.0.0 through 9.12.0.1, contains an execution with unnecessary privileges vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to elevation of privileges.  | 6.7             | <a href="#">CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H</a><br>☑ |
| CVE-2026-22270        | Dell PowerScale OneFS, versions prior to 9.10.1.6 and versions 9.11.0.0 through 9.12.0.1, contains an uncontrolled search path element vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to denial of service, elevation of privileges, and information disclosure.              | 6.7             | <a href="#">CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H</a><br>☑ |
| CVE-2026-21423        | Dell PowerScale OneFS, versions prior to 9.10.1.6 and versions 9.11.0.0 through 9.12.0.1, contains an incorrect default permissions vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to code execution, denial of service, elevation of privileges, and information disclosure. | 6.7             | <a href="#">CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H</a><br>☑ |
| CVE-2026-21424        | Dell PowerScale OneFS, versions prior to 9.10.1.6 and versions 9.11.0.0 through 9.12.0.1, contains an execution with unnecessary privileges vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.  | 6.7             | <a href="#">CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H</a><br>☑ |
| CVE-2026-21425        | Dell PowerScale OneFS, versions prior to 9.10.1.6 and versions 9.11.0.0 through 9.12.0.1, contains an incorrect privilege assignment vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.  | 6.7             | <a href="#">CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H</a><br>☑ |
| CVE-2026-21426        | Dell PowerScale OneFS, versions prior to 9.10.1.6 and versions 9.11.0.0 through 9.12.0.1, contains an execution with unnecessary privileges vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to denial of service, elevation of privileges, and information disclosure.         | 6.7             | <a href="#">CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H</a><br>☑ |
| CVE-2026-21422        | Dell PowerScale OneFS, versions 9.10.0.0 through 9.13.1.0, contains an external control of system or configuration setting vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to protection mechanism bypass.   | 3.4             | <a href="#">CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:L</a><br>☑ |

⚠ 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

| CVEs Addressed   | Product          | Affected Versions                  | Remediated Versions       | Link  |
|--|------------------|------------------------------------|---------------------------|---|
| CVE-2026-21421, CVE-2026-22270, CVE-2026-21423, CVE-2026-21424, CVE-2026-21425, CVE-2026-21426                 | PowerScale OneFS | Versions prior to 9.10.1.6         | Version 9.10.1.6 or later | <a href="#">PowerScale OneFS Downloads Area</a> |
| CVE-2026-21421, CVE-2026-22270, CVE-2026-21423, CVE-2026-21424, CVE-2026-21425, CVE-2026-21426, CVE-2026-21422 | PowerScale OneFS | Versions 9.11.0.0 through 9.12.0.1 | Version 9.13.0.0 or later | <a href="#">PowerScale OneFS Downloads Area</a> |
| CVE-2026-21422   | PowerScale OneFS | Version 9.10.0.0 through 9.13.1.0  | Version 9.14.0.0 or later | <a href="#">PowerScale OneFS Downloads Area</a> |

| CVEs Addressed   | Product          | Affected Versions                  | Remediated Versions       | Link  |
|--|------------------|------------------------------------|---------------------------|---|
| CVE-2026-21421, CVE-2026-22270, CVE-2026-21423, CVE-2026-21424, CVE-2026-21425, CVE-2026-21426                 | PowerScale OneFS | Versions prior to 9.10.1.6         | Version 9.10.1.6 or later | <a href="#">PowerScale OneFS Downloads Area</a> |
| CVE-2026-21421, CVE-2026-22270, CVE-2026-21423, CVE-2026-21424, CVE-2026-21425, CVE-2026-21426, CVE-2026-21422 | PowerScale OneFS | Versions 9.11.0.0 through 9.12.0.1 | Version 9.13.0.0 or later | <a href="#">PowerScale OneFS Downloads Area</a> |
| CVE-2026-21422   | PowerScale OneFS | Version 9.10.0.0 through 9.13.1.0  | Version 9.14.0.0 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](#).

### Workarounds & Mitigations

| CVE ID | Workaround and Mitigations |
|--------|----------------------------|
|        |                            |

|                |   |
|----------------|---|
| CVE-2026-21422 | <p><b>Issue:</b></p> <p>During the first time installation of Dell PowerScale OneFS versions 9.10.0.0 through 9.13.1.0, the initial run of the Security Checker will reset the SSH configuration to default settings.</p> <p><b>Note:</b> Systems that reach these versions through an upgrade path retain their existing (custom) SSH configuration and are therefore not affected.</p> <p><b>Remediation:</b></p> <p>Customers who intend to modify the default SSH settings must allow Security Checker to complete its first run before applying any custom SSH settings. To do this, run the following commands:</p> <ol style="list-style-type: none"> <li>1. Start the Security Checker:</li> </ol> <pre>isi security check start</pre> <ol style="list-style-type: none"> <li>2. Verify completion:</li> </ol> <pre>isi security check status</pre> <ol style="list-style-type: none"> <li>3. Once the Security Checker has successfully completed, SSH configuration changes can be applied safely without being overwritten.</li> </ol> |
|----------------|---|

## Revision History

| Revision | Date       | Description   |
|----------|------------|---|
| 1.0      | 2026-02-25 | Initial Release   |
| 2.0      | 2026-04-29 | Major update: Revised affected version range and mitigation guidance for CVE-2026-21422 |

## Related Information

[Dell Security Advisories and Notices](#)

[Dell Vulnerability Response Policy](#)

[CVSS Scoring Guide](#)

## Legal Disclaimer

## Affected Products

PowerScale OneFS

### Article Properties

**Article Number:** 000432452

**Article Type:** Dell Security Advisory

**Last Modified:** 29 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](#)

## Provide Feedback

#### Accurate



#### Useful



#### Easy to Understand



#### Was this article helpful?

Yes  No

Additional Information (optional)

0/3000 characters

Text input area for additional feedback information.

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

[Submit Feedback](#)

|                               |                             |                              |                                 |                          |
|-------------------------------|-----------------------------|------------------------------|---------------------------------|--------------------------|
| <a href="#">SG/EN</a>         | <a href="#">Account</a>     | <a href="#">Support</a>      | <a href="#">Connect with Us</a> | <a href="#">Site Map</a> |
| Site Map                      | My Account                  | Support Home                 | Community                       | SG/EN                    |
| Order Status                  |                             | Contact Technical Support    | Contact Us                      |                          |
| Profile Settings              |                             | Returns                      |                                 |                          |
| My Products                   |                             |                              |                                 |                          |
| Dell Rewards Balance          |                             |                              |                                 |                          |
| <a href="#">Our Offerings</a> | <a href="#">Our Company</a> | <a href="#">Our Partners</a> | <a href="#">Resources</a>       |                          |
| Artificial Intelligence       | Who We Are                  | Find a Partner               | Blog                            |                          |
| Products                      | Careers                     | OEM Solutions                | Dell Rewards                    |                          |
| Solutions                     | Dell Technologies Capital   | Partner Program              | Events                          |                          |
| Services                      | Investors                   |                              | Email Sign-Up                   |                          |
| Deals                         | Newsroom                    |                              | Privacy Centre                  |                          |
|                               | Recycling                   |                              | Security & Trust Centre         |                          |
|                               | Corporate Impact            |                              | Trial Software Downloads        |                          |

[Customer Stories](#)

[Dell Technologies](#)

[Dell Premier for Business](#)

[Copyright © 2026 Dell Inc.](#)

[Terms of Sale](#)

[Privacy Statement](#)

[Cookies, Ads & Emails](#)

[Legal & Regulatory](#)

[Accessibility](#)