



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

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

Support Home / Knowledge Base Article

Print Email Alert English

# DSA-2026-163: Security Update for Dell AppSync Vulnerabilities

Summary: Dell AppSync 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
- Acknowledgements
- Related Info

## Legal Disclaimer

## Affected Products

Provide Feedback



Please select a product to check article relevancy × [Identify Your Product](#) ▾



## Impact


High

## Details

Third-party Component	CVEs	More Information
KEYCLOAK	CVE-2022-4137	<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-2026-22767	Dell AppSync, version(s) 4.6.0, contain(s) an UNIX Symbolic Link (Symlink) Following vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information tampering.	7.3	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:H</a> 
CVE-2026-22768	Dell AppSync, version(s) 4.6.0, contain(s) an Incorrect Permission Assignment for Critical Resource vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	7.3	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H</a> 

Proprietary Code CVEs	Description	CVSS Base Score	CVSS Vector String
CVE-2026-22767	Dell AppSync, version(s) 4.6.0, contain(s) an UNIX Symbolic Link (Symlink) Following vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information tampering.	7.3	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:H</a> 
CVE-2026-22768	Dell AppSync, version(s) 4.6.0, contain(s) an Incorrect Permission Assignment for Critical Resource vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	7.3	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/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
Dell AppSync	Versions prior to 4.6.0.4	Version 4.6.1.0 or later	<a href="https://www.dell.com/support/home/product-support/product/appsync/drivers">https://www.dell.com/support/home/product-support/product/appsync/drivers</a>

Product	Affected Versions	Remediated Versions	Link
Dell AppSync	Versions prior to 4.6.0.4	Version 4.6.1.0 or later	<a href="https://www.dell.com/support/home/product-support/product/appsync/drivers">https://www.dell.com/support/home/product-support/product/appsync/drivers</a>

## Revision History

Revision	Date	Description
1.0	2026-04-01	Initial Release

## Acknowledgements

CVE-2026-22768: Dell would like to thank Marius Gabriel Mihai for reporting this issue.

CVE-2026-22767: Dell would like to thank falconCorrup for reporting this issue.

## Related Information

[Dell Security Advisories and Notices](#)

[Dell Vulnerability Response Policy](#)

[CVSS Scoring Guide](#)

## Legal Disclaimer

## Affected Products

AppSync, AppSync

### Article Properties

**Article Number:** 000446965

**Article Type:** Dell Security Advisory

**Last Modified:** 01 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](#)

[Profile Settings](#)

[Returns](#)

[X \(Twitter\)](#)

[My Products](#)

[LinkedIn](#)

[Make a Payment](#)

[Instagram](#)

[Dell Rewards Balance](#)

[YouTube](#)

**Our Offerings**

**Our Offerings**

**Our Company**

**Our Company**

**Our Partners**

**Our Partners**

**Resources**

**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](#)