



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-2026-091: Security Update for Dell Disk Library for mainframe Vulnerabilities

Summary: Dell Disk Library for mainframe 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
PowerEdge Platform BIOS	CVE-2025-24305, CVE-2025-21090, CVE-2025-20109, CVE-2024-36293, CVE-2024-28047, CVE-2025-20068, CVE-2025-20105, CVE-2025-20028, CVE-2025-20027, CVE-2025-20073, CVE-2024-21859, CVE-2024-31155, CVE-2024-38796, CVE-2024-45332, CVE-2025-20054, CVE-2024-39279, CVE-2024-31157, CVE-2025-20064	<a href="#">DSA-2025-297</a> , <a href="#">DSA-2025-156</a> , <a href="#">DSA-2025-041</a> , <a href="#">DSA-2025-297</a> , <a href="#">DSA-2025-042</a> , <a href="#">DSA-2025-038</a> , <a href="#">DSA-2025-156</a>
SUSE Linux Enterprise Server 15 SP4	CVE-2025-69420, CVE-2025-69421, CVE-2026-22795, CVE-2026-22796	<a href="https://suse.com">https://suse.com</a> 
Angular	CVE-2021-4231	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
Babel	CVE-2023-45133	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
Moment.js	CVE-2022-24785, CVE-2022-31129	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
ansi-html	CVE-2021-23424	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
jQuery	CVE-2020-11022, CVE-2020-11023	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
bn.js	CVE-2026-2739	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
body-parser	CVE-2024-45590	<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> 
browserify-sign	CVE-2023-46234	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
chart.js	CVE-2020-7746	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
cipher-base	CVE-2025-9287	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
cookie	CVE-2024-47764	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
cross-spawn	CVE-2024-21538	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
debug	CVE-2017-16137	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
decode-uri-component	CVE-2022-38900	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
Elliptic	CVE-2024-48949, CVE-2024-42461, CVE-2025-14505, CVE-2024-42460, CVE-2024-42459, CVE-2024-48948, CVE-2021-44906	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
flatted	CVE-2026-32141, CVE-2026-33228	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
follow-redirects	CVE-2024-28849, CVE-2023-26159	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 

Third-party Component	CVEs	More Information
form-data	CVE-2025-7783	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
http-cache-semantics	CVE-2022-25881	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
ip	CVE-2023-42282	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
js-yaml	CVE-2025-64718	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
JSON5	CVE-2022-46175	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
lodash	CVE-2025-13465	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
Minimist	CVE-2020-7598	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
node-tar	CVE-2024-28863	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
nth-check	CVE-2021-3803	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
on-headers	CVE-2025-7339	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
parse-uri	CVE-2024-36751	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
path-to-regexp	CVE-2024-45296, CVE-2024-52798	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
pbkdf2	CVE-2025-6547, CVE-2025-6545	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
postcss	CVE-2021-23382, CVE-2021-23368	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
rollup	CVE-2026-27606	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
send	CVE-2024-43799	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
sha.js	CVE-2025-9288	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
socket.io-parser	CVE-2026-33151, CVE-2023-32695, CVE-2022-2421, CVE-2020-36049	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
terser	CVE-2022-25858	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
tough-cookie	CVE-2023-26136	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
validator	CVE-2025-56200, CVE-2021-3765, CVE-2025-12758	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
webpack-subresource-integrity	CVE-2020-15262	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
ws	CVE-2024-37890	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 

Third-party Component	CVEs	More Information
xml2js	CVE-2023-0842	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
xmlhttprequest	CVE-2020-28502	<a href="https://nvd.nist.gov/vuln/search">https://nvd.nist.gov/vuln/search</a> 
xmlhttprequest-ssl	CVE-2021-31597	<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-2026-23773	Dell Disk Library for Mainframe, version(s) DLM 8700/2700 contain(s) a Server-Side Request Forgery (SSRF) vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Server-side request forgery.	4.3	<a href="#">CVSS:3.1/AV:N/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-2026-23773	Dell Disk Library for Mainframe, version(s) DLM 8700/2700 contain(s) a Server-Side Request Forgery (SSRF) vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Server-side request forgery.	4.3	<a href="#">CVSS:3.1/AV:N/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
Disk Library for mainframe DLM8700	Versions prior to 7.0.1.0	Version 7.0.1.0 or later	<a href="https://www.dell.com/support/product-details/product/disk-library-for-mainframe-dlm8700/drivers">https://www.dell.com/support/product-details/product/disk-library-for-mainframe-dlm8700/drivers</a>
Disk Library for mainframe DLM2700	Versions prior to 7.0.1.0	Version 7.0.1.0 or later	<a href="https://www.dell.com/support/product-details/product/disk-library-for-mainframe-dlm2700/drivers">https://www.dell.com/support/product-details/product/disk-library-for-mainframe-dlm2700/drivers</a>

Product	Affected Versions	Remediated Versions	Link
Disk Library for mainframe DLM8700	Versions prior to 7.0.1.0	Version 7.0.1.0 or later	<a href="https://www.dell.com/support/product-details/product/disk-library-for-mainframe-dlm8700/drivers">https://www.dell.com/support/product-details/product/disk-library-for-mainframe-dlm8700/drivers</a>

Product	Affected Versions	Remediated Versions	Link
Disk Library for mainframe DLm2700	Versions prior to 7.0.1.0	Version 7.0.1.0 or later	<a href="https://www.dell.com/support/product-details/product/disk-library-for-mainframe-dlm2700/drivers">https://www.dell.com/support/product-details/product/disk-library-for-mainframe-dlm2700/drivers</a>

## Revision History

Revision	Date	Description
1.0	2026-04-28	Initial Release
2.0	2026-04-28	Updated CVE description for CVE-2026-23773
3.0	2026-04-29	Added CVE-2024-39279, CVE-2024-31157, CVE-2025-20064 to the advisory

## 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

Disk Library, Disk Library for mainframe, Disk Library for mainframe DLm2700, Disk Library for mainframe DLm8700

### Article Properties

**Article Number:** 000458131

**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](#)

<a href="#">US/EN</a>	<b>Account</b>	<b>Support</b>	<b>Connect with Us</b>	<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>		
<b>Our Offerings</b>	<b>Our Company</b>	<b>Our Partners</b>	<b>Resources</b>	
<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>	
<b>Dell Technologies</b>	<b>Dell Premier for Business</b>	<b>Dell Financial Services</b>		
<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>	