



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	DSA-2025-297 , DSA-2025-156 , DSA-2025-041 , DSA-2025-297 , DSA-2025-042 , DSA-2025-038 , DSA-2025-156
SUSE Linux Enterprise Server 15 SP4	CVE-2025-69420, CVE-2025-69421, CVE-2026-22795, CVE-2026-22796	https://suse.com 
Angular	CVE-2021-4231	https://nvd.nist.gov/vuln/search 
Babel	CVE-2023-45133	https://nvd.nist.gov/vuln/search 
Moment.js	CVE-2022-24785, CVE-2022-31129	https://nvd.nist.gov/vuln/search 
ansi-html	CVE-2021-23424	https://nvd.nist.gov/vuln/search 
jQuery	CVE-2020-11022, CVE-2020-11023	https://nvd.nist.gov/vuln/search 
bn.js	CVE-2026-2739	https://nvd.nist.gov/vuln/search 
body-parser	CVE-2024-45590	https://nvd.nist.gov/vuln/search 
brace-expansion	CVE-2025-5889	https://nvd.nist.gov/vuln/search 
browserify-sign	CVE-2023-46234	https://nvd.nist.gov/vuln/search 
chart.js	CVE-2020-7746	https://nvd.nist.gov/vuln/search 
cipher-base	CVE-2025-9287	https://nvd.nist.gov/vuln/search 
cookie	CVE-2024-47764	https://nvd.nist.gov/vuln/search 
cross-spawn	CVE-2024-21538	https://nvd.nist.gov/vuln/search 
debug	CVE-2017-16137	https://nvd.nist.gov/vuln/search 
decode-uri-component	CVE-2022-38900	https://nvd.nist.gov/vuln/search 
Elliptic	CVE-2024-48949, CVE-2024-42461, CVE-2025-14505, CVE-2024-42460, CVE-2024-42459, CVE-2024-48948, CVE-2021-44906	https://nvd.nist.gov/vuln/search 
flatted	CVE-2026-32141, CVE-2026-33228	https://nvd.nist.gov/vuln/search 
follow-redirects	CVE-2024-28849, CVE-2023-26159	https://nvd.nist.gov/vuln/search 
form-data	CVE-2025-7783	https://nvd.nist.gov/vuln/search 

Third-party Component	CVEs	More Information
http-cache-semantics	CVE-2022-25881	https://nvd.nist.gov/vuln/search 
ip	CVE-2023-42282	https://nvd.nist.gov/vuln/search 
js-yaml	CVE-2025-64718	https://nvd.nist.gov/vuln/search 
JSON5	CVE-2022-46175	https://nvd.nist.gov/vuln/search 
lodash	CVE-2025-13465	https://nvd.nist.gov/vuln/search 
Minimist	CVE-2020-7598	https://nvd.nist.gov/vuln/search 
node-tar	CVE-2024-28863	https://nvd.nist.gov/vuln/search 
nth-check	CVE-2021-3803	https://nvd.nist.gov/vuln/search 
on-headers	CVE-2025-7339	https://nvd.nist.gov/vuln/search 
parse-uri	CVE-2024-36751	https://nvd.nist.gov/vuln/search 
path-to-regexp	CVE-2024-45296, CVE-2024-52798	https://nvd.nist.gov/vuln/search 
pbkdf2	CVE-2025-6547, CVE-2025-6545	https://nvd.nist.gov/vuln/search 
postcss	CVE-2021-23382, CVE-2021-23368	https://nvd.nist.gov/vuln/search 
rollup	CVE-2026-27606	https://nvd.nist.gov/vuln/search 
send	CVE-2024-43799	https://nvd.nist.gov/vuln/search 
sha.js	CVE-2025-9288	https://nvd.nist.gov/vuln/search 
socket.io-parser	CVE-2026-33151, CVE-2023-32695, CVE-2022-2421, CVE-2020-36049	https://nvd.nist.gov/vuln/search 
terser	CVE-2022-25858	https://nvd.nist.gov/vuln/search 
tough-cookie	CVE-2023-26136	https://nvd.nist.gov/vuln/search 
validator	CVE-2025-56200, CVE-2021-3765, CVE-2025-12758	https://nvd.nist.gov/vuln/search 
webpack-subresource-integrity	CVE-2020-15262	https://nvd.nist.gov/vuln/search 
ws	CVE-2024-37890	https://nvd.nist.gov/vuln/search 
xml2js	CVE-2023-0842	https://nvd.nist.gov/vuln/search 

Third-party Component	CVEs	More Information
xmlhttprequest	CVE-2020-28502	https://nvd.nist.gov/vuln/search 
xmlhttprequest-ssl	CVE-2021-31597	https://nvd.nist.gov/vuln/search 

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	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N 

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	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N 

 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	https://www.dell.com/support/product-details/product/disk-library-for-mainframe-dlm8700/drivers
Disk Library for mainframe DLM2700	Versions prior to 7.0.1.0	Version 7.0.1.0 or later	https://www.dell.com/support/product-details/product/disk-library-for-mainframe-dlm2700/drivers

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	https://www.dell.com/support/product-details/product/disk-library-for-mainframe-dlm8700/drivers
Disk Library for mainframe DLM2700	Versions prior to 7.0.1.0	Version 7.0.1.0 or later	https://www.dell.com/support/product-details/product/disk-library-for-mainframe-dlm2700/drivers

Revision History

Revision	Date	Description
1.0	2026-04-28	Initial Release
2.0	2026-04-28	Updated CVE description for CVE-2026-23773

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: 28 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 field for additional information

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

Submit Feedback

US/EN	Account	Support	Connect with Us	Site Map
Site Map	My Account	Support Home	Community	US/EN
Order Status		Contact Technical Support	Contact Us	
Profile Settings		Returns	X (Twitter)	
My Products			LinkedIn	
Make a Payment			Instagram	
Dell Rewards Balance			YouTube	
Our Offerings	Our Company	Our Partners	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	