



Search Dell or identify your p

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
- Dell Financial Services
- Partner Program Sign In

US/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-2026-058: Security Update for Dell Storage Manager - Replay Manager for Microsoft Servers Vulnerabilities

Summary: Dell Storage Manager - Replay Manager for Microsoft Servers remediation is available for a vulnerability 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

Proprietary Code CVEs	Description	CVSS Base Score	CVSS Vector String
CVE-2026-23772	Dell Storage Manager - Replay Manager for Microsoft Servers, version(s) 8.0, contain(s) an Improper Privilege Management 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:N/S:U/C:L/I:H/A:H</a> ✉

Proprietary Code CVEs	Description	CVSS Base Score	CVSS Vector String
CVE-2026-23772	Dell Storage Manager - Replay Manager for Microsoft Servers, version(s) 8.0, contain(s) an Improper Privilege Management 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:N/S:U/C:L/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 Storage Manager - Replay Manager for Microsoft Servers	Versions prior to 8.0.3	Version 8.0.3 or later	<a href="https://www.dell.com/support/product-details/product/dell-storage-manager/overview">https://www.dell.com/support/product-details/product/dell-storage-manager/overview</a>

Product	Affected Versions	Remediated Versions	Link
Dell Storage Manager - Replay Manager for Microsoft Servers	Versions prior to 8.0.3	Version 8.0.3 or later	<a href="https://www.dell.com/support/product-details/product/dell-storage-manager/overview">https://www.dell.com/support/product-details/product/dell-storage-manager/overview</a>

## Revision History

Revision	Date	Description
1.0	2026-04-15	Initial Release

## Acknowledgements

CVE-2026-23772: 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

Storage System Management, Dell Storage Manager

### Article Properties

**Article Number:** 000453020

**Article Type:** Dell Security Advisory

**Last Modified:** 15 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> Account	<b>Support</b> Support	<b>Connect with Us</b> Connect with Us	Site Map
<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="#">X (Twitter)</a>	
<a href="#">Profile Settings</a>	<a href="#">Returns</a>	<a href="#">LinkedIn</a>	<a href="#">Instagram</a>	
<a href="#">My Products</a>		<a href="#">YouTube</a>		
<a href="#">Make a Payment</a>				
<a href="#">Dell Rewards Balance</a>				
<b>Our Offerings</b> Our Offerings	<b>Our Company</b> Our Company	<b>Our Partners</b> Our Partners	<b>Resources</b> Resources	
<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>	