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.

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

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

⚠ 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	https://www.dell.com/support/product-details/product/dell-storage-manager/overview

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	https://www.dell.com/support/product-details/product/dell-storage-manager/overview

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

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 use[illegible] the affected product(s). Dell Technologies assesses the risk based on an average of risks across a diverse set of installed systems and ma[illegible] represent the actual risk to your local installation and individual environment. It is recommended that all users determine the applicability o[illegible] information to their individual environments and take appropriate actions. The information set forth herein is provided "as is" without warra[illegible] any kind. Dell Technologies expressly disclaims all warranties, either express or implied, including the warranties of merchantability, fitness 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

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

Provide Feedback

Accurate

☆ ☆ ☆ ☆ ☆

Useful

☆ ☆ ☆ ☆ ☆

Easy to Understand

☆ ☆ ☆ ☆ ☆

Was this article helpful?

◯ Yes ◯ No

Additional Information (optional) 0/3000 characters

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

Submit Feedback

Contact Support