



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

Support Home / Knowledge Base Article

Print Email Alert English

DSA-2026-131: Security Update for Dell/Alienware Purchased Apps for an Improper Link Resolution Before File Access Vulnerability.

Summary: Dell/Alienware Purchased Apps remediation is available for an Improper Link Resolution Before File Access vulnerability that could be exploited by malicious users to compromise the ... [View More](#)

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

Medium

Details

Proprietary Code CVEs	Description	CVSS Base Score	CVSS Vector String
CVE-2026-27105	Dell/Alienware Purchased Apps, versions prior to 1.1.31.0, contain an Improper Link Resolution Before File Access ('Link Following') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Arbitrary File Write	6.3	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H ✉

Proprietary Code CVEs	Description	CVSS Base Score	CVSS Vector String
CVE-2026-27105	Dell/Alienware Purchased Apps, versions prior to 1.1.31.0, contain an Improper Link Resolution Before File Access ('Link Following') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Arbitrary File Write	6.3	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/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	Software/Firmware	Affected Versions	Remediated Versions	Release Date (MM/DD/YYYY)	Link
Dell/Alienware Purchased Apps	Software	Versions prior to 1.1.31.0	Version 1.1.31.0 or later	04/20/2026	Dell/Alienware Purchased Apps Driver Details

Product	Software/Firmware	Affected Versions	Remediated Versions	Release Date (MM/DD/YYYY)	Link
Dell/Alienware Purchased Apps	Software	Versions prior to 1.1.31.0	Version 1.1.31.0 or later	04/20/2026	Dell/Alienware Purchased Apps Driver Details

Revision History

Revision	Date	Description
1.0	2026-04-28	Initial Release
2.0	2026-04-28	Added Revision History Table and Acknowledgement

Acknowledgements

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 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

Alienware Purchased Apps, Dell Purchased Apps

Article Properties

Article Number: 000438321

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](#)

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](#)

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