



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

Home / Support Home / Knowledge Base Article

Print Email Alert English

DSA-2026-143: Security update for Dell ObjectScale prior to 4.1.0.3 and 4.2.0.0 Insertion of Sensitive Information into Log File Vulnerability

Summary: Dell ObjectScale versions prior to 4.1.0.3 and version 4.2.0.0 remediation is available for Insertion of Sensitive Information into Log File vulnerability that could be exploited by ... [View More](#)

Detailed Article ^

- Impact
- Details
- Affected Products & Remediation
- Workarounds & Mitigations
- Revision History
- 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-2026-28261	Dell Elastic Cloud Storage, version 3.8.1.7 and prior, and Dell ObjectScale, versions prior to 4.1.0.3 and version 4.2.0.0, contains an Insertion of Sensitive Information into Log File vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to secret exposure. The attacker may be able to use the exposed secret to access the vulnerable system with privileges of the compromised account.	7.8	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H ☑

Proprietary Code CVEs	Description	CVSS Base Score	CVSS Vector String
CVE-2026-28261	Dell Elastic Cloud Storage, version 3.8.1.7 and prior, and Dell ObjectScale, versions prior to 4.1.0.3 and version 4.2.0.0, contains an Insertion of Sensitive Information into Log File vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to secret exposure. The attacker may be able to use the exposed secret to access the vulnerable system with privileges of the compromised account.	7.8	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/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
Elastic Cloud Storage	Versions prior to 3.8.1.7	Version 4.2.0.1 or later	Open a Service Request for an Operating Environment Upgrade and Quote DSA-2026-143
ObjectScale	Versions prior to 4.1.0.3	Version 4.1.0.3	Open a Service Request for an Operating Environment Upgrade and Quote DSA-2026-143
ObjectScale	Version 4.2.0.0	Version 4.2.0.1 or later	Open a Service Request for an Operating Environment Upgrade and Quote DSA-2026-143

Product	Affected Versions	Remediated Versions	Link
Elastic Cloud Storage	Versions prior to 3.8.1.7	Version 4.2.0.1 or later	Open a Service Request for an Operating Environment Upgrade and Quote DSA-2026-143
ObjectScale	Versions prior to 4.1.0.3	Version 4.1.0.3	Open a Service Request for an Operating Environment Upgrade and Quote DSA-2026-143

ObjectScale	Version 4.2.0.0	Version 4.2.0.1 or later	Open a Service Request for an Operating Environment Upgrade and Quote DSA-2026-143
-------------	-----------------	--------------------------	----------------------------------------------------------------------------------------------------

Note:

1. Customers on any supported affected versions/releases listed in the 'Affected Products and Remediation' section may also upgrade directly to the 4.2.0.1 release or later.
2. Dell recommends all customers have their ObjectScale systems upgraded at the earliest opportunity by opening an "Operating Environment Upgrade" Service Request.
3. Please visit the [Security Update Release Schedule for Supported Versions of ObjectScale \(formerly ECS\)](#) for more information.

Workarounds & Mitigations

None

Revision History

Revision	Date	Description
1.0	2026-04-06	Initial Release

Related Information[Dell Security Advisories and Notices](#)[Dell Vulnerability Response Policy](#)[CVSS Scoring Guide](#)**Legal Disclaimer****Affected Products**

ECS, ObjectScale, ECS Appliance, ECS Appliance Hardware Series, ECS Appliance Software with Encryption, ECS Appliance Software without Encryption, ObjectScale Software without Encryption, ObjectScale Appliance Series, ObjectScale Software Series

Article Properties**Article Number:** 000449325**Article Type:** Dell Security Advisory**Last Modified:** 06 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](#)

US/EN	Account	Support	Connect with Us	Site Map
Site Map	Account	Support Home	Connect with Us	US/EN
Order Status	Contact Technical Support	Community	Contact Us	
Profile Settings	Returns	X (Twitter)	LinkedIn	
My Products		Instagram	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