

Multiple Maximum and Critical Severity Flaws in Dell Container Storage Modules (CVE-2026-63688 & CVE-2026-63692)

Oct 05, 2026

☐ WHITE

[View Alert](#)

Dell has [released](#) patches for several significant vulnerabilities affecting its **Container Storage Modules (CSM)** Authorization security module, which connects enterprise storage arrays to Kubernetes environments.

Dell urges administrators to update their container storage modules to version 1.18.0 or later at the earliest opportunity and patch affected systems promptly. Organizations should also practice least-privilege account management, enforce patch management, and implement standard security measures such as exploit protection and vulnerability scanning.

Health-ISAC provides this information to increase situational awareness and encourage organizations to assess their risk exposure to the vulnerabilities.

Additional Info

Analysis:

On October 01, 2026, Dell [issued](#) patches for multiple security vulnerabilities in its **Container Storage Modules (CSM)** Authorization security module, which connects Dell enterprise storage arrays to Kubernetes environments. The [primary security issues](#), tracked as **CVE-2026-63688** and

CVE-2026-63692, stem from the absence of authentication mechanisms for critical core functions. Unauthenticated remote actors can exploit these gaps to bypass authorization controls, retrieve backend administrator credentials, and acquire administrative access across registered storage infrastructure and tenant services. Dell advises administrators to update affected components to version **1.18.0** or **later**.

Below is the list of vulnerabilities patched by Dell:

- **CVE-2026-63688** (CVSS: 10.0) - Missing authentication in the csm-authorization-storage gRPC server allows unauthenticated remote attackers to gain full administrative control over storage backend credentials.
- **CVE-2026-63692** (CVSS: 10.0) - Missing authentication in the authorization proxy and tenant service allows unauthenticated network attackers to bypass controls and elevate privileges to administrative levels.
- **CVE-2026-67269** (CVSS: 9.9) - Improper privilege management in the ContainerStorageModule Custom Resource reconciler allows low-privileged remote attackers to gain root-level access on cluster nodes.
- **CVE-2026-54472** (CVSS: 9.8) - Use of hard-coded credentials in the CSM Authorization module allows remote unauthenticated attackers to forge administrative tokens and bypass proxy controls.
- **CVE-2026-61421** (CVSS: 9.8) - Use of a hard-coded cryptographic key in the archived karavi-authorization component's JWT authentication allows attackers using the documented default secret to forge admin tokens.
- **CVE-2026-67273** (CVSS: 9.6) - Improper neutralization of template engine elements allows low-privileged remote attackers to escalate privileges and gain cluster-wide access to Kubernetes Secrets.
- **CVE-2026-67270** (CVSS: 8.2) - Improper certificate validation in the proxy-server component allows unauthenticated adjacent network attackers to expose storage administrator credentials.
- **CVE-2026-76105** (CVSS: 7.7) - Use of insufficiently random values allows unauthenticated local attackers to cause information tampering.
- **CVE-2026-61411** (CVSS: 7.7) - Sensitive information insertion into log files allows low-privileged remote attackers to cause information disclosure.

- **CVE-2026-70411** (CVSS: 7.1) - Missing authentication in the csm-authorization-tenant gRPC service allows unauthenticated adjacent network attackers to create unauthorized tenant entities and inject roles.
- **CVE-2026-63689** (CVSS: 6.5) - Sensitive information insertion into log files leads to potential information disclosure for low-privileged remote attackers.
- **CVE-2026-63691** (CVSS: 6.1) - Missing authorization in the PowerMax csireverseproxy allows unauthenticated adjacent network attackers unauthorized access.
- **CVE-2026-63690** (CVSS: 5.4) - Missing authentication for critical functions across multiple PowerFlex, PowerMax, and PowerStore CSI drivers allows unauthenticated adjacent network attackers to disclose information.

Health sector organizations increasingly rely on containerized platforms and Kubernetes to manage critical patient data repositories, electronic health record (EHR) systems, and imaging databases. Vulnerabilities in underlying storage management components create risks to operational continuity and data security. Unauthorized access to storage controllers could enable bad actors to tamper with sensitive clinical records, disrupt real-time healthcare application services, or access confidential patient databases. Securing enterprise storage systems that support healthcare infrastructure is vital to maintaining system availability, ensuring patient safety, and upholding regulatory compliance requirements across medical facilities and cloud environments.

Because sophisticated actor groups frequently target storage management layers to compromise operational networks, prompt patch management is essential for defending core enterprise data assets. Delayed remediation expands the exposure window for critical hospital infrastructure, potentially leading to unauthorized system access or broad service disruptions. Establishing robust access controls, promptly applying software security updates, and auditing Kubernetes configurations help protect a health sector organization's storage platforms from exploitation. Maintaining rigorous isolation controls between storage proxies and general network zones provides an additional defense tier against potential unauthorized access.

Recommendations and Mitigations:

Health-ISAC recommends organizations review and assess their risk exposure to these vulnerabilities and implement the following:

- [Upgrade](#) all Dell Container Storage Modules to version 1.18.0 or higher.
- Audit Kubernetes access controls and rotate backend storage administrator credentials.
- Enforce strict network segmentation to isolate CSM Authorization proxies from public internet exposure.
- Restrict access to administrative endpoints using zero-trust network policies and multi-factor authentication.
- Monitor storage logs continuously for anomalous access requests or unauthorized credential usage.
- **Review the Health Industry Cybersecurity Practices (HICP): [Managing Threats and Protecting Patients](#)** Resources.

<hr size=1 width="100%" align=center>

Alert Id	d19b6669
Category	Vulnerability Bulletins
References	dell bleepingcomputer hhs
Tags	CVE-2026-67273, CVE-2026-61421, CVE-2026-54472, CVE-2026-67269, CVE-2026-63692, CVE-2026-63688, Dell Container Storage Modules, Dell

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Please provide your feedback



Download the App

Available on iOS, Android and Web



For more updates and alerts, visit: <https://health-isac.cyware.com/webapp/>

Health-ISAC is an invite only platform. Please DO NOT forward this email to anyone. If you are not supposed to receive this email, please report to toc@h-isac.org

--

You received this message because you are subscribed to the Google Groups "TLP Green - Health-ISAC Partners" group.

To unsubscribe from this group and stop receiving emails from it, send an email to health-isac-partners+unsubscribe@h-isac.org.

To view this discussion visit <https://groups.google.com/a/h-isac.org/d/msgid/health-isac-partners/010001a10a1f32f4-cf7c985d-f700-4d28-9a45-e5b9d6f37136-000000%40email.amazonses.com>.