# NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-54489

## Summary

CVE-2026-54489 is a newly disclosed Critical vulnerability. It is not yet on CISA's actively-exploited list; treat it as proactive patching before it is weaponised. Dell Virtual Storage Integrator for VMware vSphere Client, versions prior to 10.11.1.0, contain(s) a Sensitive Information Disclosure vulnerability. An unauthenticated remote attacker could potentially exploit this vulnerability, leading to information disclosure and session hijacking. This vulnerability is considered critical as it allows an unauthenticated attacker to obtain active session credentials and fully impersonate authenticated users, including administrators. Dell recommends customers to upgrade at the earliest opportunity.

## What we know

- **CVE:** CVE-2026-54489
- **Status:** Newly disclosed, not yet known-exploited (not on CISA KEV)
- **Severity:** CVSS 9.1 Critical, Network-exploitable, no privileges required, no user interaction (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N)
- **Exploitation likelihood (EPSS):** 0%

## Recommended action

Patch as a fix becomes available, prioritised by the exposure and EPSS above. Until then, restrict network access to the affected service now (segment it, put it behind a VPN, or take it offline) until you can patch. This does not yet trigger CRA 24-hour reporting, which requires active exploitation, but patching ahead of exploitation is the whole point.

---

*Sources: NIST NVD. Public data; an advisory of a newly disclosed vulnerability, not an incident report. Verify applicability to your estate before acting.*