EXPLOITED VULNERABILITY ADVISORY: CVE-2026-59310

Summary

CVE-2026-59310 in Broadcom VMware vCenter is being actively exploited in the wild. VMware vCenter contains a directory traversal vulnerability in the Syslog server. A malicious actor with network access to vCenter may exploit this issue to execute arbitrary code. CISA requires federal remediation by 2026-08-21; under the CRA, exploitation of an affected product must be reported within 24 hours.

What we know

- **CVE:** CVE-2026-59310
- **Affected:** Broadcom VMware vCenter
- **Exploitation:** Actively exploited, added to CISA KEV on 2026-08-18
- **Severity:** CVSS 9.8 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:H)
- **Exploitation likelihood (EPSS):** 1%
- **Weakness:** CWE-22

Recommended action

Patch CVE-2026-59310 by 2026-08-21. If you cannot patch immediately, restrict network access to the affected service now (segment it, put it behind a VPN, or take it offline) until you can patch. If you ship an affected product, be ready to file the CRA 24-hour report the moment you find it exploited.

Sources: CISA Known Exploited Vulnerabilities, NIST NVD. Public data; an advisory of active exploitation, not an incident report. Verify applicability to your estate before acting.