

EXPLOITED VULNERABILITY ADVISORY: CVE-2026-65400

Summary

CVE-2026-65400 in Apple macOS is being actively exploited in the wild. An authentication issue was addressed with improved state management. This issue is fixed in macOS Sequoia 15.7.9, macOS Sonoma 14.8.9, macOS Tahoe 26.6.1. An attacker on the network may be able to authenticate to Screen Sharing without valid credentials. 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-2026-65400
- **Affected:** Apple macOS
- **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):** 0%
- **Weakness:** CWE-287

Recommended action

Patch CVE-2026-65400 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.