EXPLOITED VULNERABILITY ADVISORY: CVE-2026-68820

Summary

CVE-2026-68820 in Microsoft Windows Ancillary Function Driver for WinSock is being actively exploited in the wild. Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally. CISA requires federal remediation by 2026-08-25; under the CRA, exploitation of an affected product must be reported within 24 hours.

What we know

- **CVE:** CVE-2026-68820
- **Affected:** Microsoft Windows Ancillary Function Driver for WinSock
- **Exploitation:** Actively exploited, added to CISA KEV on 2026-08-11
- **Severity:** CVSS 7.0 High, Local-exploitable, no user interaction (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)
- **Weakness:** CWE-416

Recommended action

Patch CVE-2026-68820 by 2026-08-25. If you cannot patch immediately, apply available vendor mitigations and monitor for exploitation until patched. 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.