

CVE-2026-68820

Microsoft Windows Ancillary Function Driver for WinSock Use-After-Free Vulnerability

CISA KEV since Aug 11, 2026

Actively exploited

Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 7.0 High · NVD	EPSS 0.003 25.1st percentile · FIRST	CISA DEADLINE Aug 25, 2026 CISA federal deadline · Overdue by 58 days
---	---------------------------------------	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☒ KEV recency	Added to CISA KEV within the last 90 days
☒ EPSS	0.003 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.0	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines.

Basis: CISA KEV required action

Affected and fixed versions · 5 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
windows 10 1607	< 10.0.14393.9418	10.0.14393.9418	NVD
windows 10 1809	< 10.0.17763.9115	10.0.17763.9115	NVD
windows 10 21h2	< 10.0.19044.7663	10.0.19044.7663	NVD
windows 10 22h2	< 10.0.19045.7663	10.0.19045.7663	NVD
windows 11 23h2	< 10.0.22631.7517	10.0.22631.7517	NVD
windows 11 24h2	< 10.0.26100.9106	10.0.26100.9106	NVD
windows 11 25h2	< 10.0.26200.9106	no fixed version listed	NVD
windows 11 26h1	< 10.0.28000.2704	no fixed version listed	NVD



Sources

Vendor guidance	github.com/advisories/GHSA-c433-3382-mw5v	Additional guidance	msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68820
portal.msrc.microsoft.com	portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2026-68820	BOD 26-04	cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk
Forensics Triage Requirements	cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk	NVD	nvd.nist.gov/vuln/detail/CVE-2026-68820
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-56468
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-68820		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.