

CVE-2026-85880

Microsoft Windows Heap-Based Buffer Overflow Vulnerability

CISA KEV since Sep 8, 2026

Actively exploited

Heap-based buffer overflow in Windows ALPC allows an authorized attacker to elevate privileges locally.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.036 89.5th percentile · FIRST	CISA DEADLINE Sep 22, 2026 CISA federal deadline · Overdue by 31 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	0.036 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.8	☐ 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

PACKAGE	AFFECTED	FIXED IN	SOURCE
windows 10 1607	< 10.0.14393.9512	10.0.14393.9512	NVD
windows 10 1809	< 10.0.17763.9245	10.0.17763.9245	NVD
windows 10 21h2	< 10.0.19044.7725	10.0.19044.7725	NVD
windows 10 22h2	< 10.0.19045.7725	10.0.19045.7725	NVD
windows server 2012	r2	no fixed version listed	NVD
windows server 2016	< 10.0.14393.9512	10.0.14393.9512	NVD
windows server 2019	< 10.0.17763.9245	10.0.17763.9245	NVD
windows server 2022	< 10.0.20348.5622	no fixed version listed	NVD



Sources

Vendor guidance	github.com/advisories/GHSA-96fm-jjf3-wv64	Additional guidance	msrc.microsoft.com/update-guide/vulnerability/CVE-2026-85880
msrc.microsoft.com	msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-85880	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-2026-85880
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-73365
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-85880		

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