



TLP: CLEAR

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



CYBER ADVISORY

Thursday September 10, 2026

CAL-CSIC-202609-A-004

Multiple Vulnerabilities Addressed in Latest Microsoft Security Update

Privilege Escalation

Under Active Exploitation

Patch Available

The California Cybersecurity Integration Center (Cal-CSIC) has identified multiple vulnerabilities affecting Microsoft in its latest [September 2026 Security Update](#), two of which are under active exploitation.¹

1. CVE-2026-85880, a Heap-based buffer overflow in Windows ALPC which potentially allows an authorized attacker to elevate privileges locally. It carries a CVSS v3.1 base score of 7.8 (High).²
2. CVE-2026-81963, an Improper link resolution before file access ('link following') in Windows Update Stack which potentially allows an authorized attacker to elevate privileges locally. It carries a CVSS v3.1 base score of 7.8 (High).³

Both vulnerabilities have been added to the CISA Known Exploited Vulnerabilities (KEV)^{4, 5} catalog due to active exploitation in the wild. Both vulnerabilities have been added to the CISA Known Exploited Vulnerabilities (KEV)^{6, 7} catalog due to the active exploitation in the wild. No public Proof-of-Concept (PoC) exploit code has been identified at this time.

The Cal-CSIC recommends applying the latest Microsoft September 2026 Security Patch immediately.

Vendor Advisory:

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-85880>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81963>

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR

Affected Product, Components/Software and Versions

Affected Software	Release / Edition	Affected Build Numbers
Windows 11	Version 26H1	Prior to 10.0.28000.2954
	Version 25H2	Prior to 10.0.26200.9445
	Version 24H2	Prior to 10.0.26100.9445
	Version 23H2	Prior to 10.0.22631.7582
	Version 22H2	Prior to 10.0.22621.7582
Windows 10	Version 22H2	Prior to 10.0.19045.7725
Windows 10 Enterprise LTSC	Version 21H2	Prior to 10.0.19044.7725
	Version 1809	Prior to 10.0.17763.9245
	Version 1607 (LTSC)	Prior to 10.0.14393.9512
Windows Server 2025	Version 24H2	Prior to 10.0.26100.33438
Windows Server 2022	Version 21H2	Prior to 10.0.20348.5622
Windows Server 2019	Version 1809	Prior to 10.0.17763.9245
Windows Server 2016	Version 1607	Prior to 10.0.14393.9512
Windows Server 2012 / 2012 R2	6.2 / 6.3 (ESU)	Prior to Sept 2026 Rollup

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: California Cybersecurity Integration Center | California Governor's Office of Emergency Services

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR

References:

¹ Microsoft; "September 2026 Security Updates"; <https://msrc.microsoft.com/update-guide/releaseNote/2026-Sep>; accessed 10 September 2026

² CVE.org; "CVE-2026-85880"; <https://www.cve.org/CVERecord?id=CVE-2026-85880>; accessed 10 September 2026

³ CVE.org; "CVE-2026-81963"; <https://www.cve.org/CVERecord?id=CVE-2026-81963>; accessed 10 September 2026

⁴ CISA; "Known Exploited Vulnerabilities Catalog"; https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-85880; accessed 10 September 2026

⁵ CISA; "Known Exploited Vulnerabilities Catalog"; https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-81963; accessed 10 September 2026

⁶ CISA; "Known Exploited Vulnerabilities Catalog"; https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-85880; accessed 10 September 2026

⁷ CISA; "Known Exploited Vulnerabilities Catalog"; https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-81963; accessed 10 September 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR