CYBER ADVISORY

Thursday, April 30, 2026 **CAL-CSIC-202604-A-008**

Critical Vulnerability on Windows Shell Spoofing

Spoofing Vulnerability | Credential Harvesting | Exploited in the Wild | Patch Available

Executive Summary:

The California Cybersecurity Integration Center (Cal-CSIC) has identified CVE-2026-32202, as a spoofing vulnerability affecting Windows Shell components, stemming from a residual flaw in the previous mitigation for CVE-2026-21510.[1] CVE-2026-32202 carries a Common Vulnerability Scoring System (CVSS) v3.1 base score of 4.3.[2] Its operational risk is *significant*, and is currently being exploited in the wild based on CISA Known Exploited Vulnerabilities (KEV) catalog.[3] Successful exploitation allows an unauthenticated attacker to force a Windows system into leaking sensitive authentication material (Net-NTLMv2 hashes), enabling unauthorized credential harvesting and facilitates lateral movement within the environment without requiring direct user execution of a malicious file.

The Cal-CSIC recommends following the vendor's patching guidance and referring to the Microsoft April 2026 Security Update as soon as possible.

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32202

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2026-21510

Affected Components and Versions:

Component Affected	Versions Impacted
Windows 10/11	Versions 23H2, 22H2, and 21H2 (All Editions)
Windows Server	Windows Server 2022, 2019, and 2016 (Including Core/Desktop Experience)
Azure Stack	Azure Stack HCI and related cloud-based Windows endpoints

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

References:

[1] NIST; CVE-2026-32202 Detail; https://nvd.nist.gov/vuln/detail/CVE-2026-32202; accessed 29 April 2026
[2] Microsoft; CVE-2026-32202; https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32202; accessed 29 April 2026
[3] CISA; Known Exploited Vulnerabilities Catalog; https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-32202; accessed 29 April 2026