CYBER ADVISORY

Wednesday, February 11, 2026 **CAL-CSIC-202602-A-007**

Active Exploitation of Multiple Microsoft Products

Unauthorized Access	Authentication Bypass	Privilege Escalation	Patch Available

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of multiple Microsoft vulnerabilities added to CISA's Known Exploited Vulnerabilities (KEV) catalog.[1] These six vulnerabilities range from a CVSS v3.1 Base Score rating of 8.8 to 6.2. These include CVE-2026-21510, CVE-2026-21513, CVE-2026-21514, CVE-2026-21519, CVE-2026-21533. CISA notes that vulnerabilities of this nature are commonly leveraged by malicious cyber actors and present substantial risk to the federal enterprise. Although no verified public proof of concept links is available currently, Microsoft has confirmed active exploitation in the wild.

Analyst Comment: *Organizations need to prioritize applying available patches or implementing the appropriate mitigations as soon as possible regardless of the level of known exploitation and CVSS severity level.*

The Cal-CSIC recommends organizations immediately update their Windows 11 devices. If a device is still on Windows 10, then update to Windows 10 KB5075912 extended security update. For further information on Microsoft's February 2026 Patch details, please refer to this link.

https://msrc.microsoft.com/update-guide/releaseNote/2026-feb

Microsoft CVEs

CVE-ID	Severity	Description
CVE-2026-21510	8.8 High	Windows Shell manages core user interface components including File Explorer and the execution of shortcut files. This vulnerability allows a crafted file or link to bypass built in security warnings such as SmartScreen protections.
CVE-2026-21513	8.8 High	MSHTML is the legacy Microsoft browser rendering engine used by Internet Explorer mode and embedded web content in Windows applications. The vulnerability permits bypass of security enforcement when rendering specially crafted HTML content.
CVE-2026-21514	7.8 High	Microsoft Word is a document processing application within Microsoft Office and Microsoft 365 used for creating and editing text documents. This vulnerability allows bypass of Object Linking and Embedding protections when opening crafted documents.
CVE-2026-21519	7.8 High	Desktop Window Manager handles graphical composition and rendering of the Windows interface. The flaw allows a locally authenticated attacker to escalate privileges to SYSTEM. Improper handling of objects within the window management process permits privilege boundary crossing. Exploitation requires prior access to the target system.
CVE-2026-21533	7.8 High	Remote Desktop Services enables remote graphical access to Windows systems for administration and user sessions. This vulnerability permits a local authenticated user to gain SYSTEM level privileges. Improper privilege management within service components enables escalation after login. The attacker must already possess valid credentials.
CVE-2026-21525	6.2 Medium	Remote Access Connection Manager manages dial up and VPN connections within Windows. The vulnerability allows a local attacker to trigger a service crash through improper memory handling. Exploitation results in denial of service rather than code execution. The attacker must possess local access.

References

[1] CISA "CISA Adds Six Known Exploited Vulnerabilities to Catalog" https://www.cisa.gov/news-events/alerts/2026/02/10/cisa-adds-six-known-exploited-vulnerabilities-catalog; accessed 11 February 2026