CYBER ADVISORY

Friday, November 21, 2025 **CAL-CSIC-ADVISORY-202511-A-008**

Microsoft Windows Kernel Elevation of Privilege Vulnerability

Zero-Day	Active Exploitation	Remote Code Execution	Proof-of-Concept

The California Cybersecurity Integration Center (Cal-CSIC) has identified a set of high-impact Windows vulnerabilities. CVE-2025-60724, with a CVSS v3.1 score of 9.8[1], allows an unauthenticated remote attacker to gain initial access and execute code. This initial access can be followed by an Escalation of Privilege (EoP) exploitation, including the Windows Kernel zero-day, CVE-2025-62215 with a CVSS v3.1 score of 7.0[2]. This vulnerability is actively exploited in the wild[3] and, with a public proof-of-concept available[4], may be used to escalate low-level user privileges up to SYSTEM access, achieving full administrative control over a compromised device.

This combination along with other multiple CVEs listed below could potentially be used to gain initial access, elevate privileges, and perform remote code execution to achieve full system compromise.

Microsoft CVEs:

CVE ID	Vulnerability Type	CVSS v3.1 Score	Affected Product(s)	Affected Versions
CVE-2025-60724	Remote Code Execution (RCE)	9.8 (Critical)	Windows Graphics Component (GDI+)	**Windows 10 (all versions), Windows 11 (all versions), Windows Server 2012, 2016, 2019, 2022**
CVE-2025-30398	Information Disclosure (ID)	8.1 (High)	Nuance PowerScribe 360	**Versions 3.0 and earlier (Hotfix 1 to Hotfix 14)**
CVE-2025-59512	Elevation of Privilege (EoP)	7.8 (High)	Windows Customer Experience Improvement Program (CEIP)	**Windows 10 (all versions), Windows 11 (all versions), Windows Server 2019, 2022**
CVE-2025-60705	Elevation of Privilege (EoP)	7.8 (High)	Windows Client-Side Caching	**Windows 10 (all versions), Windows 11 (all versions), Windows Server 2019, 2022**
CVE-2025-62199	Remote Code Execution (RCE)	7.8 (High)	Microsoft Office	**Microsoft Office 2019, 2021, and 365 (up to build 16.0.x)**

CVE-2025-62215	**Elevation of Privilege (EoP)**	7.0 (High)	Windows Kernel	**Windows 10 (21H2 and later), Windows 11 (21H2 and later), Windows Server 2019, Windows Server 2022**
CVE-2025-60716	Elevation of Privilege (EoP)	7.0 (High)	DirectX Graphics Kernel	**Windows 10 (all versions), Windows 11 (all versions), Windows Server 2019, Windows Server 2022**
CVE-2025-60719	Elevation of Privilege (EoP)	7.0 (High)	Windows Ancillary Function Driver for WinSock (AFD)	**Windows 10 (all versions), Windows 11 (all versions), Windows Server 2019, 2022**
CVE-2025-62213	Elevation of Privilege (EoP)	7.0 (High)	Windows Ancillary Function Driver for WinSock (AFD)	**Windows 10 (all versions), Windows 11 (all versions), Windows Server 2019, 2022**
CVE-2025-62217	Elevation of Privilege (EoP)	7.0 (High)	Windows Ancillary Function Driver for WinSock (AFD)	**Windows 10 (all versions), Windows 11 (all versions), Windows Server 2019, 2022**
CVE-2025-62214	Remote Code Execution (RCE)	6.7 (Medium)	Visual Studio	**Visual Studio 2022 (prior to 17.8.6), Visual Studio 2019 (prior to 16.11.33)**

The Cal-CSIC recommends immediately applying the patches released by Microsoft as part of the November 2025 Patch Tuesday update cycle.

For further information on applying Microsoft's security patch and workarounds please use this link:

- **November 11, 2025—KB5068861 (OS Builds 26200.7171 and 26100.7171) - Microsoft Support**

References

[1] NVD; "CVE-2025-60724 Detail" https://nvd.nist.gov/vuln/detail/CVE-2025-60724, accessed 19 November 2025

[2] Microsoft Security Response Center (MSRC); "Windows Kernel Elevation of Privilege Vulnerability CVE-2025-62215" https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-62215; accessed 20 November 2025

[3] SOC Radar; "November 2025 Patch Tuesday: Microsoft Fixes 63 Vulnerabilities, Including Windows Kernel Zero-Day (CVE-2025-62215)" https://socradar.io/november-2025-patch-tuesday-microsoft-cve-2025-62215/; accessed 19 November 2025

[4] Github; "CVE-2025-62215-exploit-poc" https://github.com/dexterm300/CVE-2025-62215-exploit-poc; accessed 19 November 2025