مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates- Microsoft- November 2025

Tracking #:432317996

Date:12-11-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Microsoft has released its November 2025 Patch Tuesday, addressing a total of 68 vulnerabilities, including a high-priority zero-day flaw already being actively exploited in the wild.

TECHNICAL DETAILS:

Microsoft has released its November 2025 Patch Tuesday security updates, addressing 68 vulnerabilities across multiple products and services.
This includes:

- 1 actively exploited zero-day vulnerability
- 5 critical severity flaws
- 64 important vulnerabilities

The updates span core components such as Windows Kernel, Microsoft Office, Visual Studio, DirectX, SQL Server, Windows Hyper-V, and Edge (Chromium-based).

Zero-day and Critical Severity Vulnerabilities:

CVE ID	Title / Component	Vulnerability Type	Impact	Attack Vector / Notes	Severity
CVE-2025-62215	Windows Kernel Elevation of Privilege	Race Condition (EoP)	Gain SYSTEM privileges	Actively exploited zero-day; requires authenticated access	Critical / Exploited
CVE-2025-60724	GDI+ Component	Remote Code Execution (Heap Overflow)	Execute arbitrary code remotely	Exploitation via crafted metafile document	Critical
CVE-2025-62199	Microsoft Office	Remote Code Execution (Use-after-free)	Execute arbitrary code locally	User interaction required (malicious document)	Critical
CVE-2025-60716	DirectX Graphics Kernel	Elevation of Privilege (Use-after-free)	Gain SYSTEM privileges	Race condition; requires authenticated attacker	Critical
CVE-2025-62214	Visual Studio	Command Injection	Execute arbitrary code locally	Requires authenticated access	Critical
CVE-2025-30398	Nuance PowerScribe 360	Information Disclosure	Sensitive data exposure	Exploitation via unauthenticated API call	Critical

Affected Products

This release impacts multiple product families and services, including:

- **Windows OS:** Kernel, DirectX, Smart Card, Routing and Remote Access (RRAS), Bluetooth RFCOMM Driver, Multimedia Scheduler, Log File System, Hyper-V, WLAN, and TDX.sys.
- **Microsoft Office Suite:** Excel, Word, SharePoint, and Dynamics 365 (on-premises & cloud).
- **Developer Tools:** Visual Studio, Visual Studio Code, GitHub Copilot, and CoPilot Chat Extension.
- **Server Components:** SQL Server, Windows License Manager, Configuration Manager.
- **Other Components:** Nuance PowerScribe 360, OneDrive for Android, Microsoft Graphics Component, Windows Subsystem for Linux GUI.

RECOMMENDATIONS:

Prioritize Deployment

- Deploy the November 2025 cumulative updates across all Windows endpoints and servers.
- Patch CVE-2025-62215 (Zero-day) on high-priority systems first.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://msrc.microsoft.com/update-guide/releaseNote/2025-Nov