EnCyb

Severity: Critical

Advisory Type: Security

Various Vulnerabilities in MS Windows

Advisory Report

TLP: WHITE

SECURITY THREAT ADVISORY COUNCIL (STAC)

Empowering organizations with cutting-edge cybersecurity strategies to combat emerging digital threats effectively.

EXECUTIVE SUMMARY

Microsoft's recent December 2025 Patch Tuesday resolves over 57 vulnerabilities, including three zero-days and multiple critical Office-based RCE flaws, one of which is actively exploited. Organizations should urgently prioritize patching zero-day and high-risk components to mitigate active threats and prevent privilege-escalation attack chains.

- Active Region: Global
- Affected Sector: All sectors using Windows, MS Office, and PowerShell, including developer environments.
- Affected Products: All Windows and Office users are affected
- Severity: Critical, Important and Low severity flaws, including three zero-days.
- Published Date: December 09, 2025

TECHNICAL DETAILS – CRITICAL VULNERABILITIES

CVE-2025-62554 – MS Office RCE

- Attack Vector: The MS Office document parsing pipeline mishandles object metadata during deserialization.
- Cause: A type confusion condition causes the parser to treat an attacker-controlled object as a trusted structure, enabling redirection of execution flow.
- Prerequisite: User interaction to load the malicious document (Open or Preview).
- Risk: Allows controlled code execution in user context; low-complexity exploit due to predictable parser behavior.

CVE-2025-62557 – MS Office RCE

- Attack Vector: The Office memory allocator incorrectly manages object lifetime during document rendering.
- Cause: A use-after-free (UAF) fault where a freed heap pointer is subsequently dereferenced, permitting overwrite of adjacent memory with attacker data.
- Prerequisite: User must open a malicious Office document crafted with unstable object reference structures.
- Risk: Reliable path to full RCE; attackers can pivot into payload staging (e.g., shellcode injection via heap grooming).

CVE-2025-62562 – MS Outlook RCE

- Attack Vector: Outlook's MIME/HTML rendering engine processes untrusted email content in the preview pane.
- Cause: A memory corruption vulnerability triggered by malformed rendering directives or object length fields in incoming messages.
- Prerequisite: In many configurations, only message preview is required—parsing occurs automatically.
- Risk: High-impact RCE enabling credential extraction, malware deployment, or mailbox takeover without explicit user interaction.

IMPORTANT/LOW VULNERABILITIES

CVE	TITLE	SEVERITY	IMPACT
CVE-2025-62572	Application Information Service EoP	Important	EoP
CVE-2025-62550	Azure Monitor Agent RCE	Important	RCE
CVE-2025-64671	GitHub Copilot for JetBrains RCE	Important	RCE
CVE-2025-62569	MS Brokering File System EoP	Important	EoP
CVE-2025-62469	MS Brokering File System EoP	Important	EoP
CVE-2025-64666	MS Exchange EoP	Important	EoP
CVE-2025-64667	MS Exchange Spoofing	Important	Spoof
CVE-2025-64670	Win DirectX Info Disclosure	Important	InfoDisc
CVE-2025-62552	MS Access RCE	Important	RCE
CVE-2025-62560	MS Excel RCE	Important	RCE
CVE-2025-62563	MS Excel RCE	Important	RCE
CVE-2025-62561	MS Excel RCE	Important	RCE
CVE-2025-62564	MS Excel RCE	Important	RCE
CVE-2025-62553	MS Excel RCE	Important	RCE
CVE-2025-62556	MS Excel RCE	Important	RCE
CVE-2025-62558	MS Word RCE	Important	RCE
CVE-2025-62559	MS Word RCE	Important	RCE
CVE-2025-62555	MS Word RCE	Important	RCE
CVE-2025-64672	MS SharePoint Spoofing	Important	Spoof
CVE-2025-62457	Win Cloud Files Minifilter EoP	Important	EoP
CVE-2025-62454	Win Cloud Files Minifilter EoP	Important	EoP
CVE-2025-62221	Win Cloud Files Minifilter EoP	Important	EoP
CVE-2025-62470	Win Common Log File System EoP	Important	EoP

CVE-2025-62468	Win Defender FW Info Disclosure	Important	InfoDisc
CVE-2025-62463	Win DirectX DoS	Important	DoS
CVE-2025-62465	Win DirectX DoS	Important	DoS
CVE-2025-62573	Win DirectX EoP	Important	EoP
CVE-2025-64679	Win DWM Core Library EoP	Important	EoP
CVE-2025-64680	Win DWM Core Library EoP	Important	EoP
CVE-2025-62567	Win Hyper-V DoS	Important	DoS
CVE-2025-62571	Win Installer EoP	Important	EoP
CVE-2025-62455	MSMQ EoP	Important	EoP
CVE-2025-54100	PowerShell RCE	Important	RCE
CVE-2025-62464	Win ProjFS EoP	Important	EoP
CVE-2025-55233	Win ProjFS EoP	Important	EoP
CVE-2025-62462	Win ProjFS EoP	Important	EoP
CVE-2025-62467	Win ProjFS EoP	Important	EoP
CVE-2025-62461	Win ProjFS Filter Driver EoP	Important	EoP
CVE-2025-62474	Win RAS EoP	Important	EoP
CVE-2025-62472	Win RAS EoP	Important	EoP
CVE-2025-62456	Win ReFS RCE	Important	RCE
CVE-2025-62549	Win RRAS RCE	Important	RCE
CVE-2025-62473	Win RRAS Info Disclosure	Important	InfoDisc
CVE-2025-64678	Win RRAS RCE	Important	RCE
CVE-2025-62565	Win File Explorer EoP	Important	EoP
CVE-2025-64661	Win Shell EoP	Important	EoP
CVE-2025-64658	Win File Explorer EoP	Important	EoP
CVE-2025-59517	Win VSP Driver EoP	Important	EoP
CVE-2025-59516	Win VSP Driver EoP	Important	EoP
CVE-2025-62458	Win32k EoP	Important	EoP
CVE-2025-62223	MS Edge for Mac Spoofing	Low	Spoof

RECOMMENDATIONS

- Apply all Important Windows kernel and driver updates to prevent EoP attacks.
- Patch all Critical and zero-day vulnerabilities immediately by following below reference source.
- Restrict untrusted documents and email attachments; enable Protected View and block macros.
- Harden PowerShell with strict execution policies and enhanced monitoring.
- Test patches on critical applications before rollout. But avoid delaying deployment.
- Verify patch completion with post-update scans.
- Enforce least-privilege access to reduce the impact of successful exploitation.
- Strengthen email security with advanced attachment and URL scanning.
- Tighten application allowlisting to block untrusted binaries and scripts.

REFRENCE

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

SECURE, SCALE, SUCCEED WITH

CONFIDENCE

EnCyb

www.encyb.com/contact-us/ EnCyb soc@encyb.com www.encyb.com