- The first vulnerability is CVE-2024-30051, a flaw in the Microsoft Scripting Engine (MSSE). This affects all supported versions of Windows 10 and 11, including their server versions. It allows attackers to run arbitrary code on vulnerable systems using the MSSE library.

- The second vulnerability is CVE-2025-32701, which exploits a weakness in the Windows Common Log File System (CLFS) driver, known as afd.sys. This affects all supported versions of Windows 10 and 11, including their server versions. It allows attackers to escalate their privileges on vulnerable systems using this component.

- The third vulnerability is CVE-2025-32702, which exploits a flaw in the Windows Ancillary Function Driver (WAFD), also known as clfn.exe. This affects all supported versions of Windows 10 and 11, including their server versions. It allows attackers to inject code into vulnerable systems using this component.

- The fourth vulnerability is CVE-2025-30401, which exploits a flaw in the Desktop Window Manager (DWM), also known as win32cwnd.dll or wm_win32c.dll. This affects all supported versions of Windows 10 and 11, including their server versions. It allows attackers to take control of vulnerable systems by exploiting this component.

- The fifth vulnerability is CVE-2025-30399, which exploits a flaw in the WinRAR file archiver driver, known as m_winrar.dll. This affects all supported versions of Windows 10 and 11, including their server versions. It allows attackers to create and execute malicious files using this component.