Five Zero-Days Actively Exploited – Microsoft May 2025 Patch Tuesday

Overview

Microsoft released fixes for 72 vulnerabilities this month, including five zero-days already being exploited in the wild. Four of the five are elevation-of-privilege vulnerabilities that allow attackers to gain SYSTEM-level access once inside a host. The fifth impacts the Microsoft Scripting Engine and allows for remote code execution through malicious web content in Edge or Internet Explorer mode.

These zero-days affect all supported versions of Windows 10, Windows 11, and associated server builds. Although Microsoft has not released specific IoCs or exploitation details, they've confirmed active abuse in the wild.

TL;DR

Microsoft's May 2025 Patch Tuesday includes fixes for five actively exploited zero-day vulnerabilities, all of which allow privilege escalation or remote code execution.

These flaws impact core Windows components, including the Common Log File System, Desktop Window Manager, WinSock, and Microsoft's Scripting Engine. Environments should be patched immediately.

Vulnerability Breakdown

- CVE-2025-30400 (CVSS 7.8) **– DWM Core Library EoP**
  Elevation-of-privilege via a use-after-free in Desktop Window Manager. Grants SYSTEM-level access.
- CVE-2025-32701 (CVSS 7.8) **– Common Log File System Driver EoP**
  Use-after-free bug giving SYSTEM access through the CLFS driver. Part of a known attack pattern.
- CVE-2025-32706 (CVSS 7.8) **– Common Log File System Driver EoP**
  Improper input validation flaw also affecting the CLFS driver.
- CVE-2025-32709 (CVSS 7.8) **– Ancillary Function Driver for WinSock EoP**
  Use-after-free vulnerability in the afd.sys driver that allows local privilege escalation to SYSTEM.
- CVE-2025-30397(CVSS 7.5) **– Microsoft Scripting Engine RCE**
  Type confusion vulnerability in the scripting engine exploited via web content. Attackers must trick users into clicking a malicious link, but successful exploitation leads to remote code execution.

For the second month in a row, Microsoft has patched multiple zero-days tied to privilege escalation, mostly use-after-free bugs in core components like CLFS and afd.sys. These flaws are becoming a reliable tool for attackers who already have a foothold. They're simple and lead straight to SYSTEM access. Aspire recommends you patch affected products as soon as possible.

Aspire Protects

- **Patch –** Apply all May 2025 Windows updates immediately across all endpoints and servers. See the links above for guidance.
- Prioritize systems exposed to the internet, high-risk users, and critical infrastructure.
- Monitor for abnormal privilege escalation, LSASS access, or unusual registry or service changes post-patch.
- Educate users on phishing and social engineering - CVE-2025-30397 requires user interaction.
- Consider enhanced EDR visibility for lateral movement post-EoP, especially in hybrid AD environments.

TTPs to Watch

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – All four EoP zero-days can be used by attackers to gain SYSTEM access after initial compromise.

Execution

- Exploitation for Client Execution [T1203] – CVE-2025-30397 can be triggered through malicious web content requiring minimal user interaction.

Defense Evasion

- Indicator Removal on Host [T1070.004] – Attackers abusing SYSTEM access may disable security tools or clear logs.

Credential Access

- OS Credential Dumping [T1003.001] – SYSTEM access allows access to LSASS and stored credentials.

IoCs

There are no known IoCs associated with the above vulnerabilities at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

These vulnerabilities affect nearly every Windows environment, but the risk is higher for sectors where attackers often seek privilege escalation to access sensitive systems or move laterally.

- Healthcare
- Education
- Retail
- Finance
- Manufacturing
- Government

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**

- The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
- Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

CVE-2025-32709 - Security Update Guide - Microsoft - Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability

CVE-2025-30397 - Security Update Guide - Microsoft - Scripting Engine Memory Corruption Vulnerability

CVE-2025-32706 - Security Update Guide - Microsoft - Windows Common Log File System Driver Elevation of Privilege Vulnerability

CVE-2025-32701 - Security Update Guide - Microsoft - Windows Common Log File System Driver Elevation of Privilege Vulnerability

CVE-2025-30400 - Security Update Guide - Microsoft - Microsoft DWM Core Library Elevation of Privilege Vulnerability