Security Advisory 2025-017

Critical Vulnerabilitites in Microsoft Products

2025-04-10 — v1.0

TLP:CLEAR

History:

- *10/04/2025 — v1.0 – Initial publication*

Summary

On 8 April 2025, Microsoft released fixes addressing more than 100 vulnerabilities in various Microsoft products, 11 of which are rated as Critical [1,2,3].

It is recommended updating as soon as possible, prioritising critical devices and public facing assets.

Technical Details

This advisory describes some notable vulnerabilities addressed by the April 2025 Patch Tuesday.

The vulnerability **CVE-2025-29824**, with a CVSS score of 7.8, is a user-after-free vulnerability in the Windows Common Log File System (CLFS) that can be exploited by attackers to elevate their privileges to `SYSTEM` on previously compromised Windows machines. This vulnerability is being exploited in the wild.

The vulnerabilities **CVE-2025-26663** and **CVE-2025-26670**, both with a CVSS score of 8.1, are unauthenticated Remote Code Execution (RCE) vulnerabilities caused by user-after-free weaknesses in the Windows Lightweight Directory Access Protocol (LDAP). To be exploitable, they require an attacker to win a race condition via specially crafted requests sequentially sent to a vulnerable LDAP server.

The vulnerabilities **CVE-2025-27480** and **CVE-2025-27482**, both with a CVSS score of 8.1, are RCE vulnerabilities in Windows Remote Desktop Services (RDP). To exploit them, an attacker must first connect to a system with the Remote Desktop Gateway role and trigger a race condition to create an exploitable use-after-free scenario.

The vulnerabilities **CVE-2025-29791**, **CVE-2025-27749**, **CVE-2025-27748**, **CVE-2025-27745**, and **CVE-2025-27752**, all with a CVSS score of 7.8, are remote code execution flaws in Microsoft Office and Excel applications that could be exploited by a bad actor using a specially crafted Excel document, resulting in full system control.

Affected Products

These vulnerabilities affect several Microsoft products such as Windows 10 and 11, Windows Server, Microsoft Office, Hyper-V.

Please refer to the vendor website for more information for an exhaustive list of affected products [1].

Recommendations

It is recommended updating as soon as possible, prioritising critical devices and public facing assets.

It is also recommended restricting access to affected services, such as RDP and LDAP, to only trusted sources.

References

[1] https://msrc.microsoft.com/update-guide/releaseNote/2025-apr

[2] https://www.helpnetsecurity.com/2025/04/08/patch-tuesday-microsoft-zero-day-cve-2025-29824/

[3] https://thehackernews.com/2025/04/microsoft-patches-126-flaws-including.html