CERT-EU

Security Advisory 2025-032

Multiple Vulnerabilities in Microsoft Products

2025-08-18 — v1.0

TLP:CLEAR

History:

- *18/08/2025 — v1.0 – Initial publication*

Summary

On August 13, 2025, Microsoft released its August 2025 Patch Tuesday advisory addressing 111 security flows in various products among which 16 are rated as critical [1].

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

Technical Details

Below are listed the notable vulnerabilities among those rated as critical by Microsoft:

The vulnerability **CVE-2025-50176**, with a CVSS score of 7.8, is due to a type confusion flaw in the DirectX Graphics Kernel allowing an authenticated attacker to execute code locally [2].

The vulnerability **CVE-2025-50165**, with a CVSS score of 9.8, is due to the use of untrusted pointer dereference in Microsoft Graphics Component allowing an authenticated attacker to execute code over a network without user interaction [3].

The vulnerabilities **CVE-2025-53740** and **CVE-2025-53731**, with a CVSS score of 8.4, are use after free security flaws in Microsoft Office, and allow a remote attacker to execute code locally. Microsoft confirmed that the Preview Pane is also an attack vector [4,5].

The vulnerabilities **CVE-2025-53784** and **CVE-2025-53733**, with a CVSS score of 8.4, are use after free security flaws in Microsoft Word, and allow a remote attacker to execute code locally. Microsoft confirmed that the Preview Pane is also an attack vector [6,7].

The vulnerability **CVE-2025-48807**, with a CVSS score of 7.5, is due to improper restriction of communication channel to intended endpoints in Windows Hyper-V allowing an authenticated attacker to execute code locally. The vulnerable endpoint is only available over the local VM interface as all external communication is blocked. This means an attacker needs to execute code from the local machine to exploit the vulnerability. This vulnerability also requires an interaction from an administrator [8].

The vulnerability **CVE-2025-53766**, with a CVSS score of 9.8, is a heap-based buffer overflow flaw in Windows GDI+ an unauthenticated attacker to execute code over a network. An attacker doesn't require any privileges on the systems hosting the web services. Successful exploitation of this vulnerability could cause Remote Code Execution or Information Disclosure on web services that are parsing documents that contain a specially crafted metafile, without the involvement of a victim user. An attacker could trigger this vulnerability by convincing a victim to download and open a document that contains a specially crafted metafile. In the worst-case scenario, an attacker could trigger this vulnerability on web services by uploading documents containing a specially crafted metafile without user interaction [9].

The vulnerability **CVE-2025-50177**, with a CVSS score of 8.1, is a use after free vulnerability in Windows Message Queuing allowing an unauthenticated attacker to execute code over a network. To exploit this vulnerability, an attacker would need to send a series of specially crafted MSMQ packets in a rapid sequence over HTTP to a MSMQ server. This could result in remote code execution on the server side [10].

The vulnerability **CVE-2025-53778**, with a CVSS score of 8.8, is due to improper authentication in Windows NTLM and allows an authenticated attacker to elevate privileges over a network. An attacker who successfully exploited this vulnerability could gain SYSTEM privileges [11].

Affected Products

Microsoft Office, Office Word and Microsoft Windows are affected by the vulnerabilities described above.

For the list of all products affected, refer to Microsoft's advisory [1].

Recommendations

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

References

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

[2] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-50176

[3] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-50165

[4] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53740

[5] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53731

[6] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53784

[7] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53733

[8] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-48807

[9] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53766

[10] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-50177

[11] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53778