Security Advisory 2024-045

Multiple Vulnerabilities in Microsoft Products

May 16, 2024 — v1.0

TLP:CLEAR

History:

- *16/05/2024 — v1.0 – Initial publication*

Summary

On May 16, 2024, Microsoft addressed 61 vulnerabilities in its May 2024 Patch Tuesday update, including two actively exploited zero-days [1]. This Patch Tuesday also fixes one critical vulnerability, a Microsoft SharePoint Server Remote Code Execution Vulnerability [1].

It is recommended applying updates as soon as possible on affected products.

Technical Details

Actively Exploited Zero-Days

The first zero-day vulnerability, tracked as **CVE-2024-30040** with a CVSS score of 10, is described as an OLE mitigation bypass in Microsoft 365 and Microsoft Office which protect users from vulnerable COM/OLE controls [3]. An unauthenticated attacker who successfully exploited this vulnerability could gain code execution through convincing a user to open a malicious document at which point the attacker could execute arbitrary code in the context of the user [3].

The second zero-day vulnerability, tracked as **CVE-2024-30051** with a CVSS score of 6.8, is an elevation of privilege residing in the Windows DWM Core Library. An attacker who successfully exploited this vulnerability could gain SYSTEM privileges [4].

Critical Vulnerability

A Microsoft SharePoint Server remote code execution vulnerability, tracked as **CVE-2024-30044** with a CVSS score of 8.3, was also fixed. An authenticated attacker with Site Owner permissions or higher could upload a specially crafted file to the targeted Sharepoint Server and craft specialised API requests to trigger deserialisation of the file's parameters. This would enable the attacker to perform remote code execution in the context of the Sharepoint Server [5].

Affected Products

Affected products include, but are not limited to, Microsoft Windows, Microsoft Office, SharePoint Server, Windows Defender, Visual Studio [2].

Recommendations

It is recommended applying updates as soon as possible on affected assets.

References

[1] https://www.bleepingcomputer.com/news/microsoft/microsoft-may-2024-patch-tuesday-fixes-3-zero-days-61-flaws/

[2] https://msrc.microsoft.com/update-guide/releaseNote/2024-May

[3] https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-30040

[4] https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-30051

[5] https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-30044