Security Advisory 2024-116

Microsoft November 2024 Patch Tuesday

2024-11-13 — v1.0

TLP:CLEAR

History:

- *13/11/2024 — v1.0 – Initial publication*

Summary

Microsoft's November 2024 Patch Tuesday addresses 91 vulnerabilities, including four zero-day vulnerabilities. Two of these zero-days, CVE-2024-43451 (NTLM Hash Disclosure Spoofing) and CVE-2024-49039 (Windows Task Scheduler Elevation of Privilege), have been actively exploited. These vulnerabilities allow attackers to potentially gain unauthorised access or escalate privileges through minimal user interaction or crafted applications [1-4].

Technical Details

- **CVE-2024-43451**: An NTLM Hash Disclosure Spoofing vulnerability allows attackers to capture NTLMv2 hashes through minimal interaction with a malicious file, enabling authentication as the compromised user [3].
- **CVE-2024-49039**: A Windows Task Scheduler vulnerability allows privilege escalation to Medium Integrity level, enabling attackers to execute RPC functions usually restricted to privileged accounts [2].
- **CVE-2024-49040**: A spoofing vulnerability in Microsoft Exchange allows manipulation of the `P2 FROM` header, causing spoofed emails to appear legitimate [1].
- **CVE-2024-49019**: An Active Directory Certificate Services flaw allows domain administrator access by abusing version 1 certificate templates [4].

Affected Products

- Microsoft Exchange Server (CVE-2024-49040) [1]
- Microsoft Windows, all versions (CVE-2024-49039 and CVE-2024-43451) [2,3]
- Active Directory Certificate Services (CVE-2024-49019) [4]

Recommendations

It is highly recommended to install the latest patch available to mitigates these vulnerabilities.

References

[1] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49040

[2] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49039

[3] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43451

[4] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49019