CERT-EU

Security Advisory 2024-106

Multiple Critical Vulnerabilities in Microsoft Products

2024-10-09 — v1.0

TLP:CLEAR

History:

- *09/10/2024 — v1.0 – Initial publication*

Summary

On October 8, 2024, Microsoft addressed 118 vulnerabilities in its October 2024 Patch Tuesday update, including five zero-day vulnerabilities. This Patch Tuesday also fixes three critical vulnerabilities [1,2].

Technical Details

We highlight here the zero-day vulnerabilities, but it is highly recommended to deploy Microsoft patches for all 118 vulnerabilities identified.

The vulnerability **CVE-2024-43573**, with a CVSS score 6.5, could be a bypass of a previous vulnerability that abused MSHTML to spoof file extensions in alerts displayed when opening files [3].

The vulnerability **CVE-2024-43572**, with a CVSS score 7.8, is a vulnerability that could allow malicious Microsoft Saved Console (MSC) files to perform remote code execution on vulnerable devices.[4].

The vulnerability **CVE-2024-6197**, with a CVSS score 8.8, is a `libcurl` remote code execution flaw that could cause commands to be executed when Curl attempts to connect to a malicious server [5].

The vulnerability **CVE-2024-20659**, with a CVSS score 7.1, is a UEFI bypass that could allow attackers to compromise the hypervisor and kernel [6].

The vulnerability **CVE-2024-43583**, with a CVSS score 7.1, is an elevation of privileges flaw that could give attackers SYSTEM privileges in Windows [7].

Affected Products

Detailed information about each vulnerability and affected systems can be found in Microsoft's security bulletins [1].

Recommendations

It is recommended applying updates to the affected devices as soon as possible, prioritising Internet facing devices, and critical servers.

References

[1] https://msrc.microsoft.com/update-guide/releaseNote/2024-Oct

[2] https://www.bleepingcomputer.com/news/microsoft/microsoft-october-2024-patch-tuesday-fixes-5-zero-days-118-flaws/

[3] https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-43573

[4] https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-43572

[5] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6197

[6] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20659

[7] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43583