Security Advisory 2024-093

Multiple Critical Vulnerabilities in Microsoft Products

2024-09-11 — v1.0

TLP:CLEAR

History:

- *11/09/2024 — v1.0 – Initial publication*

Summary

On September 10, 2024, Microsoft addressed 79 vulnerabilities in its September 2024 Patch Tuesday update, including four zero-day vulnerabilities. This Patch Tuesday also fixes seven critical vulnerabilities [1,2].

Technical Details

We highlight here the zero-day vulnerabilities, but it is highly recommended to deploy Microsoft patches for all 79 vulnerabilities identified.

CVE-2024-38014, with a CVSS score 7.8, is a Windows Installer Elevation of Privilege Vulnerability that could allow an attacker to gain SYSTEM privileges [3].

CVE-2024-38217, with a CVSS score 5.4, is a Windows Mark of the Web Security Feature Bypass Vulnerability that could allow an attacker to host a file on an attacker-controlled server, then convince a targeted user to download and open the file. This could allow the attacker to interfere with the Mark of the Web functionality [4].

CVE-2024-38226, with a CVSS score 7.3, is a Microsoft Publisher Security Feature Bypass Vulnerability that could allow an attacker to bypass Office macro policies used to block untrusted or malicious files [5].

CVE-2024-43491, with a CVSS score 9.8, is a Microsoft Windows Update Remote Code Execution Vulnerability that could allow an attacker to exploit previously mitigated vulnerabilities on Windows 10, version 1507 (Windows 10 Enterprise 2015 LTSB and Windows 10 IoT Enterprise 2015 LTSB) systems that have installed the Windows security update released on March 12, 2024—KB5035858 (OS Build 10240.20526) or other updates released until August 2024. All later versions of Windows 10 are not impacted by this vulnerability [6].

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-Sep

[2] https://www.bleepingcomputer.com/news/microsoft/windows-10-kb5043064-update-released-with-6-fixes-security-updates/

[3] https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-38014

[4] https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-38217

[5] https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-38226

[6] https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-43491