Security Advisory 2024-067

# Multiple Vulnerabilities in Microsoft Products

*July 12, 2024 — v1.1*

**TLP:CLEAR**

*History:*

- *10/07/2024 — v1.0 – Initial publication*
- *12/07/2024 — v1.1 – Add information about CVE-2024-38021*

## Summary

On July 10, 2024, Microsoft addressed 139 vulnerabilities in its July 2024 Patch Tuesday update, including four zero-day vulnerabilities. Two zero-day vulnerabilities are actively exploited [1,2,3]. Additionally, five critical vulnerabilities leading to Remote Code Execution have been patched.

It is recommended updating as soon as possible.

## Technical Details

### Zero-day Vulnerabilities

The zero-day vulnerability **CVE-2024-38080**, with a CVSS score of 7.8, allow attackers to gain `SYSTEM` privileges on the host machine, but initial local access is required to exploit the flaw, according to Microsoft [4]. This vulnerability is being exploited.

The zero-day vulnerability **CVE-2024-38112**, with a CVSS score of 7.5, is a spoofing vulnerability in Windows MSHTML Platform that can be triggered with a specially crafted HTML file [5]. Exploitation of this vulnerability likely requires the use of an "attack chain" of exploits or programmatic changes on the target host. This vulnerability is being exploited.

The zero-day vulnerability **CVE-2024-35264**, with a CVSS score of 8.1, is a RCE vulnerability affecting .NET and Visual Studio. According to the advisory, the attack complexity is high because some conditions are beyond the attacker's control [6].

The zero-day vulnerability **CVE-2024-37985**, with a CVSS score of 5.9, affects ARM systems. By exploiting this vulnerability, an attacker would be able to view heap memory from a privileged process running on the server [7]. According to the advisory, the attack complexity is high because some conditions are beyond the attacker's control.

### Other Critical Vulnerabilities

The vulnerabilities **CVE-2024-38076**, **CVE-2024-38077**, and **CVE-2024-38074**, with a CVSS score of 9.8, affect the Windows Remote Desktop Licensing Service component that manages client access licenses (CALs) for remote desktop services, and could lead to remote code execution if exploited [8,9,10].

The vulnerability **CVE-2024-38060**, with a CVSS score of 8.8, is a Windows Imaging Component Remote Code Execution Vulnerability. [11]

The vulnerability **CVE-2024-38023**, with a CVSS score of 7.2, is a Microsoft SharePoint Server Remote Code Execution Vulnerability. [12]

**[New]** The vulnerability **CVE-2024-38021**, with a CVSS scode of 8.8, is a Remote Code Execution flow in Microsoft Outlook. It is not considered critical by Microsoft because it requires a one click user interaction for untrusted senders (while it does not require any user interaction for trusted sender). Attackers could exploit this vulnerability to gain unauthorised access, execute arbitrary code, and cause substantial damage without any user interaction. The absence of authentication requirements makes it particularly dangerous, as it opens the door to widespread exploitation. [13]

## Affected Products

Affected products include, but are not limited to, Microsoft Windows, Microsoft Server, Microsoft Office and Microsoft Sharepoint, .NET and Visual Studio, Windows Remote Desktop Licensing Service.

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

## Recommendations

It is recommended applying updates to all affected assets as soon as possible, prioritising Internet facing devices, and devices affected by zero-day and critical vulnerabilities.

## References


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

[2] https://www.bleepingcomputer.com/news/microsoft/microsoft-july-2024-patch-tuesday-fixes-142-flaws-4-zero-days/

[3] https://krebsonsecurity.com/2024/07/microsoft-patch-tuesday-july-2024-edition/

[4] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38080

[5] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112

[6] https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-35264

[7] https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-37985

[8] https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-38076

[9] https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-38077

[10] https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-38074

[11] https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-38060

[12] https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-38023

[13] https://blog.morphisec.com/cve-2024-38021-microsoft-outlook-moniker-rce-vulnerability