10 years CERT-EU

Security Advisory 2024-080

Multiple Critical Vulnerabilities in Microsoft Products

August 14, 2024 — v1.0

TLP:CLEAR

History:

- *14/08/2024 — v1.0 – Initial publication*

Summary

On August 13, 2024, Microsoft addressed 89 vulnerabilities in its August 2024 Patch Tuesday update, including ten zero-day vulnerabilities. This Patch Tuesday also fixes six critical vulnerabilities [1,2].

Technical Details

We highlight here the most critical vulnerabilities, but it is highly recommended to deploy Microsoft patches for all 89 vulnerabilities identified.

CVE-2024-38063, with a CVSS score 9.8, is a Windows TCP/IP Remote Code Execution Vulnerability that could allow an unauthenticated attacker to repeatedly send IPv6 packets, which include specially crafted packets, to a Windows machine which could enable remote code execution [3].

CVE-2024-38140, with a CVSS score 9.8, is a Windows Reliable Multicast Transport Driver (RMCAST) Remote Code Execution Vulnerability that could allow an unauthenticated attacker to exploit the vulnerability by sending specially crafted packets to a Windows Pragmatic General Multicast (PGM) open socket on the server, without any interaction from the user [4].

CVE-2024-38199, with a CVSS score 9.8, is a zero-day Windows Line Printer Daemon (LPD) Service Remote Code Execution Vulnerability that could allow an unauthenticated attacker to send a specially crafted print task to a shared vulnerable Windows Line Printer Daemon (LPD) service across a network. Successful exploitation could result in remote code execution on the server [5,6].

CVE-2024-38108, with a CVSS score 9.3, is an Azure Stack Hub Spoofing Vulnerability that could allow an unauthenticated attacker to exploit this vulnerability by getting the victim to load malicious code into their web browser on the virtual machine, allowing the attacker to leverage an implicit identity of the virtual machine. The victim's web browser then would determine which host endpoints are accessible [7].

CVE-2024-38109, with a CVSS score 9.1, is an Azure Health Bot Elevation of Privilege Vulnerability that could allow an authenticated attacker to exploit an Server-Side Request Forgery

(SSRF) vulnerability in Microsoft Azure Health Bot to elevate privileges over a network [8].

CVE-2024-38159 and **CVE-2024-38160**, with a CVSS score 9.1, is a Windows Network Virtualization Remote Code Execution Vulnerability that could allow an attacker to exploit the vulnerability by taking advantage of the unchecked return value in the wnv.sys component of Windows Server 2016. By manipulating the content of the Memory Descriptor List (MDL), the attacker could cause unauthorised memory writes or even free a valid block currently in use, leading to a critical guest-to-host escape [9,10].

Affected Products

Affected products include, but are not limited to, Microsoft Windows, Microsoft Server, Microsoft Office and Microsoft Azure.

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 assets as soon as possible.

References

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

[2] https://www.bleepingcomputer.com/microsoft-patch-tuesday-reports/Microsoft-Patch-Tuesday-August-2024.html

[3] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38063

[4] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38140

[5] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38199

[6] https://www.bleepingcomputer.com/news/microsoft/microsoft-august-2024-patch-tuesday-fixes-9-zero-days-6-exploited/

[7] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38108

[8] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38109

[9] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38159

[10] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38160