Security Advisory 2024-056

Multiple Vulnerabilities in Microsoft Products

June 19, 2024 — v1.2

TLP:CLEAR

History:

- *12/06/2024 — v1.0 – Initial publication*
- *17/06/2024 — v1.1 – Adding information about vulnerabilities*
- *19/06/2024 — v1.2 – Adding information about vulnerabilities*

Summary

On June 11, 2024, Microsoft addressed 58 vulnerabilities in its June 2024 Patch Tuesday update, including one zero-day vulnerability (CVE-2023-50868) [1,2,3]. This Patch Tuesday also fixes one critical vulnerability (CVE-2024-30080), a Microsoft Message Queuing (MSMQ) remote code execution vulnerability [4]. Finally, worth a mention are a couple of remote code execution vulnerabilities in Microsoft Outlook (CVE-2024-30103) [5] and Windows Wi-Fi Driver (CVE-2024-30078) [6].

Technical Details

A critical vulnerability in Microsoft Message Queuing (MSMQ), tracked as **CVE-2024-30080** with a CVSS score of 9.8, could allow remote code execution on an affected server. An attacker could exploit this vulnerability by sending a specially crafted malicious MSMQ packet to an MSMQ server. Successful exploitation would enable the attacker to execute arbitrary code on the server, potentially taking control of the system [4].

CVE-2023-50868, with a CVSS score 6.5, is a zero-day vulnerability in DNSSEC validation where an attacker could exploit standard DNSSEC protocols intended for DNS integrity by using excessive resources on a resolver, causing a denial of service for legitimate users [2,3].

One of the remote code execution vulnerabilities addressed in the latest update is **CVE-2024-30103**, with a CVSS score of 8.8. This vulnerability affects Microsoft Outlook. An attacker, authenticated with valid Exchange user credentials, could exploit this vulnerability by bypassing Outlook registry block lists and creating malicious DLL files, potentially leading to remote code execution [5].

CVE-2024-30078, with a CVSS score of 8.8, is a remote code execution vulnerability in Windows Wi-Fi Driver. An unauthenticated attacker could send a malicious networking packet to an adjacent system using a Wi-Fi networking adapter, enabling remote code execution. Exploiting this vulnerability requires the attacker to be within proximity of the target system to send and receive radio transmissions [6].

Affected Products

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

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-Jun

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

[3] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-50868

[4] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-30080

[5] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30103

[6] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-30078