Security Advisory 2022-079

Exploited 0-days and Critical Vulnerabilities in Microsoft Windows

November 9, 2022 — v1.0

TLP:CLEAR

History:

- *09/11/2022 — v1.0 – Initial publication*

Summary

On November 8, 2022, Microsoft released its Patch Tuesday advisory which contains information about 68 flaws, for which 11 are rated as critical, and 6 are exploited 0-day vulnerabilities [1]. The exploitation of these vulnerabilities could lead to elevation of privilege, security feature bypass, remote code execution, information disclosure, denial of service and spoofing [2].

It is highly recommended applying the fixes as soon as possible.

Technical Details

This month's Patch Tuesday fixes six actively exploited zero-day vulnerabilities (publicly disclosed or actively exploited with no official fix available), with one being publicly disclosed:

- `CVE-2022-41128` is a Remote Code Execution vulnerability in the JScript9 Scripting Language. This could be exploited by convincing a user to visit a specially crafted server share or website (usually using phishing techniques).
- `CVE-2022-41091` is a Security Feature Bypassing vulnerability. An attacker could craft a malicious file that will evade Mark of the Web (MOTW) defences resulting in a limited loss of integrity and availability of security features such as Protected View in Microsoft Office, which rely on MOTW tagging [3].
- `CVE-2022-41073` is an Elevation of Privilege Vulnerability, which could allow an attacker to gain **SYSTEM** privileges by exploiting a flaw in the Windows Print Spooler.
- `CVE-2022-41125` is an Elevation of Privilege Vulnerability, which could allow an attacker to gain **SYSTEM** privileges by exploiting a flaw in the Windows CNG Key Isolation Service.
- `CVE-2022-41040` is an Elevation of Privilege Vulnerability in Microsoft Exchange Server (`ProxyNotShell`), that could allow an attacker to run PowerShell in the context of the **SYSTEM**.
- `CVE-2022-41082` is a Remote Code Execution Vulnerability in Microsoft Exchange Server (`ProxyNotShell`). As an authenticated user, the attacker could attempt to trigger malicious code in the context of the server's account through a network call.

Affected Products

- Microsoft Windows Server from version 2008 R2, to version 2022 are affected.
- Microsoft Windows Desktop from version Windows 7, to version Windows 11 are affected.
- Microsoft Exchange Server 2013 Cumulative Update 23 is affected [4]
- Microsoft Exchange Server 2016 Cumulative Updates 22 and 23 are affected [4]
- Microsoft Exchange Server 2019 Cumulative Updates 11 and 12 are affected [4]

Recommendations

CERT-EU recommends applying the available fixes as soon as possible.

References

[1] https://www.bleepingcomputer.com/microsoft-patch-tuesday-reports/November-2022.html

[2] https://www.bleepingcomputer.com/news/microsoft/microsoft-november-2022-patch-tuesday-fixes-6-exploited-zero-days-68-flaws/

[3] https://twitter.com/wdormann/status/1544416883419619333

[4] https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-microsoft-exchange-server-2019-2016-and-2013-november-8-2022-kb5019758-2b3b039b-68b9-4f35-9064-6b286f495b1d