Security Advisory 2023-001

Zero-day and Critical Vulnerabilities in Microsoft Windows

January 11, 2023 — v1.0

TLP:CLEAR

History:

- *11/01/2023 — v1.0 – Initial publication*

Summary

On January 10, 2023, on their first Patch Tuesday of 2023, **Microsoft** fixed an actively exploited zero-day Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability and a total of 98 flaws [1]. Eleven of them were classified as **critical** by Microsoft as they allow remote code execution, bypass security features, or elevate privileges.

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

Technical Details

According to Microsoft, the zero-day vulnerability `CVE-2023-21674` is a Sandbox escape vulnerability that could lead to the elevation of privileges. *An attacker who successfully exploited this vulnerability could gain SYSTEM privileges.* [1][2]

There is a functional exploit code for the zero-day vulnerability.

The number of bugs in each vulnerability category is listed below:

- 39 Elevation of Privilege Vulnerabilities
- 4 Security Feature Bypass Vulnerabilities
- 33 Remote Code Execution Vulnerabilities
- 10 Information Disclosure Vulnerabilities
- 10 Denial of Service Vulnerabilities
- 2 Spoofing Vulnerabilities

Affected Products

Multiple versions of Microsoft Windows [2]. Please refer to the links provided for each vulnerability in order to identify the exact versions of each affected system and the patch that should be applied.

Recommendations

CERT-EU highly recommends installing the updates provided by Microsoft.

References

[1] https://www.bleepingcomputer.com/news/microsoft/microsoft-january-2023-patch-tuesday-fixes-98-flaws-1-zero-day/

[2] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21674