Security Advisory 2023-090

Microsoft Software Critical Zero-Day Vulnerabilities

November 20, 2023 — v1.0

TLP:CLEAR

History:

- *20/11/2023 — v1.0 – Initial publication*

Summary

On November 15, 2023, Microsoft released patches for 63 security flaws in its software, including five new zero-day vulnerabilities, three of which are actively exploited. These vulnerabilities pose significant risks and require immediate attention [1].

Technical Details

Among the vulnerabilities, the five disclosed zero-day vulnerabilities are:

- `CVE-2023-36025` - CVSS score **8.8**: A weakness that allows malicious content to bypass the Windows SmartScreen Security feature. SmartScreen is a built-in Windows component that tries to detect and block malicious websites and files. Microsoft's security advisory for this flaw says attackers could exploit it by getting a Windows user to click on a booby-trapped link to a shortcut file.
- `CVE-2023-36033` - CVSS score **7.8** : Microsoft has fixed an actively exploited and publicly disclosed Windows DWM Core Library vulnerability that can be used to elevate privileges to `SYSTEM` .
- `CVE-2023-36036` - CVSS score **7.8** : Microsoft has fixed an actively exploited and publicly disclosed Windows DWM Core Library vulnerability that can be used to elevate privileges to `SYSTEM` .
- `CVE-2023-36038` - CVSS score **8.2** : ASP.NET Core Denial of Service. An attacker that could successfully exploit this vulnerability could trigger an `OutOfMemoryException` , resulting in a DoS condition.
- `CVE-2023-36413` - CVSS score **6.5** : Microsoft Office Security Feature Bypass. An attacker could exploit this vulnerability using social engineering tactics to convince a target to open a malicious Microsoft Office file on a vulnerable system. Successful exploitation would result in a bypass of security features of Microsoft Office designed to protect users including Protected View and the file would be opened in editing mode instead of protected mode.

Affected Products

For the zero-day vulnerabilities, the affected products are:

- Microsoft Windows;
- ASP.NET;
- Microsoft Office.

Specific product and version details are available on Microsoft's security update guide [2]. This is also valid for the other vulnerabilities.

Recommendations

CERT-EU recommends immediate application of Microsoft's November patches [1].

References

[1] https://thehackernews.com/2023/11/alert-microsoft-releases-patch-updates.html

[2] https://msrc.microsoft.com/update-guide/releaseNote/2023-Nov