Security Advisory 2023-045

Microsoft July 2023 Patch Tuesday

July 12, 2023 — v1.0

TLP:CLEAR

History:

- *12/07/2023 — v1.0 – Initial publication*

Summary

Microsoft has released its July 2023 Patch Tuesday security updates, addressing a total of 130 vulnerabilities, including five that were exploited in the wild as zero-day vulnerabilities. Microsoft has also issued guidance on the malicious use of Microsoft signed drivers [1,2].

Technical Details

The July 2023 Patch Tuesday updates address vulnerabilities across various Microsoft products and services, including Windows, Microsoft Office, Microsoft Edge, and more. The vulnerabilities range from elevation of privilege, security feature bypass, remote code execution, information disclosure, denial of service, and spoofing.

The vulnerabilities which exploitation have been detected:

- `CVE-2023-32046` : Windows MSHTML Platform Elevation of Privilege Vulnerability;
- `CVE-2023-32049` : Windows SmartScreen Security Feature Bypass Vulnerability;
- `CVE-2023-36874` : Windows Error Reporting Service Elevation of Privilege Vulnerability;
- `CVE-2023-36884` : Office and Windows HTML Remote Code Execution Vulnerability;
- `CVE-2023-35311` : Microsoft Outlook Security Feature Bypass Vulnerability;
- `ADV230001` : Guidance on Microsoft Signed Drivers Being Used Maliciously.

We would like to point out that `CVE-2023-36884` is being used in recent phishing campaigns [3].

Affected Products

- Windows (multiple versions, services, drivers and etc.);
- Microsoft Office (SharePoint, Outlook, Access, Excel);
- .NET and Visual Studio;
- Windows Defender;
- Microsoft Dynamics;
- Microsoft Graphics Component;
- Microsoft Printer drivers;
- Paint 3D;
- Microsoft Windows Codecs Library;

- Microsoft Power Apps;
- Microsoft Graphics Component;
- Microsoft Dynamics;
- and others.

Please check Microsoft release note [1] to get a full list of affected products.

Recommendations

Microsoft urges users to apply the security updates as soon as possible to protect their systems against potential exploitation. Users should review the detailed advisory for each vulnerability and follow the steps provided to mitigate the risks associated with these vulnerabilities.

References

[1] https://msrc.microsoft.com/update-guide/releaseNote/2023-Jul

[2] https://www.tenable.com/blog/microsofts-july-2023-patch-tuesday-addresses-130-cves-cve-2023-36884

[3] https://www.microsoft.com/en-us/security/blog/2023/07/11/storm-0978-attacks-reveal-financial-and-espionage-motives/