Security Advisory 2023-064

Microsoft September 2023 Patch Tuesday

September 13, 2023 — v1.0

TLP:CLEAR

History:

- *13/09/2023 — v1.0 – Initial publication*

Summary

Microsoft has released its September 2023 Patch Tuesday Security Updates, addressing a total of 59 CVEs, including two actively exploited zero-day vulnerabilities [1].

Technical Details

This month's patches fix two zero-day vulnerabilities that are known to be actively exploited in the wild and one of them publicly disclosed. These zero-day vulnerabilities are:

- **CVE-2023-36802 - Microsoft Streaming Service Proxy Elevation of Privilege Vulnerability** [2];

Microsoft has fixed an actively exploited local privilege elevation vulnerability. An attacker who successfully exploited this vulnerability could gain SYSTEM privileges.

- **CVE-2023-36761 - Microsoft Word Information Disclosure Vulnerability** [3];

Microsoft has fixed an actively exploited vulnerability that can be used to steal NTLM hashes when opening a document, including the Preview Pane. An attacker could exploit this vulnerability to allow the disclosure of NTLM hashes, which could be used in an NTLM relay-style attack.

Affected Products

Here is the full list with Microsoft's affected products and their respective vulnerabilities in the September 2023 Patch Tuesday updates:

Tag	CVE	Base Score
Microsoft Azure Kubernetes Service	CVE-2023-29332	7.5
Azure DevOps	CVE-2023-33136	8.8
Windows Cloud Files Mini Filter Driver	CVE-2023-35355	7.8
Microsoft Identity Linux Broker	CVE-2023-36736	4.4
3D Viewer	CVE-2023-36739	7.8

Tag	CVE	Base Score
3D Viewer	CVE-2023-36740	7.8
Visual Studio Code	CVE-2023-36742	7.8
Microsoft Exchange Server	CVE-2023-36744	8.0
Microsoft Exchange Server	CVE-2023-36745	8.0
Microsoft Exchange Server	CVE-2023-36756	8.0
Microsoft Exchange Server	CVE-2023-36757	8.0
Visual Studio	CVE-2023-36758	7.8
Visual Studio	CVE-2023-36759	6.7
3D Viewer	CVE-2023-36760	7.8
Microsoft Office Word	CVE-2023-36761	6.2
Microsoft Office Word	CVE-2023-36762	7.3
Microsoft Office Outlook	CVE-2023-36763	7.5
Microsoft Office SharePoint	CVE-2023-36764	8.8
Microsoft Office	CVE-2023-36765	7.8
Microsoft Office Excel	CVE-2023-36766	7.8
Microsoft Office	CVE-2023-36767	4.3
3D Builder	CVE-2023-36770	7.8
3D Builder	CVE-2023-36771	7.8
3D Builder	CVE-2023-36772	7.8
3D Builder	CVE-2023-36773	7.8
Microsoft Exchange Server	CVE-2023-36777	5.7
.NET Framework	CVE-2023-36788	7.8
.NET and Visual Studio	CVE-2023-36792	7.8
.NET and Visual Studio	CVE-2023-36793	7.8
.NET and Visual Studio	CVE-2023-36794	7.8
.NET and Visual Studio	CVE-2023-36796	7.8
.NET Core & Visual Studio	CVE-2023-36799	6.5
Microsoft Dynamics Finance & Operations	CVE-2023-36800	7.6
Windows DHCP Server	CVE-2023-36801	5.3
Microsoft Streaming Service	CVE-2023-36802	7.8
Windows Kernel	CVE-2023-36803	5.5
Windows GDI	CVE-2023-36804	7.8
Windows Scripting	CVE-2023-36805	7.0
Microsoft Dynamics	CVE-2023-36886	7.6
Windows Kernel	CVE-2023-38139	7.8
Windows Kernel	CVE-2023-38140	5.5
Windows Kernel	CVE-2023-38141	7.8
Windows Kernel	CVE-2023-38142	7.8
Windows Common Log File System Driver	CVE-2023-38143	7.8
Windows Common Log File System Driver	CVE-2023-38144	7.8
Windows Themes	CVE-2023-38146	8.8
Microsoft Windows Codecs Library	CVE-2023-38147	8.8
Windows Internet Connection Sharing (ICS)	CVE-2023-38148	8.8
Windows TCP/IP	CVE-2023-38149	7.5
Windows Kernel	CVE-2023-38150	7.8
Windows DHCP Server	CVE-2023-38152	5.3
Azure DevOps	CVE-2023-38155	7.0
Azure HDInsights	CVE-2023-38156	7.2
Windows TCP/IP	CVE-2023-38160	5.5
Windows GDI	CVE-2023-38161	7.8
Windows DHCP Server	CVE-2023-38162	7.5
Windows Defender	CVE-2023-38163	7.8
Microsoft Dynamics	CVE-2023-38164	7.6
Microsoft Office	CVE-2023-41764	5.5

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 Microsoft 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-Sep

[2] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36802

[3] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36761