Security Advisory 2023-057

Microsoft August 2023 Patch Tuesday

August 9, 2023 — v1.0

TLP:CLEAR

History:

- *10/08/2023 — v1.0 – Initial publication*

Summary

Microsoft has released its August 2023 Patch Tuesday Security Updates, addressing a total of 74 Microsoft CVEs, including two actively exploited zero-day vulnerabilities, and six Critical vulnerabilities [1].

Technical Details

The August 2023 Patch Tuesday updates address vulnerabilities across various Microsoft products and range from elevation of privilege, security feature bypass, remote code execution, information disclosure, denial of service, and spoofing.

Zero-Day Vulnerabilities

This month's patches fix two zero-day vulnerabilities, of moderate severity, that are known to be actively exploited in the wild. These zero-day vulnerabilities are:

- ADV230003 - Microsoft Office Defense in Depth Update (publicly disclosed) [2]
- ADV230004 - Memory Integrity System Readiness Scan Tool Defense in Depth Update [3]

Critical Vulnerabilities

Additionally, 6 critical vulnerabilities are fixed in this month's security update:

- CVE-2023-36895: Microsoft Outlook Remote Code Execution Vulnerability
- CVE-2023-29328: Microsoft Teams Remote Code Execution Vulnerability
- CVE-2023-29330: Microsoft Teams Remote Code Execution Vulnerability
- CVE-2023-35385: Microsoft Message Queuing Remote Code Execution Vulnerability
- CVE-2023-36911: Microsoft Message Queuing Remote Code Execution Vulnerability
- CVE-2023-36910: Microsoft Message Queuing Remote Code Execution Vulnerability

Affected Products

Here is the full list with Microsoft's affected products, regardless of the severity of their vulnerability:

- Microsoft Office
- Memory Integrity System Readiness Scan Tool
- Microsoft Exchange Server
- Microsoft Teams
- Windows Kernel
- Windows Message Queuing
- Windows Projected File System
- Windows Reliability Analysis Metrics Calculation Engine
- Windows Fax and Scan Service
- Windows HTML Platform
- Windows Bluetooth A2DP driver
- Microsoft Dynamics
- .NET Core
- ASP.NET and Visual Studio
- Azure HDInsights
- Microsoft WDAC OLE DB provider for SQL
- Windows Group Policy
- Microsoft Office (Excel, Visio, Sharepoint, Outlook)
- Tablet Windows User Interface
- ASP.NET
- Windows Common Log File System Driver
- Windows System Assessment Tool
- Windows Cloud Files Mini Filter Driver
- Windows Wireless Wide Area Network Service
- Windows Cryptographic Services
- Role: Windows Hyper-V
- Microsoft Edge (Chromium-based)
- Dynamics Business Central Control
- SQL Server
- Microsoft Windows Codecs Library
- Windows Defender
- Azure Arc
- Microsoft Exchange Server
- Windows LDAP - Lightweight Directory Access Protocol
- Windows Mobile Device Management

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-Aug

[2] https://msrc.microsoft.com/update-guide/en-US/vulnerability/ADV230003

[3] https://msrc.microsoft.com/update-guide/en-US/vulnerability/ADV230004