CERT-EU

Security Advisory 2025-023

Critical Vulnerabilities in Microsoft Products

2025-07-09 — v1.0

TLP:CLEAR

History:

- *09/07/2025 — v1.0 – Initial publication*

Summary

On July 8, 2025, as part of the Microsoft's Patch Tuesday, Microsoft released security updates addressing 137 flaws, including one zero-day vulnerability and fourteen critical vulnerabilities [1].

It is recommended updating as soon as possible, prioritising public facing and critical assets.

Technical Details

The zero-day vulnerability **CVE-2025-49719**, with a CVSS score of 7.5, is due to improper input validation in SQL Server and allows a remote, unauthenticated attacker to access data from uninitialized memory. Microsoft also fixed one important and one critical severity vulnerabilities in SQL Server.

Microsoft fixed seven critical and eight high severity vulnerabilities in Microsoft Office, Microsoft Office Excel, Microsoft Office SharePoint, and Microsoft Office Words. These flaws are elevation of privilege, information disclosure, server spoofing, and remote code execution vulnerabilities.

Microsoft finally fixed four critical vulnerabilities in the Windows Hyper-V role, Windows Imaging Component, Windows KDC Proxy Service (KPSSVC), and in the Windows SPNEGO Extended Negotiation Mechanism.

Affected Products

Microsoft SQL Server, Microsoft Office, Microsoft Office Excel, Microsoft Office SharePoint, Microsoft Office Words and Microsoft Windows are affected by the vulnerabilities described above.

For the list of all products affected, refer to Microsoft's advisory [1].

Recommendations

It is recommended updating as soon as possible, prioritising public facing and critical assets.

References

[1] https://www.bleepingcomputer.com/microsoft-patch-tuesday-reports/Microsoft-Patch-Tuesday-July-2025.html