CERT-EU

Security Advisory 2023-028

Microsoft May 2023 Patch Tuesday

May 10, 2023 — v1.0

TLP:CLEAR

History:

- *10/05/2023 — v1.0 – Initial publication*

Summary

Microsoft has released its May 2023 Patch Tuesday security updates, addressing a total of 38 vulnerabilities, including three zero-day vulnerabilities, and six **Critical** vulnerabilities that allow remote code execution [1].

Technical Details

The May 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.

Three zero-day vulnerabilities have been fixed in this update:

- `CVE-2023-29336` : Win32k Elevation of Privilege Vulnerability
- `CVE-2023-24932` : Secure Boot Security Feature Bypass Vulnerability
- `CVE-2023-29325` : Windows OLE Remote Code Execution Vulnerability

The first two zero-days were already exploited in attacks, while the third one was publicly disclosed, but not actively exploited.

Affected Products

The May 2023 Patch Tuesday updates apply to various Microsoft products and services, including:

- Windows (multiple versions)
- Microsoft Office (various applications)
- Microsoft Edge (Chromium-based)
- Microsoft Graphics Component
- Microsoft Teams
- Microsoft Windows Codecs Library
- Remote Desktop Client
- SysInternals
- Visual Studio Code

- Windows Backup Engine
- Windows Installer
- Windows iSCSI Target Service
- Windows LDAP - Lightweight Directory Access Protocol
- Windows MSHTML Platform
- Windows Network File System
- Windows NFS Portmapper
- Windows NTLM
- Windows OLE
- Windows PGM
- Windows RDP Client
- Windows Remote Procedure Call Runtime
- Windows Secure Boot
- Windows Secure Socket Tunneling Protocol (SSTP)
- Windows SMB
- Windows Win32K

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-May