NATIONAL CSIRT-CY

CVE-2025-0628

17/01/2026

Microsoft January 2026 Patch

Executive Summary

This Tuesday on the 13th of month Microsoft released its latest Patch KB5074109.

This patch addresses and fixes **114** CVEs. 3 of those are Zero-Days

Out of the 114 identified flaws, eight are classified as **Critical**, while the remaining 106 are considered **Important** in terms of severity. A total of 58 vulnerabilities involve privilege escalation, making it the most common category, followed by 22 related to information disclosure, 21 to remote code execution, and five to spoofing.

In addition, we remind that In November 2025, Microsoft announced the expiration of 3 Windows Secure Boot certificates from 2011, expiring in June 2026, urging customers to update to their 2023 counterparts:

Microsoft Corporation KEK CA 2011 (June 2026) - Microsoft Corporation KEK 2K CA 2023 (for signing updates to DB and DBX)

Microsoft Windows Production PCA 2011 (October 2026) - Windows UEFI CA 2023 (for signing the Windows boot loader)

Microsoft UEFI CA 2011 (June 2026) - Microsoft UEFI CA 2023 (for signing third-party boot loaders) and Microsoft Option ROM UEFI CA 2023 (for signing third-party option ROMs)

Notable CVE's that are addressed

- CVE-2026-0628: Chromium vulnerability
- CVE-2026-20805: Desktop Window Manager
- CVE-2025-21265: Affecting secure boot certificate expiration.
- CVE-2026-20876: Windows Virtualization-Based Security (VBS) privilege escalation vulnerability

Solution

Apply the latest patch from Microsoft in all your systems.

Common Weakness Enumeration

http://cwe.mitre.org/data/definitions/862.html

Common Vulnerabilities & Exposures

https://nvd.nist.gov/vuln/detail/CVE-2026-0628

Please distribute this information among your subsidiaries and partners, and also share with us any pertinent information and findings you may have (e.g IOCs, TTPs etc)

The Digital Security Authority extends its appreciation for the continued collaboration.

Disclaimer

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments