MULTIPLE SEVERE VULNERABILITIES IN MICROSOFT WINDOWS

Vairav CVE Report

Date: March 12th, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148
Baluwatar, Kathmandu

Phone: +977 4541540
Mobile: +977-9820105900
Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Multiple severe vulnerabilities, including CVE-2025-24035, CVE-2025-24045, CVE-2025-24983, CVE-2025-24984, CVE-2025-24985, CVE-2025-24991, CVE-2025-24993, CVE-2025-26633, and CVE-2025-26630, have been identified in Microsoft Windows components. The most severe vulnerabilities allow remote code execution (RCE) and elevation of privilege (EoP), with CVSS scores up to 8.1. If exploited, these vulnerabilities could lead to system compromise, data exposure, and privilege escalation.

VULNERABILITY DETAILS

CVE-2025-24035

- **Description**: Sensitive data storage in improperly locked memory in Windows Remote Desktop Services allows an unauthorized attacker to execute code over a network.
- **Impact**: Successful exploitation allows arbitrary code execution.
- **CVSS Score**: 8.1 (Critical)

CVE-2025-24045

- **Description**: A remote code execution vulnerability in Windows Remote Desktop Services due to a race condition. An attacker who can successfully exploit this vulnerability could execute arbitrary code on the affected system.
- **Impact**: Execution of arbitrary code, potentially leading to full system compromise.
- **CVSS Score**: 8.1 (Critical)

CVE-2025-24983

- **Description**: A use-after-free vulnerability in the Windows Win32 Kernel Subsystem that allows an authenticated attacker to escalate privileges to SYSTEM level.
- **Impact**: Successful exploitation grants the attacker full control over the affected system.
- **CVSS Score**: 7.0 (High)

CVE-2025-24984

- **Description**: An information disclosure vulnerability in the Windows NTFS file system that could allow an attacker with physical access to read portions of heap memory by inserting a malicious USB device.
- **Impact**: Exposure of sensitive memory data, potentially aiding further attacks.
- **CVSS Score**: 4.6 (Medium)

CVE-2025-24985

- **Description**: An integer overflow in the Windows Fast FAT File System Driver that could let an attacker execute remote code if a local user mounts a maliciously crafted Virtual Hard Disk (VHD).
- **Impact**: Execution of arbitrary code on the affected system.
- **CVSS Score**: 7.8 (High)

CVE-2025-24991

- **Description**: An information disclosure vulnerability resulting from improper logging of sensitive data in Windows NTFS, which may allow local attackers to access portions of heap memory.
- **Impact**: Exposure of sensitive memory data, potentially aiding privilege escalation.
- **CVSS Score**: 5.5 (Medium)

CVE-2025-24993

- **Description**: A heap-based buffer overflow in Windows NTFS that could let an attacker execute code locally by enticing a user to mount a specially crafted VHD file.
- **Impact**: Execution of arbitrary code on the affected system.
- **CVSS Score**: 7.8 (High)

CVE-2025-26633

- **Description**: A security feature bypass vulnerability in Microsoft Management Console (MMC) due to improper neutralization, allowing an attacker to bypass security features.
- **Impact**: Potential to bypass security restrictions, leading to unauthorized actions.
- **CVSS Score**: 7.0 (High)

CVE-2025-26630

- **Description**: A use-after-free flaw in Microsoft Access that could allow an attacker to execute arbitrary code by tricking a victim into opening a malicious file.
- **Impact**: Execution of arbitrary code on the affected system.
- **CVSS Score**: 7.8 (High)

AFFECTED VERSIONS

- Windows 10 versions prior to update 21H2
- Windows Server versions prior to update 2019
- Microsoft Access versions prior to 2025

EXPLOIT DETAILS

These vulnerabilities are particularly concerning in environments where users interact with external storage devices or mount VHD files. Exploitation could lead to full system compromise, data exposure, and privilege escalation. Notably, CVE-2025-24985 and CVE-2025-24993 have been exploited in the wild as zero-day vulnerabilities.

RECOMMENDED ACTIONS

Microsoft has released patches addressing these vulnerabilities as part of the March 2025 Patch Tuesday updates. Administrators and users are advised to apply these updates promptly to mitigate potential risks.

ADDITIONAL SECURITY MEASURES

- **Restrict Physical Access**: Limit physical access to systems to trusted personnel to reduce the risk of exploitation of vulnerabilities like CVE-2025-24984.
- **User Training**: Educate users about the dangers of opening files from untrusted sources, particularly in relation to vulnerabilities like CVE-2025-26630.
- **Network Segmentation**: Implement network segmentation to limit the potential impact of compromised systems, especially concerning vulnerabilities in Remote Desktop Services.

REFERENCES

- https://www.bleepingcomputer.com/news/microsoft/microsoft-march-2025-patch-tuesday-fixes-7-zero-days-57-flaws/
- https://www.tenable.com/blog/microsofts-march-2025-patch-tuesday-addresses-56-cves-cve-2025-26633-cve-2025-24983
- https://securityonline.info/microsoft-patch-tuesday-march-2025-addresses-67-vulnerabilities-including-seven-zero-day-flaws/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com