Microsoft Patches Six Zero-Day Vulnerabilities

Overview

This week, Microsoft released security updates addressing 57 vulnerabilities across its products, including six zero-day flaws currently under active exploitation. These vulnerabilities affect Windows NTFS, the Win32 Kernel Subsystem, the Microsoft Management Console, and the Fast FAT File System Driver. Successful exploitation could allow attackers to execute arbitrary code, escalate privileges, or disclose sensitive information.

Zero-Day Vulnerabilities Breakdown

- **CVE-2025-24991 (CVSS 5.5) – Windows NTFS Information Disclosure Vulnerability**
  - Attackers can trick users into mounting a malicious virtual hard disk (VHD) file to leak memory contents.
  - Could expose sensitive information, aiding in further exploitation.
- **CVE-2025-24993 (CVSS 7.8) – Windows NTFS Remote Code Execution Vulnerability**
  - A heap-based buffer overflow in NTFS allows remote code execution (RCE).
  - Exploitation requires tricking users into mounting a specially crafted VHD.
- **CVE-2025-24983 (CVSS 7.0) – Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability**
  - Exploited in the wild via the PipeMagic backdoor.
  - Allows attackers to escalate privileges to SYSTEM-level access.
  - Affects older Windows versions but is also present in Windows 10 (build 1809) and Windows Server 2016.
- **CVE-2025-24984 (CVSS 4.6)– Windows NTFS Information Disclosure Vulnerability**
  - Attackers with physical access can exploit this flaw by inserting a malicious USB drive.
  - Allows for memory leak, potentially exposing credentials or other sensitive data.

- **CVE-2025-24985 (CVSS 7.8)– Windows Fast FAT File System Driver Remote Code Execution Vulnerability**
    - Exploitation requires a user to mount a malicious VHD file.
    - Attackers can execute arbitrary code, leading to full system compromise.
    - Similar techniques have been used in phishing and pirated software distribution.
- **CVE-2025-26633 (CVSS 7.0) – Microsoft Management Console Security Feature Bypass Vulnerability**
    - Requires user interaction, such as opening a malicious .msc file.
    - Could allow attackers to bypass security measures and execute unauthorized commands.
    - Typically used in phishing and social engineering attacks.

Affected Products

- Windows 8.1, Server 2012 R2 (No longer supported but still targeted)
- Windows 10 (build 1809), Windows Server 2016
- Windows 11 and Server 2019 (Not listed as vulnerable)

If left unpatched, the six zero-days could help attackers steal sensitive data from memory, install malware, disable security features, and deploy ransomware. An organization's encryption keys and credentials could also be exposed. Since these vulnerabilities are already under active exploitation, Aspire recommends patching immediately.

Aspire Protects

- **Patch** – Update Windows systems immediately. Find patch guidance in the links below:
    - CVE-2025-24991
    - CVE-2025-24993
    - CVE-2025-24893
    - CVE-2025-24894
    - CVE-2025-24895
    - CVE-2025-26633
- Disable USB ports where possible to reduce exposure to CVE-2025-24984.

- Restrict the ability to mount VHD files to prevent exploitation of CVE-2025-24991, CVE-2025-24993, and CVE-2025-24985.
- Warn employees against opening unknown **.msc** files or mounting unfamiliar VHD images.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – Attackers may exploit public-facing NTFS flaws.

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – Elevation of privilege exploits like CVE-2025-24983.

Execution

- User Execution [T1204] – Users tricked into executing malicious VHD or .msc files.

Credential Access

- OS Credential Dumping [T1003] – Memory leaks exposing sensitive credentials.

Persistence

- Boot or Logon Autostart Execution [T1547] – Attackers may establish persistence post-exploitation.

IoCs

- Execution of malicious **.msc** files
- Presence of the PipeMagic backdoor

There are no other known IoCs associated with the above vulnerabilities at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

The vulnerability may impact the following industries/sectors:

- Finance
- Ecommerce
- Healthcare
- Government

- Manufacturing
- Retail
- Energy
- Education
- Telecommunications
- And others

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

CVE-2025-24991 - Security Update Guide - Microsoft - Windows NTFS Information Disclosure Vulnerability

CVE-2025-24993 - Security Update Guide - Microsoft - Windows NTFS Remote Code Execution Vulnerability

CVE-2025-24983 - Security Update Guide - Microsoft - Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability

CVE-2025-24984 - Security Update Guide - Microsoft - Windows NTFS Information Disclosure Vulnerability

CVE-2025-24985 - Security Update Guide - Microsoft - Windows Fast FAT File System Driver Remote Code Execution Vulnerability

CVE-2025-26633 - Security Update Guide - Microsoft - Microsoft Management Console Security Feature Bypass Vulnerability