Patch, Exploit, Repeat: A Never-Ending Cycle for Windows Common Log File System Driver Vulnerabilities

Operating system components are often the most attractive targets for attackers, and securing them is fundamental to system defense. One such component, the Windows Common Log File System (CLFS) driver, plays a critical role in the Windows operating system for log file management for both user-mode and kernel-mode applications. Given its elevated access and widespread usage, it has been frequently exploited by threat actors (especially ransomware operators) over the past years, making its timely patching a top priority.

Looking at the past few months, multiple high-severity vulnerabilities have been discovered in the CLFS driver since 2024 (many of which have also been actively exploited). These vulnerabilities often allow for elevation of privilege, enabling attackers to gain SYSTEM-level access and execute arbitrary code.

Microsoft has responded by releasing a series of critical patches during its monthly Patch Tuesday updates, and here is a review of the addressed vulnerabilities since 2024, highlighting how these vulnerabilities were exploited by threat actors.

Image source: SOCRadar.io

Storm-2460:
identified by Microsoft as the group being the RansomEXX ransomware operator, is a highly advanced threat actor that exploits zero-day vulnerabilities like CVE-2025-29824 to deploy ransomware and execute double-extortion attacks across global sectors.

Aliases: RansomEXX, RansomEXX2, Defray777, Defray DarkSide

Country: Worldwide

IOCs:

131.188.40[.]189

199.58.81[.]140

In December 2024, Microsoft addressed CVE-2024-49138 (CVSS 7.8), a heap-Based Buffer Overflow vulnerability exploited in-the-wild prior to its patching. This vulnerability stemmed from improper handling of log files within the CLFS driver, and was successfully exploited by attackers to elevate their privileges on the target host to SYSTEM. A similar Elevation of Privilege (EoP) vulnerability was fixed a few months later during March 2025 Patch Tuesday (CVE-2025-24059, CVSS 7.8), which could lead to arbitrary code execution (even though there were no signs of active exploitation). Later in April 2025, Microsoft fixed CVE-2025-29824 (CVSS 7.8), a "Use After Free" vulnerability allowing an attacker to manipulate the memory state.

As reported by Microsoft Threat Intelligence Center and Microsoft Security Response Center, the exploit campaign (attributed to the threat actor Storm-2460) targeted organizations across diverse sectors, including IT and real estate in the U.S.A., finance in Venezuela, retail in Saudi Arabia, and a Spanish software company. The attackers used the PipeMagic malware, deployed via malicious MSBuild scripts, to load the exploit in memory.

In a separate incident involving CVE-2025-29824, attackers linked to the Play Ransomware operation (also known as Balloonfly) exploited the Windows CLFS vulnerability before it was patched in April 2025. The attack targeted a U.S. company and, while no ransomware was deployed, the attackers leveraged the vulnerability to install the Grixba infostealer, a custom tool associated with Balloonfly.

Image source: SOCRadar.io

Play Ransomware:
also known as Balloonfly, is a sophisticated ransomware group active since June 2022, targeting organizations globally, including critical infrastructure, government, and various industries.
Aliases: Balloonfly, PlayCrypt
Country: Worldwide
IOCs:

- 72.5.161[.]12,
- 68.183.105[.]34,
- 9c70f766d3b84fc2bb298efa37cc9191f28bec336329cc11468cfadbc3b137f4
- 0f1bad70c7bd1e0a69562853ec529355462fcd0423263a3d39d6d0d70b780443

.And lastly, during May 2025 Patch Tuesday, CVE-2025-32701 and CVE-2025-32706 (CVSS 7.8) were addressed. Both CVEs are still EoP vulnerabilities in the CLFS driver whose exploitation has been detected, and improper input validation allows an authorized attacker to elevate privileges locally to gain SYSTEM. In the same Patch Tuesday, another CLFS Driver vulnerability was fixed (CVE-2025-30385, CVSS 7.8), but has been assessed by Microsoft as "Exploitation More Likely".

All abovementioned incidents highlight how multiple threat actors were likely in possession of the exploits prior to their public disclosure. This reinforces the critical importance of patching zero-day vulnerabilities immediately upon release, especially for CLFS vulnerabilities, which can allow for local privilege escalation, and therefore are valuable to ransomware groups in the post-compromise phase. Another suggestion is to monitor for indicators, such as abnormal executables behavior, creation of log files in suspicious locations, and connections to known ransomware infrastructure indicating exploitation attempts.

Do you have any questions? Don't hesitate to contact the team (info@basevision.ch) and check out our service: Extended Threat Intelligence & Hunting Service