SignDrop proof of concept claims SYSTEM access through Windows CLFS driver



Public exploit code called SignDrop claims a local Windows user can reach SYSTEM privileges through the Common Log File System driver. Source details are limited, so treat it as a local privilege escalation risk.

- Public proof-of-concept code named SignDrop was released earlier this week.
- It claims a local Windows user can obtain SYSTEM privileges via the Common Log File System driver.
- It targets a log-authentication feature added to the driver last year.
- The technique abuses how clfs.sys creates companion files when a privileged process opens a prepared log, using path redirection.
- The source excerpt gives no CVE number or patch status.

Public exploit code named SignDrop was released earlier this week. It claims that a local Windows user can gain SYSTEM privileges through the Common Log File System (CLFS) driver.

What the source describes

The proof of concept targets a log-authentication feature added to the driver last year. According to the report, it abuses the way clfs.sys creates companion files when a privileged process opens a prepared log. By using path redirection, the exploit is said to take control of the outcome and reach SYSTEM.

The source excerpt available to us does not provide a CVE identifier, affected version list, patch status or evidence of exploitation in the wild. We have not filled those gaps, and readers should confirm them with Microsoft's official guidance.

Why it matters

This is a local privilege escalation issue, so an attacker would first need a foothold on a Windows system. The practical risk is that a low-privileged account, such as one obtained through phishing or stolen credentials, could be elevated to full control of the machine. Public proof-of-concept code generally shortens the time before others adapt it.

Recommended stance

No action is needed to stop an outside attack on its own, but institutions should prepare. Watch for vendor advisories, confirm that endpoint detection covers privilege escalation behaviour, and limit who can log on to servers and sensitive workstations.

What to do now

1. Monitor Microsoft security advisories for a CVE and update covering CLFS, and schedule the patch once available.
2. Ask your EDR provider whether detections cover CLFS-based privilege escalation and public PoC behaviour.
3. Restrict interactive and remote logon rights on servers and sensitive workstations to those who need them.
4. Review alerts for unusual file creation or path redirection by privileged processes on Windows hosts.
5. Record the issue in your vulnerability register and set a target remediation date under your patch management process.