Windows 0-day dropped by disgruntled researcher hands hackers System rights

The researcher continued:

> *What makes it funnier is the fact that it can be used against any antimalware engine to bypass their self defense (or tamper protection) mechanism as you can trigger arbitrary file creation in the context of their own antimalware process so from the perspective of their kernel drivers, the file creation request is coming from their own legit process so it passes, this makes this vulnerability unique as it can be used to turn off any antivirus/EDR.*

Nightmare Eclipse said the exploit worked against Windows 11 26H2, Windows 11 26H2 Experimental, and Windows Server 2025 Experimental. People can see if their systems are vulnerable by checking the CLFS authentication mode. If it's in learning mode or enforcement mode, the system is vulnerable, and the PoC supplied in the post should spawn a SYSTEM shell. Nightmare Eclipse has published numerous other Windows zero-days in recent months.

Researcher Will Dormann said in an interview that he has been able to reproduce the exploit and that it works as described, but not on all versions of Windows 11. But there's a catch, he said.

"The requirements are important in that it seems to require Windows 26H2, and one that has existed for more than 90 days, it seems," he explained. "That is, you can't just take a new

26H2 system and install updates and have it work.”

For a system to be vulnerable, Dormann said, the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CLFS\Authentication\Mode
value must be 0 or 1.” Of the many machines Dormann uses, only a single one met this requirement.

Microsoft does staged rollouts of Windows updates, such as 26H2, so it’s not clear how many people have it. You can check by running the “winver” command. Microsoft representatives didn’t respond to an email seeking comment.

https://arstechnica.com/security/2026/11/windows-0-day-dropped-by-disgruntled-researcher-hands-hackers-system-rights/