2025-07-02 16:41:11

The summary for this set of articles is as follows:

1. Microsoft released a large number of patches addressing 70 vulnerabilities, including five zero-day flaws that are already being actively exploited by attackers. Two of these zero-days affect the Windows Common Log File System (CLFS) driver and can be used to elevate privileges on vulnerable devices.

2. Microsoft also patched two other zero-days related to privilege escalation: one in the Ancillary Function Driver (afd.sys) and another in the Desktop Window Manager (DWM).

3. Another zero-day patched by Microsoft was a flaw in the Microsoft Scripting Engine, which is used by Internet Explorer and Internet Explorer mode in Microsoft Edge.

4. The summary also includes an article about a civil lawsuit where a cybercriminal named Conor Brian Fitzpatrick, known as "Pompompurin," agreed to pay $700,000 in connection with a data breach at a healthcare company he had exploited through his role as the administrator of the popular hacking forum BreachForums.

5. Lastly, there is an article about the Russian cyber espionage group APT29 (also known as Cozy Bear) being connected to the malware backdoor "Reductor" that has infected at least 14 IT companies worldwide since 2018. The malware is believed to be used for intelligence gathering and industrial espionage.