Four groups caught using the same Chrome and Windows exploit kit

A nearly identical exploit kit that targets critical vulnerabilities in both Chromium-based browsers and older versions of Windows is being actively used by at least four hacking groups, some of which have ties to the Chinese government.

Researchers from security firm Proofpoint said Wednesday that BlueMoon, the name they gave to the kit, chains three vulnerabilities together so the attackers using it can install malware of their choice. BlueMoon exploits two Chromium vulnerabilities and one in the kernel of Windows 10 (Oct. 2018 Update), Windows Server 2019, Windows 10 2004, Windows Server 2022, and the initial release of Windows 11. All three vulnerabilities have received patches in the past 24 hours.

Deployed rapidly, widely shared

The attacks lacked the stealth found in many campaigns. More often, hackers want to exploit newly discovered vulnerabilities sparingly to lengthen their longevity. Proofpoint hypothesized that one reason for the widely used and visible exploit chain was to take advantage of a “patch gap” in the Chromium supply chain, which spans the time a patch is available from developers and the time that patch is incorporated into browsers such as Chrome and Edge. Another likely contributor was the use of AI, which can often spot vulnerabilities faster than discovery performed solely by humans.

Read full article

Comments

https://arstechnica.com/information-technology/2026/09/4-groups-caught-using-the-same-chrome-and-windows-exploit-kit/