

Forum:[Hack Forums](#)

Thread: [BlueHammer Vulnerability Exploited in Ransomware Attacks](#)

MadScientist - June 30, 2026, 3:19 pm

A Microsoft Defender vulnerability tracked as BlueHammer and CVE-2026-33825 is being exploited in ransomware attacks, according to the cybersecurity agency CISA.

BlueHammer is one of the several exploits disclosed in recent months by a disgruntled researcher known as Chaotic Eclipse and Nightmare Eclipse. The researcher is unhappy with Microsoft's handling of vulnerability reports, which is why several exploits were made public before the tech giant had a chance to release fixes.

CVE-2026-33825 was publicly disclosed on April 2 and Microsoft released patches on April 14, when it informed customers that an authenticated attacker can exploit the security hole for privilege escalation.

While Microsoft's advisory — last updated on April 30 — admits that exploitation of the flaw is 'more likely', it still does not confirm in-the-wild exploitation.

Cybersecurity firm Huntress saw the vulnerability being exploited in attacks as a zero-day before Microsoft released patches.

CISA added BlueHammer to its Known Exploited Vulnerabilities (KEV) catalog on April 22 and the agency has now updated the entry to specify that the weakness has been leveraged in ransomware campaigns.

It's unclear which ransomware group has exploited CVE-2026-33825; there do not appear to be any recent reports describing its exploitation.

CISA does not notify users when a vulnerability included in its KEV list starts being exploited by ransomware groups, which has raised questions regarding the practical utility of these updates for defenders.

Source - <https://www.securityweek.com/bluehammer-vulnerability-exploited-in-ransomware-attacks/>