Divulgation sauvage : quand un chercheur frustré arme l'attaquant

2 mai 2026 • Mis à jour le 17 mai 2026 • 8 min de lecture • 1243 mots • 230 vues • ♥

La divulgation sauvage de trois 0-days Defender en avril 2026 par un chercheur frustré n'est pas un accident. C'est le symptôme d'un contrat social qui s'effrite entre éditeurs et chercheurs sécurité — analyse et conséquences opérationnelles.

Un seul chercheur a publié trois zero-days Microsoft Defender en moins d'un mois. L'industrie a observé l'exploitation in-the-wild dans les 72 heures. C'est un signal qu'on a tort de minimiser : la responsible disclosure, en tant que contrat social, est en train de s'effriter.

L'affaire Chaotic Eclipse, en deux temps

Le 2 avril 2026, un chercheur connu sous les pseudonymes Chaotic Eclipse et Nightmare-Eclipse publie sur GitHub un PoC fonctionnel pour BlueHammer (CVE-2026-33825), une race condition TOCTOU dans Microsoft Defender qui permet à un compte standard d'escalader à SYSTEM. Pas de coordination préalable avec le MSRC, pas de fenêtre d'embargo, le code est accompagné d'une notice expliquant que l'auteur publie par frustration face à la gestion antérieure de ses rapports par Microsoft.

Microsoft réagit dans le Patch Tuesday du 14 avril en intégrant le correctif. Entre les deux dates, douze jours pendant lesquels le PoC tourne dans la nature. CISA confirme une exploitation in-the-wild observée dès le 10 avril. Le 17 avril, le même chercheur double la mise en publiant deux nouveaux 0-days Defender — RedSun et UnDefend — qui restent non corrigés à ce jour.

L'affaire n'est pas anecdotique. Elle fait écho à plusieurs épisodes récents : la divulgation sauvage des bugs Microsoft Print Spooler en 2021, les détails techniques publiés par des chercheurs Trend Micro après des désaccords avec ZDI, ou la frustration documentée de plusieurs chercheurs autour de la gestion des bounties Apple. Ce sont des incidents discrets mais récurrents, qui dessinent une tendance.