



# Patch Tuesday est mort : 28% des CVE exploités en moins de 24h

📅 10 mai 2026 • 🔄 Mis à jour le 17 mai 2026 • ⌚ 9 min de lecture • ☰ 1250 mots  
• 👁 97 vues • ❤

M-Trends 2026 : 28% des CVE publiées en 2025 ont été exploitées en moins de 24h. Le cycle Patch Tuesday hérité des années 2000 ne tient plus. Sortie du piège mensuel.



Le rapport M-Trends 2026 publié par Mandiant met un chiffre sur ce qu'on sentait depuis deux ans : 28,3 pour cent des CVE publiées en 2025 ont été exploitées dans les 24 heures suivant leur disclosure. Le Patch Tuesday mensuel hérité des années 2000 ne tient plus la route. Il faut revoir entièrement le pipeline de remédiation.

---

## Le chiffre qui change tout

---

Rappelons rapidement ce qu'est le Patch Tuesday : Microsoft a institué en 2003 le second mardi de chaque mois comme rendez-vous unique pour publier les correctifs Windows et Office. L'idée tenait debout à l'époque : fenêtre prévisible, cycle de validation interne d'un mois côté entreprise, communication groupée. Vingt ans plus tard, l'industrie entière fonctionne encore sur ce rythme : Adobe, Oracle, SAP, et même la majorité des éditeurs Linux d'entreprise alignent leurs releases sur cette cadence ou sur des cycles trimestriels.

Le problème : les attaquants, eux, n'ont jamais signé ce contrat tacite. Mandiant relève dans M-Trends 2026 que 28,3 pour cent des CVE publiées en 2025 ont vu une tentative d'exploitation dans les 24 heures suivant leur disclosure publique. Ce chiffre était à 12 pour cent en 2022, et à 4 pour cent en 2018. La courbe est exponentielle et le facteur d'accélération est connu : automatisation poussée du fingerprinting Internet par les frameworks comme Shodan, Censys et Cybertan, mais surtout entraînement de modèles d'IA spécialisés sur la lecture des advisories pour générer du code d'exploitation en quelques minutes.

Concrètement, sur 100 CVE publiées un lundi soir, environ 28 sont exploitées avant le mardi midi. Si vous attendez le Patch Tuesday du mois suivant pour patcher, vous laissez aux attaquants une fenêtre de quatre à six semaines sur des vulnérabilités déjà armées. Ce délai

---