

AI-found PHP bugs trigger an NSA alert as vulnerability volume outpaces patching; Legora and Blacksmith raise big rounds

VC Tech Radar

2026-10-22

AI-found PHP bugs trigger an NSA alert as vulnerability volume outpaces patching; Legora and Blacksmith raise big rounds

By VC Tech Radar • October 22, 2026

AI-assisted vulnerability discovery reached core web infrastructure, and investors argued remediation capacity is now the bottleneck. Capital went to legal agents, CI infrastructure and defense tech, and Mirendil reported cheap pretraining results that have not yet been independently checked.

Cyber: AI-found bugs have reached core web infrastructure

This period put real events behind the “vulnerpocalypse” thesis from earlier briefs. Wiz disclosed PHP2Shell, two critical bugs in the PHP engine that allow unauthenticated remote code execution and memory disclosure. The bugs had sat in the codebase for over a decade. According to the post relaying the disclosure, Wiz researchers used Gemini and GPT models to find them and build working exploits in about a week, which might previously have taken a team of top researchers months [1]. The same poster says four large organizations they work with took all their PHP sites offline to patch [1].

The NSA told every organization running PHP to prepare for an immediate update. If they can’t patch right away, it advised taking systems offline until the issue is mitigated [2]. The NSA notice itself doesn’t say how the bugs were found. Other disclosures landed the same day: - **GitLab**: a CVSS 10.0 flaw covering 12 years of releases, which allows unauthenticated RCE on self-managed servers [3]. - **Microsoft**: China-aligned Storm-0940 used an agentic AI pen-testing framework, ARTEX, to automate attacks on hundreds of organizations. Microsoft also ties the group to the ConnectWise supply-chain compromise [4].

Sarah Guo’s thesis gives investors the numbers: - **Intake:** CVEs went from about 4k a month to about 15k since April [5]. - **Fix rates:** HackerOne customers halved their fix times over two years, yet their backlog still grew 131% [6]. - **Patch volume:** Oracle’s quarterly patch release went from 374 fixes to 1,283. Guo says the bottleneck is hand-run regression testing done by 2024-era teams [7]. - **Her ask:** most new CVEs aren’t exploited yet, but that window closes once someone points a frontier model at the backlog. She wants a large reallocation of resources to cyber this year, “not 10%” [8].

Sam Altman went further. He no longer thinks “we’re going to be able to just patch all the bugs” and expects defense to move to AI-based approaches. He said he is astonished at how little attention the issue gets [9]. He tied any open release of OpenAI’s best internal model to a change in “the total cyber defense model of the way the internet works” [9].

At an All-In panel, one speaker estimated that 60–80% of vulnerabilities flagged by Mythos-class models are real and about 20% are hallucinated, so every finding still needs testing before a patch [10]. That points to diligence questions on verification and automated regression testing, not only on discovery.

Where capital went

- **Legora (YC W24)** raised a \$550M Series E at an \$8.8B valuation. It reports going from \$1M to \$100M ARR in under 18 months, then adding the next \$100M in under six. The US is now its largest market, and more than half of the AmLaw 50 are customers [11]. Bessemer led its \$1.8B round only last brief, so the valuation step-up is steep.
- **Blacksmith (YC W24)** raised a \$66M Series C at \$1B, led by Sequoia. CI jobs grew from 5M a week in January to more than 90M, and 10,000+ companies use it. YC’s framing: validating code, not writing it, is now the bottleneck [12]. This fits the verification theme above.
- **Watchtower Labs:** Conviction and Shield Capital co-led a \$35M seed. It builds a digital twin for military planning that sits alongside tools like Palantir [13]. Simulation runs on deterministic models, and LLMs only translate planners’ questions into inputs [13]. It holds a January 2026 Defense Innovation Unit prototype contract for logistics forecasting and has moved into mission planning [13]. CEO Akhil Iyer is a former Marine special operations team commander who later worked at Anduril [13].
- **Andrenam:** Mark Suster led its round after losing an earlier round to First Round [14]. His thesis is undersea defense: subsea cables are under threat, and cheap unmanned vehicles put seabed infrastructure “within reach of anyone” [15].
- **Stepful (YC S21)** raised a \$55M Series C for healthcare workforce training. It trained 30,000 students last year and works with seven of the 10 largest US health systems [16].
- **Doug Leone** made his first investment since returning as an active investor at Sequoia: Whop [17].

- **MVP Ventures** is reportedly raising a \$100M opportunities fund to add to its best positions. These include small early stakes in Anduril, Erebor, Stoke Space and Wispr Flow [18].

Cheaper ways to build models

Mirendil says one researcher built its first from-scratch pretrained coding model in 3.5 months with under \$10M of compute, including all experiments. It says the model is in the 100B–500B parameter range and that the recipe holds for larger versions [19]. Independent evaluations and API access are still to come [19], so treat this as a claim for now. If it holds, it weakens the assumption that frontier pretraining needs a large team.

Other efficiency signals: - **JOLT (Perplexity and NVIDIA)**: a self-distillation-plus-RL post-training method. It reportedly matches GRPO on MATH with 6.5x fewer training tokens [20]. - **Shift-1 (Applied Compute)**: a coding router that the company says cuts coding-agent cost by up to 55% with no noticeable quality drop [21]. - **Nemotron 3.5 Parse (NVIDIA)**: under 1B parameters, it took first place on LlamaIndex’s ParseBench against 150+ models [22]. - **LangChain**: Harrison Chase argues logged agent traces are training data, and a 9B model tuned on exactly your task can beat frontier models [23].

Open-weight economics. An All-In panelist estimated a self-hosted open model could cost \$1–2 per million tokens and do about 95% of the work [10]. He forecast that 75–90% of token usage will go to open-weight models [10]. Andrew Ng separately alleged that companies with large proprietary-model investments have lobbied to restrict open models [24].

DeepInfer update. vLLM reports decode throughput within 6% of DeepSeek’s published results under a matched setup [25]. DeepSeek’s own production figures are unaudited, and its KV-cache and load-balancing layers are not fully released [25].

Compute and hardware

Gimlet’s founder argues specialized inference chips are coming back. He cites a Goldman projection of 24x token demand against about 2x more power from 2026 to 2030 [26]. He also points to NVIDIA running inference across GPUs and Groq-derived LPUs together [26]. He says splitting workloads across different chips delivers 2–10x faster performance in the same power envelope, and that physical-infrastructure complexity may be a more durable moat than software [26]. He is talking his own book. Altman, meanwhile, called OpenAI’s own chip “the most important single thing” in its compute bets [27].

Briefly

- **Quantum:** IBM's Arvind Krishna (an All-In panelist) put a cryptography-breaking quantum computer between 2028 and 2033, with 2030 as the midpoint. He said DARPA's QBI benchmarking program has narrowed from a couple hundred companies to about 13, and that post-quantum migration should start now [10].
 - **Anthropic binders:** Anthropic and Citrini report 17 binders from 211 tested scorpion-toxin protein designs. None bound multiple toxins or was tested for neutralization, so this is not an antivenom [25].
 - **OpenAI and Anthropic finances (reported):** OpenAI is reportedly seeking about \$30B at a \$1.4T+ valuation. A reported review of Anthropic's draft prospectus cites \$16.3B in first-half revenue and more than \$600B in future compute commitments. Neither is verified [25].
-

Sources

1. r/artificial post by u/Haunting_Ganache_850
2. X post by @NSACyber
3. X post by @TheHackersNews
4. X post by @MsftSecIntel
5. X post by @saranormous
6. X post by @saranormous
7. X post by @saranormous
8. X post by @saranormous
9. Sam Altman, Co-Founder and CEO of OpenAI: Staying Human While Scaling Superintelligence
10. Arvind Krishna & Nikesh Arora: Quantum Threat, Open vs Frontier AI, AI Cyber Warfare & SaaS Collapse
11. X post by @ycombinator
12. X post by @ycombinator
13. X article by @saranormous
14. X post by @msuster
15. X post by @msuster
16. X post by @ycombinator
17. X post by @doug Leone
18. Anduril Investor MVP Ventures Eyes \$100 Million Opportunities Fund
19. X post by @bneyshabur
20. X post by @AravSrinivas
21. X post by @appliedcompute
22. X post by @jerryjliu0
23. X post by @hwchase17
24. Andrew Ng Podcast: Is AI fearmongering a funding stunt?
25. [AI News] DeepSeek DeepInfer: Open Source SOTA Inference running 155T toks/day/cluster making \$22m/day at ~80% margin for a 81 day

payback

26. X article by @zainasgar

27. Sam Altman: RSI, AI Consciousness, OpenAI's New Hardware, Compute, and more!