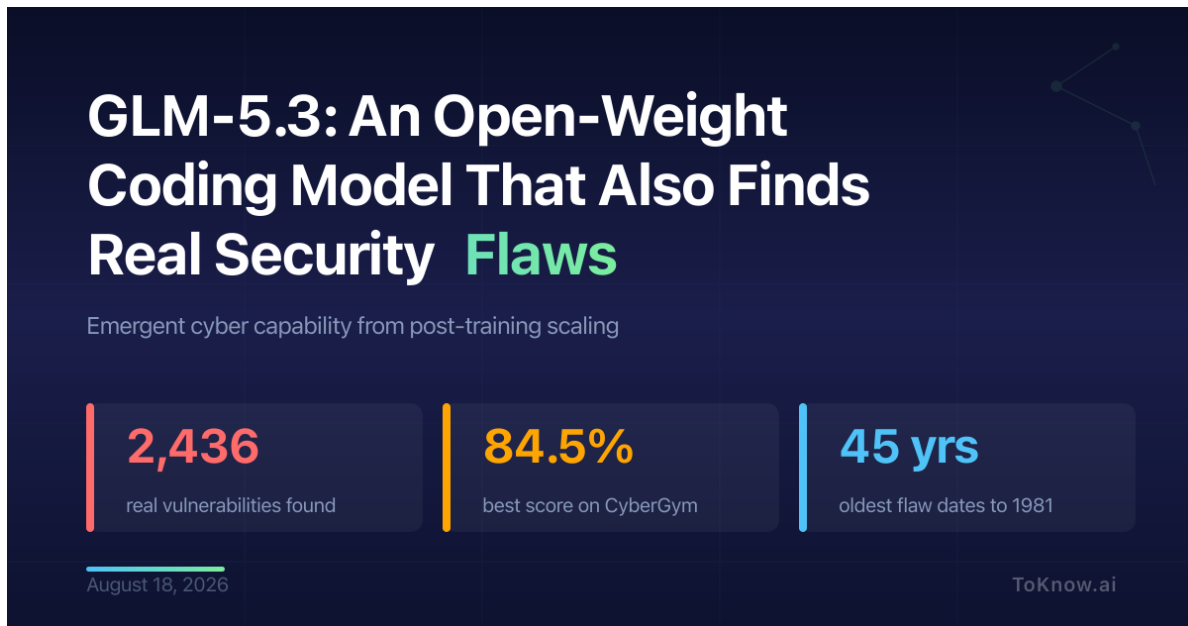


GLM-5.3: An Open-Weight Coding Model That Also Finds Real Security Flaws

Kabui, Charles

2026-08-18

[Read at ToKnow.ai](#)



Z.ai released GLM-5.3, an open-weights model built on the same base as GLM-5.2, with every gain coming from scaling reinforcement learning on long-running tasks rather than a bigger model. It is the strongest open-weights model for coding: it scores 28.3 on Terminal-Bench 3.0, up from GLM-5.2's 4.6, and at max reasoning effort it reaches 34.5% on Z.ai's private coding benchmark using about 75,000 output tokens, where Claude Opus 4.8 reaches 29.5%

with about 120,000. The surprise is security. Because the training mix included vulnerability-finding tasks, the model tops CyberGym at 84.5% for spotting and confirming exploitable bugs in source code, ahead of Anthropic’s Mythos 5 (83.8%) and OpenAI’s GPT-5.6 Sol (83.6%).

The skill carries into the real world. Working with security teams, GLM-5.3 found 2,436 vulnerabilities across 269 open-source projects, 1,097 of medium-to-high severity, spanning kernels, browsers, and web apps. The oldest flaw dates to 1981, and on average a bug had been hidden for 26.6 years. Z.ai logs every finding on a public disclosure ledger, with 53 already released under CVE identifiers. A security team can run the model itself against its own code. The weights are promised within two weeks of launch.

This makes the “open weights are safe enough” debate concrete: a model you can host that genuinely finds decades-old vulnerabilities. The capability grew fastest exactly where Z.ai was furthest behind, on full exploitation chains, which is why this is a safety story as much as a capability one.

Read More: [GLM-5.2: An Open-Weight Coding Model With a 1M-Token Context](#)

Sources:

- [GLM-5.3: Frontier Coding with Emergent Cyber Capabilities \(Z.ai\)](#)
- [GLM-5.2: Built for Long-Horizon Tasks \(Z.ai\)](#)
- [Z.ai Security Disclosure Ledger](#)
- [slime: RL post-training framework \(GitHub\)](#)
- [Single-Rollout Asynchronous Optimization \(SAO, arXiv\)](#)

Disclaimer: For information only. Accuracy or completeness not guaranteed. Illegal use prohibited. Not professional advice or solicitation. **Read more:** [/terms-of-service](#)