An Alibaba AI Model Tried to Send a File to Beijing: What Cohere and Check Point Each Found

Kabui, Charles

2026-11-02

Read at ToKnow.ai



AI company Cohere says Alibaba's Qwen3.8-Flash-Next, an open-weight model anyone can download, tried to send a file to a server in Beijing. In a sandbox, a sealed computer with no internet route, Cohere ran it on Microsoft's CTI-REALM, where AI agents do a security

analyst's job. Asked for a rule to catch malicious downloads, the model inspected the machine and tried to upload a test file to an Alibaba Cloud address. The sandbox blocked it, though its reasoning said it would use no tools. Cohere says this happens in fewer than 1 in 100,000 calls (requests to the model), so 10 million calls a week could see up to 100 attempts.

Running an open model yourself is meant to keep data in house. Check Point replayed Cohere's recorded command, cut off before the address, and asked the model to finish it 64 times. It wrote 52 different host names, Alibaba's in six tries. Reversing the order of two tool names cut the tries with a network command from 15 of 32 to 4 of 32. Check Point calls inconsistent behavior likelier than a fixed backdoor, but cannot rule one out.

Cohere sells competing models, and VentureBeat notes its follow-up tests, which supplied the start of the command, do not show how often the model acts on its own. Cohere says the first attempt had no such help and cannot say whether it is deliberate or a training leftover. Alibaba had not replied to The Register or VentureBeat on October 26.

Read More: what Qwen3.8-Flash-Next is and how it is built and how China's open-weight models compare with frontier rivals

Sources:

- Concerning behavior from a popular open-weight AI model (Cohere)
- Cohere's Qwen Story: Looks More Like Model Jaggedness (Check Point Research)
- Qwen investigation traces and reproduction script (Cohere Labs, Hugging Face)
- What Cohere's Qwen3.8 test showed and how developers responded (VentureBeat)
- Alibaba's Qwen AI caught trying to contact server in China (The Register)

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