Amazon launched a chatbot for large companies even as internal tests indicated potential problems.

What’s new: Amazon introduced Q, an AI-powered assistant that enables employees to query documents and corporate systems. Days later, the tech newsletter Platformer obtained internal documents that indicate the model can generates falsehood and leak confidential information. (Amazon Q is not to be confused with OpenAI Q*.)

How it works: Currently available as a free preview, Q analyzes private documents, databases, and code to answer questions, generate content, and take actions. Amazon plans to offer two tiers of service: a basic chatbot ($20 per month) and the chatbot plus code generation, troubleshooting, security evaluation, and human assistance from Amazon Web Services ($25 per month). Amazon promises not to train machine learning models on Q users’ data.

The issues: Three days after Amazon unveiled Q, employees began to flag issues on internal Slack and security reporting channels.

Q provided inaccurate recommendations on issues of digital sovereignty; that is, whether or not data should be stored within a particular jurisdiction, a thorny legal issue in Europe and other parts of the world.

One employee raised a “sev 2” alert, indicating an issue severe enough to warrant paging engineers after hours and over the weekend.

Internal tests showed that Q could leak confidential information from Amazon such as internal discount programs, unreleased features, and locations of AWS data centers. Amazon spokespeople called such scenarios hypothetical and denied that Q had leaked such information.

Behind the news: Amazon is not the only major AI company whose chatbot has leaked private information. Google researchers recently found that they could prompt OpenAI’s ChatGPT to divulge personal information found in its training data.

Why it matters: For Amazon, issues with a newly released system are a bump in the road to competing effectively against competitors like Microsoft Copilot and ChatGPT Enterprise. For developers, it’s a sobering reminder that when you move fast, what breaks may be your own product.

We’re thinking: In developing an AI system, often it’s necessary to launch — in a safe and responsible way — and make improvements based on real-world performance. We congratulate the Q team on getting the product out and look forward to seeing where they take it.