Report: DeepSeek’s chat histories and internal data were publicly exposed

A cloud security firm found a publicly accessible, fully controllable database belonging to DeepSeek, the Chinese firm that has recently shaken up the AI world, “within minutes” of examining DeepSeek’s security, according to a blog post by Wiz.

An analytical ClickHouse database tied to DeepSeek, “completely open and unauthenticated,” contained more than 1 million instances of “chat history, backend data, and sensitive information, including log streams, API secrets, and operational details,” according to Wiz. An open web interface also allowed for full database control and privilege escalation, with internal API endpoints and keys available through the interface and common URL parameters.

“While much of the attention around AI security is focused on futuristic threats, the real dangers often come from basic risks—like accidental external exposure of databases,” writes Gal Nagli at Wiz’s blog. “As organizations rush to adopt AI tools and services from a growing number of startups and providers, it’s essential to remember that by doing so, we’re entrusting these companies with sensitive data. The rapid pace of adoption often leads to overlooking security, but protecting customer data must remain the top priority.”

Ars has contacted DeepSeek for comment and will update this post with any response. Wiz noted that it did not receive a response from DeepSeek regarding its findings, but after contacting every DeepSeek email and LinkedIn profile Wiz could

find on Wednesday, the company protected the databases Wiz had previously accessed within half an hour.

https://arstechnica.com/security/2025/01/report-deepseeks-chat-histories-and-internal-data-were-publicly-exposed/