A Deepseek interrompeu novos registros de conta há alguns dias, assim como o aplicativo de IA surgiu na App Store. A empresa culpou a limitação por um ataque malicioso, dizendo que os detentores de contas da AI Deepseek podiam acessar o serviço enquanto os recém -chegados teriam que esperar.

Eu me perguntava na época se o ataque malicioso era real ou se era uma manobra esconder o fato de que a infraestrutura Deepseek talvez não seja capaz de lidar com o influxo de novos usuários morrendo para ver esse rival Chatgpt O1 cujo treinamento custou apenas uma fração do que O OpenAI passou em seu modelo de raciocínio.

Eu disse que em breve aprenderemos se alguém tentou atacar os servidores Deepseek ou se o serviço está lutando com novos registros.

Alguns dias depois, as limitações de registro desapareceram, mas temos um relatório detalhando um hack potencialmente grave. Acontece que os hackers não precisaram se esforçar muito para penetrar na segurança da startup de IA chinesa. Tudo o que eles precisavam fazer era encontrar acesso aberto a um banco de dados não garantido. Eles teriam descoberto até um milhão de toras que incluíam muitas informações confidenciais.

Isso é de acordo com a empresa de segurança Wiz Research, que explorou a segurança das propriedades on -line da Deepseek, tropeçando no enorme tesouro da informação.

A empresa detalhou suas descobertas em um blog depois de notificar a Deepseek sobre a vulnerabilidade:

> A Wiz Research identificou um banco de dados Clickhouse acessível ao público pertencente à DeepSeek, que permite o controle total sobre as operações do banco de dados, incluindo a capacidade de acessar dados internos. A exposição inclui mais de um milhão de linhas de fluxos de toras contendo histórico de bate -papo, chaves secretas, detalhes de back -end e outras informações altamente sensíveis. A equipe de pesquisa do Wiz divulgou imediatamente e responsavelmente a questão à Deepseek, que garantiu prontamente a exposição.

Deepseek garantiu os dados, mas se o Wiz pudesse obter acesso a eles e navegar pelos

dados de texto simples ininterruptos, é provável que os hackers que façam isso para viver também tenham encontrado acesso a ele:

> Esse banco de dados continha um volume significativo de histórico de bate -papo, dados de back -end e informações confidenciais, incluindo fluxos de log, segredos da API e detalhes operacionais.
>
> Mais criticamente, a exposição permitiu o controle completo do banco de dados e a escalada potencial de privilégios dentro do ambiente Deepseek, sem qualquer mecanismo de autenticação ou defesa para o mundo exterior.

Wiz rotulou a vulnerabilidade Deepseek como um “risco crítico” para a própria segurança da Deepseek e seus clientes:

> Esse nível de acesso representava um risco crítico para a própria segurança da Deepseek e para seus usuários finais. Não apenas um invasor poderia recuperar logs sensíveis e mensagens de bate-papo em texto simples, mas também podem exfiltrar as senhas de texto simples e arquivos locais ao longo das informações de propriedade diretamente do servidor.

No momento, não está claro se alguém roubou os dados no banco de dados, e a Deepseek não abordou o acidente de segurança como empresa nos EUA e em outros mercados ocidentais. Por outro lado, a Deepseek disse que o serviço estava sob ataque, embora ainda estejamos ouvir detalhes sobre o hack.

Os dados parecem pertencer a usuários chineses. Quantos usuários do DeepSeek podem ter sido expostos através do banco de dados e se os potenciais clientes internacionais afetados por hackeado não são claros.

Como Wiz aponta, o incidente de segurança é muito sério, especialmente para novos aplicativos de IA que se tornam virais.

“O rápido ritmo de adoção geralmente leva a negligenciar a segurança, mas a proteção dos dados dos clientes deve permanecer a principal prioridade”, disseram os pesquisadores. “É crucial que as equipes de segurança trabalhem em estreita colaboração com os engenheiros de IA para garantir a visibilidade da arquitetura, ferramentas e modelos que estão sendo usados, para que possamos proteger dados e impedir a exposição”.

A vulnerabilidade também tem grandes implicações de privacidade, além de garantir dados confidenciais do usuário. Lembre -se de que todos os seus dados vão para a China. O Wiz mostrou que os prompts são salvos em texto simples, tornando -os acessíveis a qualquer

pessoa com o direito de inspecionar esses arquivos.

Como um usuário de IA de longa data, só posso esperar que meus bate -papos chatgpt e dados sensíveis não sejam igualmente fáceis de acessar. Por outro lado, sei que o OpenAI sofreu sua própria parte das vulnerabilidades de segurança, especialmente em seus primeiros dias.

Separadamente, o Hack Deepseek descobriu outra descoberta incomum. Pesquisadores do WIZ disseram *Conectado* Que os sistemas Deepseek são quase idênticos ao OpenAI “até detalhes como o formato das teclas da API”. Alguns dias atrás, o Openai acusou a Deepseek de usar dados do ChatGPT sem consentimento para treinar seus primeiros modelos de IA Deepseek.

(Tagstotranslate) Deepseek