DeepSeek sends sensitive data to China, unencrypted

The viral Chinese AI app DeepSeek has been accused of 'pickpocketing' user data and sending it to ByteDance servers without encryption.

The DeepSeek chatbot, which once caused a stir with its natural language processing capabilities similar to ChatGPT, is now embroiled in a controversy over security issues. A recent study found that the DeepSeek mobile app on iOS and Android secretly sent sensitive user data, including chat content, to ByteDance (TikTok's parent company) servers in China without encryption.

DeepSeek was found to not encrypt data and had dangerous vulnerabilities.

This means that hackers can easily steal DeepSeek users' personal information if they take over the connection. Not to mention, the fact that the data is stored in China also raises concerns about the risk of the Chinese government accessing and using it for espionage purposes.

"Silly" security hole

NowSecure, the security firm that discovered the issue, said DeepSeek intentionally disabled Apple's App Transport Security (ATS) security feature, which is designed to protect user data during transmission.

Additionally, DeepSeek uses the outdated 3DES encryption method and hard-coded encryption keys stored on the device, creating serious security vulnerabilities.

Advice for users

Given these security risks, NowSecure recommends that users immediately remove DeepSeek from their phones. If they still want to experience it, users should install and run the application locally on their computers to minimize internet connection and data leakage.