Un reciente análisis de la aplicación móvil de DeepSeek para iOS ha revelado serias vulnerabilidades de seguridad, destacando especialmente el hecho de que transmite información confidencial a través de internet sin ningún tipo de cifrado, dejándola expuesta a posibles interceptaciones y manipulaciones.

La auditoría, llevada a cabo por NowSecure, también identificó que la aplicación no sigue las mejores prácticas en ciberseguridad y que recopila una cantidad significativa de datos sobre los usuarios y sus dispositivos.

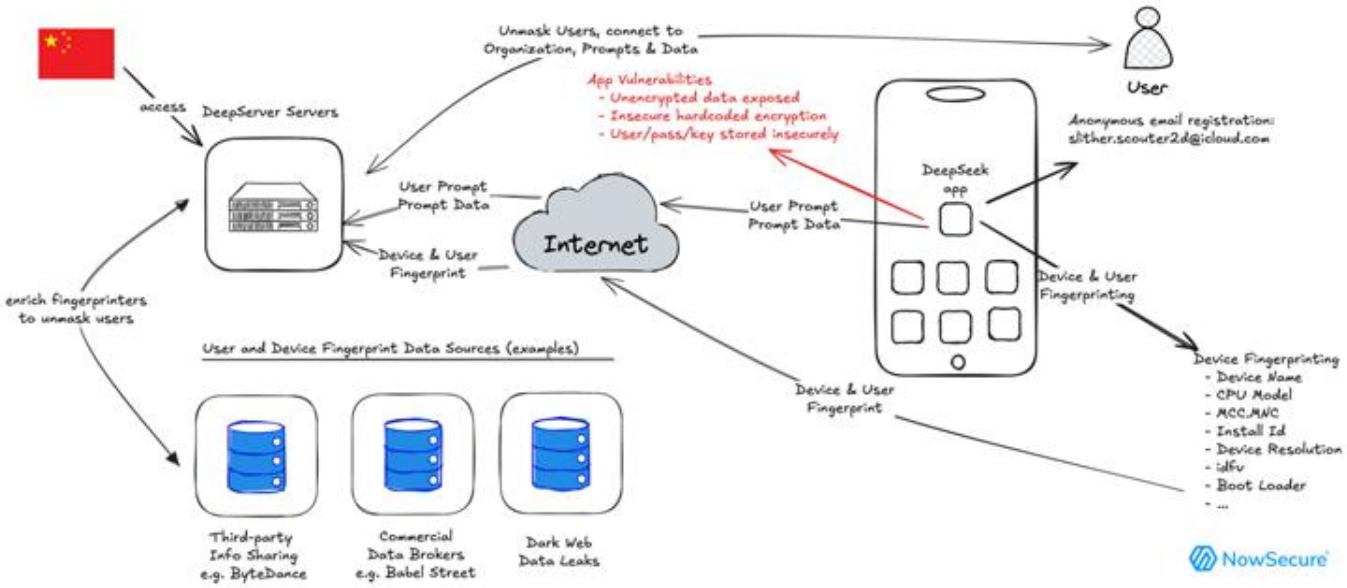
> *«La aplicación de DeepSeek para iOS envía ciertos datos de registro y detalles del dispositivo a internet sin aplicar ningún cifrado. Esto hace que la información transmitida pueda ser fácilmente interceptada y manipulada por atacantes»*, señaló la empresa.

El informe también detectó múltiples fallos en la implementación del cifrado de la información del usuario. Entre estos problemas se encuentran el uso de un algoritmo de cifrado simétrico obsoleto (3DES), la presencia de una clave de cifrado incrustada en el código de la aplicación y la reutilización de vectores de inicialización.

Además, la información es enviada a servidores que pertenecen a Volcano Engine, una plataforma de almacenamiento y computación en la nube operada por ByteDance, la misma compañía china que controla TikTok.

> *«DeepSeek para iOS desactiva por completo la función de seguridad App Transport Security (ATS), una medida de protección en el sistema iOS diseñada para evitar que datos sensibles sean enviados sin cifrar. Debido a esta configuración, la aplicación permite y efectivamente transmite datos sin protección a través de internet»,* explicó NowSecure.

Estos descubrimientos se suman a una creciente preocupación sobre el chatbot de inteligencia artificial (IA), que ha alcanzado rápidamente los primeros lugares en descargas tanto en Google Play como en la App Store de Apple en múltiples países.



Por su parte, la firma de ciberseguridad Check Point ha detectado que actores maliciosos están utilizando motores de IA de DeepSeek, así como Alibaba Qwen y OpenAI ChatGPT, para desarrollar programas de robo de información, crear contenido sin restricciones y mejorar scripts utilizados en campañas masivas de spam.

> *«A medida que los delincuentes emplean técnicas avanzadas, como la manipulación del sistema para eludir medidas de seguridad, con el fin de desarrollar malware, fraudes financieros y estrategias de distribución de spam, las organizaciones deben adoptar medidas preventivas para fortalecer sus defensas contra el uso indebido de estas tecnologías de IA»*, advirtió Check Point.

Recientemente, Associated Press reveló que el sitio web de DeepSeek está configurado para compartir las credenciales de inicio de sesión de los usuarios con China Mobile, una compañía estatal de telecomunicaciones prohibida en Estados Unidos.

Las conexiones de la aplicación con China, al igual que en el caso de TikTok, han llevado a legisladores estadounidenses a impulsar la prohibición de DeepSeek en dispositivos gubernamentales, ante el riesgo de que pueda facilitar el acceso de Pekín a la información de los usuarios.

Es importante mencionar que varios países, como Australia, Italia, los Países Bajos, Taiwán y Corea del Sur, así como agencias gubernamentales de India y Estados Unidos (incluyendo el Congreso, la NASA, la Marina, el Pentágono y el estado de Texas), han restringido el uso de DeepSeek en dispositivos oficiales.

El enorme crecimiento de DeepSeek también lo ha convertido en un objetivo frecuente de ataques cibernéticos. La empresa china de ciberseguridad XLab informó al Global Times que la plataforma ha sido blanco de ataques de denegación de servicio distribuido (DDoS) en las últimas semanas, perpetrados por las botnets Mirai hailBot y RapperBot.

Mientras tanto, los ciberdelincuentes están aprovechando la popularidad de DeepSeek para crear páginas web fraudulentas destinadas a distribuir software malicioso, ejecutar estafas de inversión y promover esquemas engañosos de criptomonedas.