Experts Flag Security, Privacy Risks in DeepSeek AI App

February 6, 2025 35 Comments

New mobile apps from the Chinese artificial intelligence (AI) company **DeepSeek** have remained among the top three "free" downloads for Apple and Google devices since their debut on Jan. 25, 2025. But experts caution that many of DeepSeek's design choices — such as using hard-coded encryption keys, and sending unencrypted user and device data to Chinese companies — introduce a number of glaring security and privacy risks.

Public interest in the DeepSeek AI chat apps swelled following widespread media reports that the upstart Chinese AI firm had managed to match the abilities of cutting-edge chatbots while using a fraction of the specialized computer chips that leading AI companies rely on. As of this writing, DeepSeek is the third most-downloaded "free" app on the Apple store, and #1 on Google Play.

DeepSeek's rapid rise caught the attention of the mobile security firm **NowSecure**, a Chicago-based company that helps clients screen mobile apps for security and privacy threats. In a teardown of the DeepSeek app published today, NowSecure urged organizations to remove the DeepSeek iOS mobile app from their environments, citing security concerns.

NowSecure founder **Andrew Hoog** said they haven't yet concluded an in-depth analysis of the DeepSeek app for **Android** devices, but that there is little reason to believe its basic design would be functionally much different.

Hoog told KrebsOnSecurity there were a number of qualities about the DeepSeek iOS app that suggest the presence of deep-seated security and privacy risks. For starters, he said, the app collects an awful lot of data about the user's device.

"They are doing some very interesting things that are on the edge of advanced device fingerprinting," Hoog said, noting that one property of the app tracks the device's name — which for many iOS devices defaults to the customer's name followed by the type of iOS device.

The device information shared, combined with the user's Internet address and data gathered from mobile advertising companies, could be used to deanonymize users of the DeepSeek iOS app, NowSecure warned. The report notes that DeepSeek communicates with **Volcengine**, a cloud platform developed by **ByteDance** (the makers of **TikTok**), although NowSecure said it wasn't clear if the data is just leveraging ByteDance's digital transformation cloud service or if the declared information share extends further between the two companies.

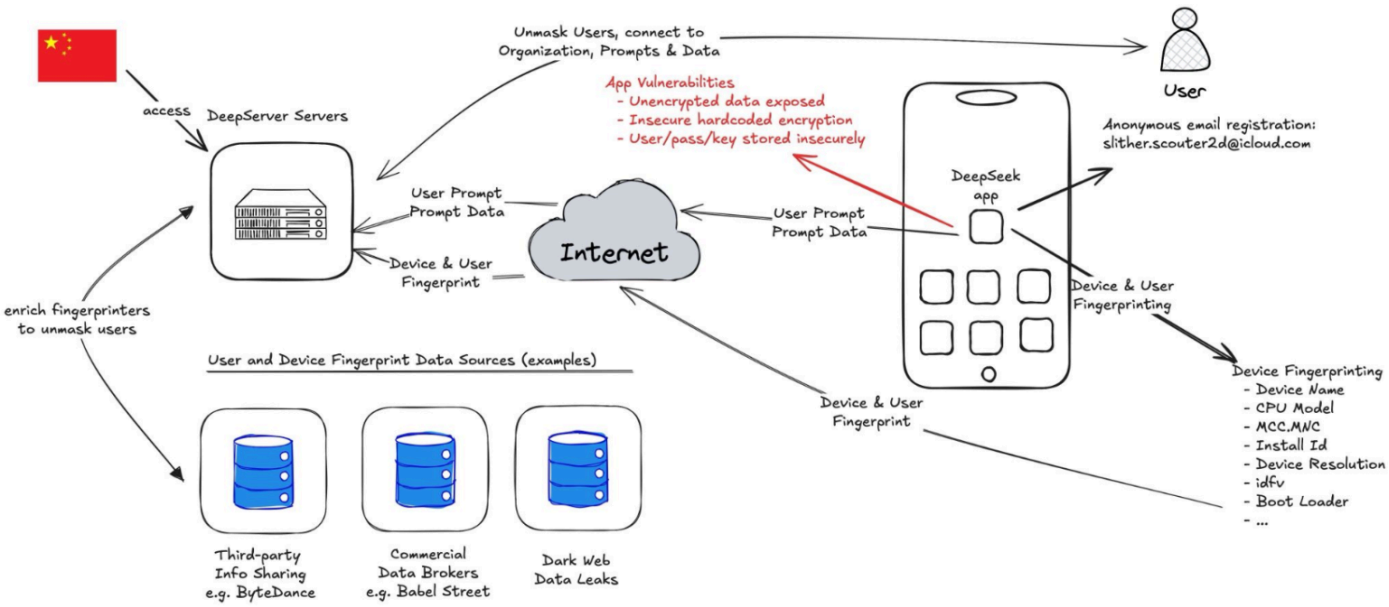

Image: NowSecure.

Perhaps more concerning, NowSecure said the iOS app transmits device information "in the clear," without any encryption to encapsulate the data. This means the data being handled by the app could be intercepted, read, and even modified by anyone who has access to any of the networks that carry the app's traffic.

"The DeepSeek iOS app globally disables App Transport Security (ATS) which is an iOS platform level protection that prevents sensitive data from being sent over unencrypted channels," the report observed. "Since this protection is disabled, the app can (and does) send unencrypted data over the internet."

Hoog said the app does selectively encrypt portions of the responses coming from DeepSeek servers. But they also found it uses an insecure and now deprecated encryption algorithm called 3DES (aka Triple DES), and that the developers had hard-coded the encryption key. That means the cryptographic key needed to decipher those data fields can be extracted from the app itself.

There were other, less alarming security and privacy issues highlighted in the report, but Hoog said he's confident there are additional, unseen security concerns lurking within the app's code.

"When we see people exhibit really simplistic coding errors, as you dig deeper there are usually a lot more issues," Hoog said. "There is virtually no priority around security or privacy. Whether cultural, or mandated by China, or a witting choice, taken together they point to significant lapse in security and privacy controls, and that puts companies at risk."

Apparently, plenty of others share this view. *Axios* reported on January 30 that U.S. congressional offices are being warned not to use the app.

"[T]hreat actors are already exploiting DeepSeek to deliver malicious software and infect devices," read the notice from the chief administrative officer for the House of Representatives. "To mitigate these risks, the House has taken security measures to restrict DeepSeek's functionality on all House-issued devices."

TechCrunch reports that Italy and Taiwan have already moved to ban DeepSeek over security concerns. *Bloomberg* writes that **The Pentagon** has blocked access to DeepSeek. *CNBC* says **NASA** also banned employees from using the service, as did the **U.S. Navy**.

Beyond security concerns tied to the DeepSeek iOS app, there are indications the Chinese AI company may be playing fast and loose with the data that it collects from and about users. On January 29, researchers at **Wiz** said they discovered a publicly accessible database linked to DeepSeek that exposed "a significant volume of chat history, backend data and sensitive information, including log streams, API secrets, and operational details."

"More critically, the exposure allowed for full database control and potential privilege escalation within the DeepSeek environment, without any authentication or defense mechanism to the outside world," Wiz wrote. [Full disclosure: Wiz is currently an advertiser on this website.]

KrebsOnSecurity sought comment on the report from DeepSeek and from Apple. This story will be updated with any substantive replies.

This entry was posted on Thursday 6th of February 2025 04:12 PM

A LITTLE SUNSHINE | LATEST WARNINGS | THE COMING STORM

ANDREW HOOG | APP TRANSPORT SECURITY | APPLE | ARTIFICIAL INTELLIGENCE | BYTEDANCE | CHINA | DEEPSEEK | DEEPSEEK AI | IOS | NOWSECURE | VOLCENGINE

35 thoughts on “Experts Flag Security, Privacy Risks in DeepSeek AI App”

Steve Everett

February 6, 2025

I have already forwarded this to everyone in our company who has a company cell phone. Already we only allow a small list of applications on our company phone via Intune. I am also concerned about the security of our employee’s personal phones.

Zog

-

February 6, 2025

I have my one own phone and believe you me, EVERY one’s cut off from deep-seek.

Romana Challans

February 6, 2025

Australian federal government, as well as several state governments, have all banned DeepSeek (for government usage) for these reasons – and one, suspects questions about Chinese government access and involvement.

MetaWalker

February 6, 2025

School Report Card:
Aptitude: A+
Achievements: A+
Diligence: B-
Impact: A+++++++++
Deepseek has a tendancy to come up with some novel approaches and doesn’t always follow the norms which have been set by his peer group. He is a loner in some respects, but I sense his presense, approach and following will grow over the course of 2025. His last piece of work was completed with haste, no doubt due to family commitments (MIC2025), but I liked the openness of the code which will allow his peer group to study and learn from it for future submissions. I’ve given his peers a copy, so they can study it in earnest and I’m hoping they will learn from it and it will inspire them to further their knowledge and understanding for all to share