

DeepSeek iOS app sends data unencrypted to ByteDance-controlled servers

Thomas Reed, staff product manager for Mac endpoint detection and response at security firm Huntress, and an expert in iOS security, said he found NowSecure's findings concerning.

"ATS being disabled is generally a bad idea," he wrote in an online interview. "That essentially allows the app to communicate via insecure protocols, like HTTP. Apple does allow it, and I'm sure other apps probably do it, but they shouldn't. There's no good reason for this in this day and age."

He added: "Even if they were to secure the communications, I'd still be extremely unwilling to send any remotely sensitive data that will end up on a server that the government of China could get access to."

HD Moore, founder and CEO of runZero, said he was less concerned about ByteDance or other Chinese companies having access to data.

"The unencrypted HTTP endpoints are inexcusable," he wrote. "You would expect the mobile app and their framework partners (ByteDance, Volcengine, etc) to Hoover device data, just like anything else—but the HTTP endpoints expose data to anyone in the network path, not just the vendor and their partners."

On Thursday, US lawmakers began pushing to immediately ban DeepSeek from all government devices, citing national security concerns that the Chinese Communist Party may have built a

backdoor into the service to access Americans' sensitive private data. If passed, DeepSeek could be banned within 60 days.

This story was updated to add further examples of security concerns regarding DeepSeek.

<https://arstechnica.com/security/2025/02/deepseek-ios-app-sends-data-unencrypted-to-bytedance-controlled-servers/>