# DeepSeek faces major security flaw in AI technology



In a striking revelation, DeepSeek, a Chinese startup renowned for its innovative advancements in AI technology, has recently faced a significant security vulnerability in its open-source model. The incident has drawn attention to potential shortcomings in the company's data protection measures, raising concerns about the maturity of its systems.

Cloud security firm Wiz conducted a thorough examination of DeepSeek's databases and made alarming discoveries within just minutes. According to Wiz's vulnerability report, researchers were able to access "a trove of completely unencrypted internal data" including sensitive information such as chat histories, backend data, log streams, API secrets, and crucial operational details. This unguarded database posed a substantial risk, given that it could be exploited to launch an attack on DeepSeek’s systems—remarkably without any authentication or protective measures in place.

Reflecting on the ease of access to this sensitive information, Nir Ohfeld, head of vulnerability research at Wiz, noted that such glaring security flaws are "right at the front door." His comments highlight a concerning trend, as he mentioned that typically, similar exposures are found in neglected services, which require extensive scanning and time to uncover.

Wiz's attempts to alert DeepSeek of the breach were fraught with difficulty; researchers struggled to make contact with anyone at the company, resorting to sending messages through LinkedIn and emails to various accounts associated with DeepSeek. Although they received no initial response, the situation prompted a swift reaction, with the database being secured within an hour of the notification.

Wiz's chief technology officer, Ami Luttwak, categorically stated, "The fact that mistakes happen is correct, but this is a dramatic mistake, because the effort level is very low and the access level that we got is very high." Luttwak further expressed concerns over the maturity of DeepSeek’s service for handling sensitive data, asserting that such vulnerabilities render it unsuitable for use with critical information.

This incident underlines the paramount importance of robust security protocols for companies dealing in advanced technologies, particularly those within the realm of artificial intelligence. As the industry continues to evolve, maintaining stringent data protection measures will be crucial in safeguarding sensitive information against potential breaches.

Source: [Noah Wire Services](https://www.noahwire.com)

## References

* <https://www.secureworld.io/industry-news/deepseek-data-exposure> - This article corroborates the security vulnerability faced by DeepSeek, highlighting the exposure of sensitive data due to poor security practices.
* <https://www.secureworld.io/industry-news/deepseek-data-exposure> - It supports the claim that Wiz researchers discovered an unprotected ClickHouse database belonging to DeepSeek, exposing internal logs and API secrets.
* <https://www.secureworld.io/industry-news/deepseek-data-exposure> - The article mentions that DeepSeek acted swiftly to secure the database after being notified by Wiz, aligning with the swift reaction described.
* <https://www.secureworld.io/industry-news/deepseek-data-exposure> - It emphasizes the broader issue of AI companies often neglecting foundational cybersecurity risks while focusing on advanced threats.
* <https://www.secureworld.io/industry-news/deepseek-data-exposure> - The article highlights the importance of basic security hygiene to prevent such breaches.
* <https://www.secureworld.io/industry-news/deepseek-data-exposure> - It notes that DeepSeek is facing regulatory investigations in Italy and has been flagged by the U.S. Navy for potential national security concerns.
* <https://www.secureworld.io/industry-news/deepseek-data-exposure> - The article underscores the need for robust cybersecurity measures in AI companies to protect sensitive data.
* <https://www.secureworld.io/industry-news/deepseek-data-exposure> - It discusses the potential risks of exposing sensitive user interactions and proprietary AI models due to security lapses.
* <https://www.secureworld.io/industry-news/deepseek-data-exposure> - The incident serves as a warning for AI security in 2025, emphasizing the urgency of addressing cybersecurity gaps.