Computer Forensics and
Security BS (hons) 2nd year

Will Gusackova
28/01/2025

Security Breaches Based on Software Vulnerabilities

Abstract of Report:

This report brief contains two breaches from DeepSeek and Trello, that impact how programmers will progress into the future, facing vulnerabilities and implementing changes and awareness of the programing faults that were once known or not known to the public. As a result, developers will need to adopt a heightened awareness of security risks, take proactive steps in identifying vulnerabilities, and implement more robust safeguards in their coding practices to prevent similar breaches moving forward.

Trello:

Trello is a web-based project management tool that uses boards, lists, and cards to organize tasks, collaborate, and track progress. It is advertised as simple, visual, and helps teams stay organized. Released on September 13th, 2011. (*Wikipedia*, 2025)

Developed with main languages: JavaScript, CoffeeScript, Node.js

Database: MongoDB

Trello's User data out in the open 2024

Trello was exploited by an unprotected open API endpoint that did not require login credentials. This flaw enabled the attacker to connect email addresses to Trello accounts, revealing user identities. The attacker then continued to exploit this vulnerability. As a result, millions of Trello users had their data stolen, putting everyone affected at significant risk. (NordPass, 2024)

Ranking this as a Critical vulnerability, as vulnerable people had their emails leaked, leading the attacker to potentially expose them to harmful phishing emails.

Computer Forensics and Security BS (hons) 2nd year

Will Gusackova
28/01/2025

Deepseek:

Deepseek, an Artificial Intelligence that was developed in China, that develops open-source large language models (LLMs). Founded by Liang Wenfeng. Deepseek was developed at a lower training cost compared to ChatGPT, which is its primary competitor. (*Wikipedia*, 2025)

Developed with main languages: Python, R, Java, C++, JavaScript, Julia.

Database: SQL, ClickHouse

(Vivek, T., 2025)

Deepseek chat logs exposed 2025

29th January 2025 a breach was detected by Wiz Researchers, which they discovered a ClickHouse database owned by deepseek, exposing log streams with chat history, secret keys, and general sensitive information. (*Nagli G.,* 2025)

This ClickHouse database had a critical vulnerability that allowed attackers to exploit a SQL injection flaw, enabling unauthorized users to interact directly with the database. Through this injection, malicious actors retrieved sensitive data, modified records, and potentially execute destructive commands.

Deepseek also had two unusual open ports "(8123 & 9000)", alongside HTTP "(80/443)", HTTP being unsecure and not encrypted. (*Nagli G.,* 2025)

The SQL injection attack gave attackers full control over the database, bypassing standard authentication measures and directly interacting with the underlying systems. This could lead to the exposure of personal information, financial data, internal business records, and other confidential materials. In some cases, attackers may have been able to escalate their privileges, gaining access to additional systems within the network. Attackers could have used this access to insert malicious scripts, alter, or delete critical data, and potentially cause widespread service disruptions.

Such breaches not only compromise data integrity but also damage the reputation of the organization, potentially leading to legal repercussions, regulatory fines, and a loss of customer trust. This breach is a reminder of the importance of implementing proper security practices, including input validation, prepared statements, and regular security audits, to prevent SQL injection vulnerabilities from being exploited.

<u>Why are these issues considered a critical venerability?</u>

The biggest flaws are cyber security based, companies with a lack of security can face difficulties with user's trust. As for deepseek, future projects can be tainted, if requesting for user's data such as emails, phone numbers etc.

Having a database that is out in the open can motivate attackers to gain unauthorized access to sensitive data stored in the database. This may include personal identifiable information (PII), financial records, intellectual property, and other confidential business information. For Trello, this was particularly critical, as many projects and user emails were exposed to potential threats. Many users verified this exposure by using the "Have I Been Pwned?" Website. (Twingate, 2025)

The exposure of sensitive data through a breach makes Trello less trustworthy, as users rely on the platform to securely manage their personal and business information. When a company experiences a data breach, especially one that reveals personally identifiable information (PII), it raises serious concerns about the security measures in place.

It is important to keep databases away from the outside world, as there are laws and regulations in place to protect personal data. Article 33 and Article 34 of the GDPR highlight the importance of promptly addressing and reporting data breaches to minimize harm to individuals and ensure compliance.

Root cause of the vulnerability:

The root cause of the deepseek vulnerability is the programmers had the database in plaintext and was left open and unauthenticated, allowing anyone with the necessary information to access the data, submit SQL data requests, or SQL injections.

This vulnerability stemmed from a lack of proper access controls, such as authentication or network restrictions, which led to the sensitive data being exposed to external parties. The database was designed for efficient real-time analytics, but its misconfiguration allowed full access to log streams containing extremely sensitive information, including chat history, API keys, and backend details.

Best ways this breach could have been avoided:

- Network Segmentation and Firewall Rules**:** By placing sensitive databases behind firewalls and isolating them from public-facing services, DeepSeek could have limited exposure to only trusted internal networks. Implementing network segmentation would have helped ensure that sensitive data was not directly accessible from the public internet.

- Access Control and Authentication: Have strict access control for databases to avoid unauthenticated people accessing the database.

- Encryption: The ClickHouse database should have been configured to avoid exposure through its HTTP interface without proper authorization. Data could have been encrypted instead of being in plaintext. Avoid the usage of HTTP, instead implement usage of HTTPS. Developers should follow best practices for configuring databases, including disabling unnecessary public-facing ports and securing the default API access points.

- Isolate the Database Server: It is crucial to isolate production database servers from other applications and services as much as possible. Dedicated database servers have a smaller attack surface, reducing the risk of external threats. To keep the server lean, only necessary services should be installed and running. Avoid installing unnecessary applications unless they are required by the database.

- SQL Injection Prevention: Validate all inputs rigorously and use prepared statements to avoid SQL injection attacks and ensure that API endpoints are protected from SQL injections or any similar vulnerabilities.

Computer Forensics and
Security BS (hons) 2nd year

Will Gusackova
28/01/2025

Grade of severity:

	DeepSeek	%	Trello	%
Severity of Impact	Didn't Impact the limited user sign-up	10/30	Vulnerable Impacted as they had personal data leaked	30/30
Exposure Time	Didn't Last that long	15/30	Personal data leak cannot be fixed	30/30
Ease of Exploitation	Very easy to access data	20/20	A lot of knowledge is needed to exploit	5/20
Reputation Damage	"AI is supposed to be smart"	10/10	Impacted trust	10/10
Legal and Regulatory Consequences	No legal action has been taken yet	5/15	Violation of GDPR	10/15
Total	Risk:	60/100	Risk:	85/100

References:

Vivek, T., 2025. *Top Programming Languages used in DeepSeek AI*. Technology With Vivek. Available at: https://www.technologywithvivek.com/2025/01/Top%20Programming%20Languages%20used%20in%20Deepseek%20AI.html#:~:text=For%20Deepseek%20AI%2C%20Python%20is,building%20high%2Dlevel%20AI%20systems. [Accessed 01 February 2025].

Nagli G., 2025. *Wiz Research uncovers exposed DeepSeek database leak*. Wiz Blog. Available at: https://www.wiz.io/blog/wiz-research-uncovers-exposed-deepseek-database-leak [Accessed 01 February 2025].

Wikipedia contributors, 2025. *DeepSeek*. Wikipedia. Available at: https://en.wikipedia.org/wiki/DeepSeek#:~:text=Hangzhou%20DeepSeek%20Artificial%20Intelligence%20Basic,Chinese%20hedge%20fund%20High%2DFlyer. [Accessed: 09 February 2025].

Citizens Information, 2023. *Overview of General Data Protection Regulation*. Citizens Information. Available at: https://www.citizensinformation.ie/en/government-in-ireland/data-protection/overview-of-general-data-protection-regulation/ [Accessed: 09 February 2025].

NordPass, 2024. *Trello Data Breach: What Happened and How You Can Protect Yourself*. NordPass. Available at: https://nordpass.com/blog/trello-data-breach/ [Accessed: 11 February 2025].

Twingate, 2025. *Trello data breach: What you need to know*. Twingate Blog. Available at: https://www.twingate.com/blog/tips/Trello-data-breach [Accessed 11 February 2025].

Wikipedia contributors, 2025. *Trello*. Wikipedia. Available at: https://en.wikipedia.org/wiki/Trello [Accessed: 15 February 2025].

Atlassian, 2012. *The Trello Tech Stack*. Atlassian Blog. Available at: https://www.atlassian.com/blog/trello/the-trello-tech-stack [Accessed 15 February 2025].

Sen K., 2025. *11 Steps to Secure SQL*. UpGuard Blog. Available at: https://www.upguard.com/blog/11-steps-to-secure-sql [Accessed 15 February 2025].