Lovable-built apps and missing database access rules (CVE-2025-48757)

IMPLEMENTED 2025 · TECHNOLOGY AND SOFTWARE · SWEDEN · BAND F · PARTLY PROVED

VERSION 1.0 · PUBLISHED 15 NOVEMBER 2026 · UPDATED 15 NOVEMBER 2026 · FACTS CHECKED 15 NOVEMBER 2026

In 2025 security researchers reported that many apps built on the Lovable platform let anyone read, and in some cases write, database tables because row-level security rules were missing or weak. The record CVE-2025-48757 was published in May 2025 and carries a note that Lovable disputes it, since each customer is responsible for protecting their app's data. Lovable added a security scan in April 2025.

ABOUT THIS SYNOPSIS

This is MarLuc's summary and grading of publicly available sources, for information only. It is not investment, legal, financial or professional advice, and should not be relied on for any decision. Readers must validate it against the original sources and, where appropriate, challenge its conclusions.

Facts and figures are as reported by the sources listed below, which may be incomplete, self-reported or out of date. Check the original source before relying on any figure.

The impact band, proof marker and SEAM view are MarLuc's opinion. The organisation is not a MarLuc client and has not reviewed or endorsed this synopsis. Names and trademarks belong to their owners.

NOTICE WORDING LAST UPDATED 16 NOVEMBER 2026

AT A GLANCE

What went wrong: AI output or malfunction; Weak oversight or controls.

AI-native company: built around AI from the start to bring about transformational change. It has folded, so the case is graded F.

AI used: AI app builder: users describe an app in plain language and the platform generates the front end and connects it to a hosted database.

Implemented: 2025. Grade: band F, Failure, Partly proved.

Headline result, as reported: A researcher's scan found 170 of 1,645 Lovable-built apps (10.3%) with inadequate database access rules; the flaw was recorded as CVE-2025-48757 in May 2025 and Lovable disputes that it is a platform flaw

1 · The case

The facts, as reported by the 5 sources listed at the end. Where a source is silent, the field says "Not reported".

Organisation

Lovable. Swedish AI-native software company. Its platform lets users build web apps by chatting with an AI. The affected apps belong to its customers, many of whom are non-specialists. Canvas block: 8. Governance and risk. Also 6. Data and technology.

Business challenge

The challenge. Lovable's apps talk to a hosted database from the user's browser, so each table needs access rules. By the researchers' account, apps created on the platform often lacked secure rules, and the burden fell on the builder.

How it was addressed. Researchers scanned 1,645 sites listed on Lovable's showcase and reported 303 endpoints across 170 projects with inadequate row-level security. They notified Lovable in March and April 2025 and published the record CVE-2025-48757 on 29 May 2025. Lovable launched a security scan in April 2025 and, per the CVE entry, disputes the finding on the basis that customers are responsible for their own data. [1] [2] [3] [4] [5]

Who implemented it

Lovable (Software vendor): Operates the AI app builder that generated the affected apps..
The affected apps were built by Lovable's customers. The database service is third party; the sources opened do not name it in Lovable's own materials, and the researchers' write-up names Supabase endpoints in examples.

Technology (SEAM pillar E)

SEAM types: not established; the sources do not say how the system works. Deployment: Vendor SaaS. Vendors and products: Lovable, Lovable app builder.

Where it was built in: Lovable generates front-end apps that call a hosted database directly from the browser with a public key, relying on row-level security rules to protect data, per the researchers.

What changed

Before: apps could be published with missing or weak access rules and no platform check. After: Lovable's April 2025 release checks for vulnerabilities on publish for apps connected to Supabase. Whether this closed the exposure is disputed by the researchers. [1] [2] [3] [4] [5]

Cost of failure

Not reported. No fines, damages or breach notifications are reported in the sources opened.

What it saved

Not reported [1] [2] [3] [4] [5]

Governance and control

The CVE record exists and the supplier disputes it. Lovable's changelog describes the scan as a start. The researchers say Lovable did not respond beyond confirming receipt, which Lovable has not been reported to dispute in the sources opened.

S2 · Accountable owner · Not reported
No named owner for secure defaults at Lovable is reported in the sources opened.

A1 · Safe use · Claimed
Lovable's position, recorded in the CVE entry, is that each customer accepts responsibility for protecting their application's data. [1]

A2 · Human in the loop · Not reported
How generated database rules are reviewed by a person is not reported.

A3 · Monitoring and assurance · Claimed
Lovable says its April 2025 scan checks for vulnerabilities when an app is published and is the start of work to make vibe coding safer by default. The researchers say it checks only that a rule exists. [2] [3]

A4 · Vendor AI · Not reported
Not reported.

A5 · Agent controls · Not reported
No agents described.

A6 · Standards and regulation · Outside scrutiny (a regulator, court, auditor or similar body acted)
The CVE record was published through MITRE and carries a CISA enrichment entry; the record states that the supplier disputes it. [1]

What worked, what did not, what is unproven

WORKED

– Lovable launched a publish-time security scan within weeks of the disclosure.

– Per its 2026 blog, Lovable later made new projects private by default and published a response when a different flaw was reported.

DID NOT

– The researchers found data and keys exposed in apps built with the platform, including a site maintained by a Lovable employee.

– Per the researchers, the scan checks that a rule exists but not that it matches the app's logic.

– Lovable's 2026 blog says an earlier answer to a separate report missed the mark.

UNPROVEN

– How many end users were harmed: Not reported.

– Whether the April 2025 scan closed the gap: disputed by the researchers; Lovable's view is not reported in the sources opened.

– Whether Lovable-built apps are less secure than apps built by hand: no comparison in the sources opened.

Timeline

Mar 2025 20 and 21 March: researchers report finding the flaw on one Lovable-built site, then a broader scan of 1,645 sites [2]

Apr 2025 Lovable confirms receipt of the researchers' email (24 March); formal disclosure follows on 14 April [2]

Apr 2025 Lovable 2.0 adds a security scan on publish (dated 25 April in Lovable's changelog; 24 April in the researchers' write-up) [3]

May 2025 CVE-2025-48757 published, with a note that the supplier disputes it [1]

Apr 2026 Separate incident: Lovable reports that backend regressions re-enabled access to chat history and source code of public projects from February 2026; it fixes this within two hours of the 20 April report [4]

2 · Grade and SEAM assessment

MarLuc's opinion, made on the evidence above. How cases are graded: marluc.co.uk/case-studies/how-we-rate

Level of change and impact

Claimed: Not applicable. Grade: F, Failure. Proof: Partly proved. Level of change: Not graded.

No level assessed: band F. Harm is shown by exposure of data in apps built on the platform, with the supplier disputing where responsibility lies.

The SEAM view and lessons learnt

The exposure sat at the join between a tool that generates an app and the person responsible for it. The builder is a non-specialist and the platform's default decides what is protected. For an organisation whose staff use such tools, the practical points are who reviews access rules before anything holds personal data, and whether the vendor's scan is treated as a check or as a guarantee.

1. Check database access rules before an AI-built app holds personal data.
2. Agree who is responsible for security before staff publish with an app builder.
3. Treat a vendor's security scan as one check, not as assurance.

Evidence

Score 2 of 4. Mixed: a CVE record disputed by the supplier, the researchers' own write-up, and the supplier's changelog. Their scan results were not independently replicated in the sources opened.

Evaluation method. CVE record and researchers' disclosure, with the supplier's dispute noted in the record; no regulator or court finding.

Sources disagree. Lovable disputes that the flaw is its own because customers are responsible for protecting their application's data. The researchers say secure defaults are the platform's job. The two sources also give different release dates for Lovable 2.0 (25 April in the changelog, 24 April in the write-up). The researchers' write-up does not state the author's employer; a different aggregator lists a competitor, which was not verified.

Status. Open: the CVE is listed as published and disputed. Current state of Lovable's defaults not checked beyond its changelog.

3 · Original sources

Read these in full. To challenge a fact or a grade, use the contact form at marluc.co.uk or the link on https://marluc.co.uk/case-studies/lovable-row-level-security-cve-2025-48757

[1] CVE Program: CVE-2025-48757 record
https://cveawg.mitre.org/api/cve/CVE-2025-48757

[2] Matt Palmer: Statement on CVE-2025-48757
https://mattpalmer.io/posts/statement-on-CVE-2025-48757/

[3] Lovable documentation: changelog
https://docs.lovable.dev/changelog

[4] Lovable: Our response to the April 2026 incident
https://lovable.dev/en/blog/our-response-to-the-april-2026-incident

[5] The Register: Lovable denies data leak, cites 'intentional behavior'
https://www.theregister.com/security/2026/04/21/lovable-denies-data-leak-cites-intentional-behavior/5226233

Lovable website: https://lovable.dev

Version 1.0 · Published 15 November 2026 · Updated 15 November 2026 · Facts checked against sources 15 November 2026 · Downloaded 26 November 2026. This PDF may be out of date: the latest version, and a way to report an error or a better source, is at https://marluc.co.uk/case-studies/lovable-row-level-security-cve-2025-48757

VERSION HISTORY

v1.0 15 November 2026 First published