

Folioport: what was found and what was fixed

Prepared for: Folioport's founder (a fictional client portal for design studios)

Prepared by: Ilya Shkura

The app: React and TypeScript on Firebase: Firestore, Storage, Cloud Functions, Authentication

FOUND

29

5 high, 12 medium, 12 low

PARTLY FIXED

3

the rest of each is listed

HIGH LEFT

0

26 of 29 fixed in three rounds

Summary for the founder

Folioport worked on the normal path, but it did not keep people to their own part of it. A client could read the studio's private notes about them, the studio could approve work in the client's name and rewrite past decisions, and file addresses kept opening after access was gone. After three rounds of fixes 26 of the 29 problems are fixed and 3 partly, with no high left; the fixed portal runs on a real Firebase project.

FOUND

29

5 high, 12 medium, 12 low

FIXED

26 of 29

3 more partly

As received: "I went through Folioport as each kind of person and fixed what I found. ... Nothing was broken: no errors, failed loads, broken text or endless spinners."

What was fine: Signed out, a visitor got nothing; projects, stages, approvals, files and share links worked as the screens promised; plans, trials and suspensions switched the right things on and off.

What mattered most

HIGH

A client's people could read the studio's private notes about them

Allowed: the notes came back

HIGH

The studio could approve a stage in the client's name

Approved, shown as approved by the client

HIGH

The studio could rewrite a decision the client had already made

Rewritten to "approved", with a new date

HIGH

A file's address kept opening after access was gone

Opens without signing in, after removal

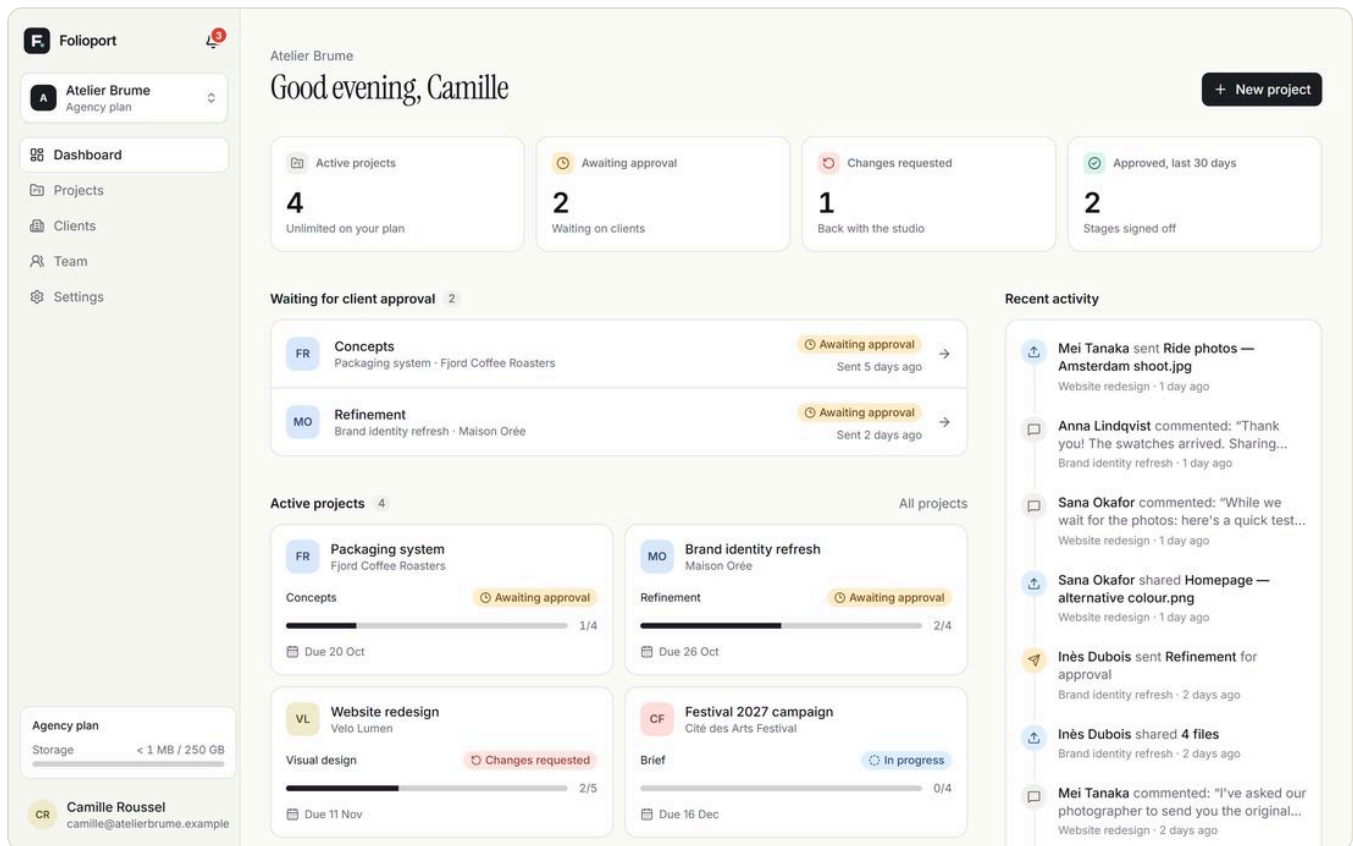
HIGH

An uploaded HTML or SVG file opened as a page on the portal's own address

Rendered as a page on the portal's address

Folioport

A portal where design studios share work with their clients: projects with stages, client approvals, files, conversations, share links, plans with limits, and an admin for the founder who runs every studio. Built with Claude Code from 12 plain-language messages.



The studio's dashboard: projects, approvals the studio waits for, recent activity

Folioport

Projects > Brand identity refresh

Brand identity refresh • Active

Maison Orée Due 26 October 2026 2 of 4 stages approved

A calmer, warmer identity for Maison Orée ahead of the 2027 range: new mark, palette and typography, ready for packaging and the web shop.

Stages Edit stages

- Stage 1: Discovery & brief (Approved)
- Stage 2: Concepts (Approved)
- Stage 3: Refinement (Awaiting approval)
- Stage 4: Final files (Upcoming)

Refinement Awaiting approval Withdraw request

The chosen route, refined: mark, palette and type pairing.

Download stage Share stage

Sent for approval 2 days ago. The client's main contact can approve it or ask for changes.

Files Download all Share files

- All files 11
- Discovery & brief 4
- Concepts 3
- Refinement 4
- From Maison Orée 2

Files Preview:

- Small-size test — 30 ml bottl... (41 KB · 30 Sep)
- Typography pairing.png (89 KB · 30 Sep)
- Colour palette v2.png (44 KB · 30 Sep)

Conversation Visible to Maison Orée

Everyone in the office pointed at it within seconds.

CR Camille Roussel STUDIO 6 Sep, 11:20
Wonderful. We'll refine A over the next two weeks — mostly the weight of the ring and how it behaves at small sizes.

AL Anna Lindqvist CLIENT 23 Sep, 16:05
Could we see how the mark looks on the 30 ml dropper bottle? That's the smallest thing it will go on.

ID Inès Dubois STUDIO 24 Sep, 10:30
Good call — we'll include a small-size test in the refinement round.

Inès Dubois sent Refinement for approval 30 Sep, 15:30

Refined sun mark, the final palette and the type pairing. Please look at the palette on screen and on the printed swatches we posted to you on Monday.

AL Anna Lindqvist CLIENT 1 Oct, 17:45
Thank you! The swatches arrived. Sharing everything with Paul tomorrow morning, we'll

Agency plan
Storage < 1 MB / 250 GB

CR Camille Roussel
camille@atelierbrume.example

A project: stages, files and the conversation with the client

Folioport Your projects Client portal

All studios A Atelier Brume K Kettle & Kern

Good evening, Anna

You work with 2 studios. Each one's projects are kept separately below.

A Atelier Brume
Projects for Maison Orée

Waiting for your approval 1

Brand identity refresh
Refinement
Sent 2 days ago Awaiting approval Review

Your projects

MO Brand identity refresh
Maison Orée
Refinement Awaiting approval 2/4
Due 26 Oct

MO Holiday gift box 2026
Maison Orée
All stages approved 4/4

Notifications 4 unread Mark all as read

- Nell Okoro sent Display concepts for approval
Kettle & Kern · Boutique display & shelf talkers · ...
- Nell Okoro shared Counter display — two concepts.jpg
Kettle & Kern · Boutique display & shelf talkers · ...
- Inès Dubois sent Refinement for approval
Atelier Brume · Brand identity refresh · 2 days ago
- Inès Dubois shared 4 files
Atelier Brume · Brand identity refresh · 2 days ago
- Nell Okoro sent Brief for approval
Kettle & Kern · Boutique display & shelf talkers · 16 d...
- Théo Marchand shared 3 files
Atelier Brume · Brand identity refresh · 1 month ago
- Camille Roussel sent Concepts for approval
Atelier Brume · Brand identity refresh · 1 month ago

Your copy

Download everything Maison Orée has with Atelier Brume: every project's files, the conversations and every approval, in one zip.

Download everything

Latest updates

AL Anna Lindqvist commented: "Thank you! The swatches arrived. Sharing..."

The client's side: projects with each studio, approvals and notifications

All findings

#	SEVERITY	FINDING	AREA	AFFECTS	STATUS
1	HIGH	A client's people could read the studio's private notes about them	Access	Studio and its clients	Fixed
2	HIGH	The studio could approve a stage in the client's name	Approvals	Clients	Fixed
3	HIGH	The studio could rewrite a decision the client had already made	Approvals	Clients	Fixed
4	HIGH	A file's address kept opening after access was gone	Files	Studio and its clients	Fixed
5	HIGH	An uploaded HTML or SVG file opened as a page on the portal's own address	Files	Everyone who opens a file	Fixed
6	MEDIUM	Freelancers and clients could read the studio's plan, trial and storage	Access	Studio	Partly
7	MEDIUM	The Free plan's two-project limit could be passed	Plans	Studio	Fixed
8	MEDIUM	Anyone could post activity that never happened	Activity	Everyone in a project	Fixed
9	MEDIUM	Names and dates on records could be someone else's	Records	Everyone	Partly
10	MEDIUM	Records of client decisions could be deleted in read-only projects	Approvals	Clients	Fixed
11	MEDIUM	People who had left could still delete their messages	Messages	Studio and its clients	Fixed
12	MEDIUM	The studio could pass its own file off as the client's	Files	Clients	Fixed
13	MEDIUM	Files without a record took up storage nobody could see	Files	Studio	Fixed
14	MEDIUM	A member could delete a client company outright	Clients	Studio	Fixed
15	MEDIUM	Deleting a project could stop halfway	Projects	Studio	Fixed
16	MEDIUM	A deleted project's messages stayed in the activity feed	Activity	Studio and its clients	Fixed
17	MEDIUM	A studio whose deletion stopped midway disappeared from the founder's list	Founder's admin	Founder	Fixed
18	LOW	Choosing a plan did not end the trial	Plans	Studio	Fixed
19	LOW	Share link counters counted every reload	Share links	Studio	Fixed
20	LOW	Answers told a missing link from someone else's and from a suspended studio	Share links	Anyone with a link	Fixed
21	LOW	A freelancer could read the owner's email	Access	Studio	Fixed
22	LOW	People without a seat kept working after the trial ended	Plans	Studio	Fixed
23	LOW	The team could change while the studio was suspended	Team	Studio	Fixed
24	LOW	Removing two people freed only one seat	Team	Studio	Fixed
25	LOW	A team record without a role could not be removed	Team	Studio	Fixed
26	LOW	Plan and trial changes were missing from the founder's log	Founder's admin	Founder	Partly
27	LOW	A "changes requested" message could exist without the decision	Messages	Clients	Fixed

28	LOW	People outside a studio could mark its notifications read	Notifications	Founder	Fixed
29	LOW	A client could be deleted without typing its name	Clients	Studio	Fixed

1 **HIGH** A client's people could read the studio's private notes about them

The studio keeps internal notes on each client company. The rules let the client's main contact and colleagues read the notes on their own company, signed in as themselves, from the browser.

Velo Lumen's colleague reads the studio's notes on Velo Lumen

AS RECEIVED

Allowed: the notes came back

AFTER THE FIX

Refused; the client's card no longer carries the notes

HOW TO REPRODUCE

1. Sign in as a client's colleague.
2. Read the studio's notes on the client's own company straight from the database.

THE FIX

The notes moved to a record only the team and the founder can read.

Check: signed in as the client's main contact and as a colleague, read the notes on their own company. **Fixed.** Access · affects: Studio and its clients

2 **HIGH** The studio could approve a stage in the client's name

Only the client's main contact should approve a stage or ask for changes; the builder's own notes said so. The rules let the owner, a member or a freelancer write the decision, and the client's portal showed it as the client's.

A freelancer approves the stage waiting for Velo Lumen

AS RECEIVED

Approved, shown as approved by the client

AFTER THE FIX

Refused: only the main contact decides

HOW TO REPRODUCE

1. Sign in as a freelancer on the project.
2. Write "approved" on a stage that waits for the client.

THE FIX

Only the client's main contact can write a decision on a stage.

Check: signed in as the owner, a member and a freelancer, wrote a decision on a waiting stage. **Fixed.** Approvals · affects: Clients

3 **HIGH** The studio could rewrite a decision the client had already made

After a client approved a stage or asked for changes, anyone on the studio's side could change the decision, its note, the name on it and its date. The record of what the client agreed to could not be trusted.

The owner edits a stage the client asked to change

AS RECEIVED

Rewritten to "approved", with a new date

AFTER THE FIX

Refused: a decision stays; a new round is a new request

HOW TO REPRODUCE

1. Sign in as the owner.
2. Change the decision, note or date on a stage the client already answered.

THE FIX

A decision is final; a new round starts only by sending the stage again.

Check: signed in as the owner, a member and a freelancer, rewrote a past decision. **Fixed**. Approvals · affects: Clients

4 **HIGH** A file's address kept opening after access was gone

The portal handed out file addresses that worked without signing in, for good. They kept opening after the person left the project, after the studio was suspended, and for anyone the address was forwarded to.

A file address copied before the colleague was removed

AS RECEIVED

Opens without signing in, after removal

AFTER THE FIX

Refused: every open checks who is asking

HOW TO REPRODUCE

1. Copy a file's address from the portal.
2. Remove the person from the project, or suspend the studio.
3. Open the address signed out.

THE FIX

Files are served only through a short-lived ticket checked on every request; old addresses stop working.

Check: opened saved file addresses signed out, after removal and after suspension. **Fixed**. Files · affects: Studio and its clients

5 HIGH An uploaded HTML or SVG file opened as a page on the portal's own address

A file uploaded as HTML or SVG, or HTML renamed as a picture, opened as a web page on the portal's address, both from a share link and in the preview. A page like that can act as the person who opens it.

An .svg uploaded by a client, opened from a share link

AS RECEIVED

Rendered as a page on the portal's address

AFTER THE FIX

Served as a download or a plain image, in a sandbox

HOW TO REPRODUCE

1. Upload an HTML or SVG file to a project.
2. Open it from a share link or the preview.

THE FIX

Unsafe types are served only as downloads, the type is read from the content, and file answers run in a sandbox.

Check: uploaded HTML, SVG and HTML under a picture's name, then opened them by link and in the preview. **Fixed**. Files affects: Everyone who opens a file

The other findings

6 **MEDIUM** Freelancers and clients could read the studio's plan, trial and storage

WHAT HAPPENS

The studio's own record, with its plan, trial, storage, counters and the reason for a suspension, was readable by freelancers and the client's people.

HOW TO REPRODUCE

1. Sign in as a freelancer.
2. Read the studio's record.

A freelancer reads the studio record

AS RECEIVED

Plan, trial end, storage and suspension reason

AFTER THE FIX

Only what the role needs

THE FIX

The record was closed and a small public profile made for what others need.

Check: signed in as a freelancer and a client, read the studio record.

Partly fixed: A freelancer still sees the "storage full" and "no seats left" flags, and one server answer tells them a trial ended (low). Access affects: Studio

7 **MEDIUM** The Free plan's two-project limit could be passed

WHAT HAPPENS

The limit was kept by a counter, not by the actual number of active projects. Several projects created at once, or a counter written by hand, let a Free studio run more than two.

HOW TO REPRODUCE

1. Sign in as the owner of a Free studio.
2. Create several projects at once.

A Free studio creates three projects in one go

AS RECEIVED

3 active projects on Free

AFTER THE FIX

Refused past 2, counted from the projects themselves

THE FIX

The limit and the over-limit notice are counted from the actual active projects.

Check: created projects past the limit in one go and with a counter written by hand. **Fixed.** Plans affects: Studio

8 **MEDIUM** Anyone could post activity that never happened

WHAT HAPPENS

Activity records were written by the browser. Anyone in a studio could add "approved" or "sent a file" for things that never happened, into another project's feed, even with the studio suspended; the bell showed it.

HOW TO REPRODUCE

1. Sign in as a member.
2. Write an activity record with no action behind it.

A member posts "Velo Lumen approved Visual design"

AS RECEIVED

In the feed and the client's bell

AFTER THE FIX

Refused: the feed is written only with the action itself

THE FIX

The server writes the feed together with the action.

Check: wrote feed records with no action, into other feeds and while suspended. **Fixed.** Activity affects: Everyone in a project

9 MEDIUM Names and dates on records could be someone else's

WHAT HAPPENS

Messages, files, decisions and links carried the name, side and date the browser sent. Anyone could sign as another person, as the other side, or back-date a record.

HOW TO REPRODUCE

1. Sign in as anyone.
2. Write a record with another person's name or an old date.

A colleague posts a message signed "Camille Roussel, studio"

AS RECEIVED

Shown as the studio owner's message

AFTER THE FIX

Name, side and date come from the account and the clock

THE FIX

Name, side and date are taken from the account and the time of the request.

Check: wrote records with other names, sides, studio names and dates. **Partly fixed:** A name that looks the same on screen still passes with a few look-alike letters (Greek u, Cyrillic d and l) (medium), and "Strauß" counts as different from "Strauss" (low). Records · affects: Everyone

10 MEDIUM Records of client decisions could be deleted in read-only projects

WHAT HAPPENS

In projects marked read-only the owner could delete the client's decision records and stages that carried decisions.

HOW TO REPRODUCE

1. Sign in as the owner.
2. Delete a decision or a decided stage in a read-only project.

The owner deletes an approved stage of a completed project

AS RECEIVED

Deleted, with the client's decision

AFTER THE FIX

Kept: removed only with the whole project

THE FIX

Decision records and decided stages stay until the whole project is deleted.

Check: deleted decisions and decided stages in read-only projects. **Fixed.** Approvals · affects: Clients

11 MEDIUM People who had left could still delete their messages

WHAT HAPPENS

Deleting your own message did not check current access: it worked after leaving the team or the client's company, and with the studio suspended.

HOW TO REPRODUCE

1. Remove a person from the project.
2. Delete their message as them.

A removed colleague deletes an old message

AS RECEIVED

Deleted after removal

AFTER THE FIX

Refused without current access

THE FIX

Deleting a message needs current access and an open studio.

Check: deleted own messages after leaving and while suspended. **Fixed.** Messages · affects: Studio and its clients

12 MEDIUM The studio could pass its own file off as the client's

WHAT HAPPENS

A member could overwrite a file the client had sent; the file kept its "from the client" mark.

HOW TO REPRODUCE

1. Sign in as a member.
2. Upload over a file the client sent, at the same address.

A member overwrites a client's upload

AS RECEIVED

New content, still marked "from Velo Lumen"

AFTER THE FIX

Refused: no file can be overwritten

THE FIX

Storage refuses to overwrite or replace any existing file.

Check: overwrote client files, also by deleting and re-uploading the bytes. **Fixed**. Files · affects: Clients

13 MEDIUM Files without a record took up storage nobody could see

WHAT HAPPENS

Bytes could be uploaded without a file record. They counted towards the studio's storage, but the studio could not see or delete them.

HOW TO REPRODUCE

1. Sign in as a client's colleague.
2. Upload straight to storage without a record.

A colleague uploads bytes with no record

AS RECEIVED

Storage used, nothing to delete

AFTER THE FIX

Refused: a file needs its record first

THE FIX

Storage accepts a file only for an existing record of the same person.

Check: uploaded bytes without records and watched the storage count. **Fixed**. Files · affects: Studio

14 MEDIUM A member could delete a client company outright

WHAT HAPPENS

A member could delete a client's card directly. People's access and projects stayed behind, and the owner's own delete then failed.

HOW TO REPRODUCE

1. Sign in as a member.
2. Delete a client's card from the database.

A member deletes Velo Lumen's card

AS RECEIVED

Card gone; access and projects left over

AFTER THE FIX

Only the owner deletes a client, with everything that belongs to it

THE FIX

Only the owner deletes a client, together with access, invitations and projects.

Check: deleted client cards as a member. **Fixed**. Clients · affects: Studio

15 **MEDIUM** Deleting a project could stop halfway

WHAT HAPPENS

If anyone from the client had written in the conversation, deleting the project failed after its files were already erased; the records of the files stayed.

HOW TO REPRODUCE

1. Sign in as the owner.
2. Delete a project where the client has written.

The owner deletes a project with client messages

AS RECEIVED

Files erased, delete refused, records left

AFTER THE FIX

Deleted whole, or nothing erased

THE FIX

A project is deleted whole; on refusal nothing is erased.

Check: deleted projects with client messages. **Fixed**. Projects · affects: Studio

16 **MEDIUM** A deleted project's messages stayed in the activity feed

WHAT HAPPENS

After a project was deleted, its feed records, with the conversation's text, stayed visible to the team and the client.

HOW TO REPRODUCE

1. Delete a project with a conversation.
2. Open the activity feed.

The feed after deleting a project

AS RECEIVED

Messages of the deleted project still shown

AFTER THE FIX

Its feed records go with it

THE FIX

Deleting a project removes its feed records.

Check: deleted projects and read the feed. **Fixed**. Activity · affects: Studio and its clients

17 **MEDIUM** A studio whose deletion stopped midway disappeared from the founder's list

WHAT HAPPENS

If a studio's deletion was interrupted, the studio vanished from the founder's admin while its data stayed.

HOW TO REPRODUCE

1. Start deleting a studio and interrupt it.
2. Open the founder's list.

A studio with an interrupted deletion

AS RECEIVED

Missing from the founder's list

AFTER THE FIX

Listed, marked as being deleted

THE FIX

The founder's list shows every studio, including those being deleted.

Check: interrupted a deletion and read the founder's list. **Fixed**. Founder's admin · affects: Founder

18 **LOW** Choosing a plan did not end the trial

WHAT HAPPENS

An owner on a trial who picked a plan kept the trial running alongside it.

HOW TO REPRODUCE

1. Start a trial.
2. Pick a plan.

The owner picks Agency during a trial

AS RECEIVED

Agency with the trial still on

AFTER THE FIX

Picking a plan ends the trial

THE FIX

Changing the plan always ends the trial.

Check: picked a plan during a trial.
Fixed. Plans · affects: Studio

19 **LOW** Share link counters counted every reload

WHAT HAPPENS

Each repeated request counted as a new open, so the studio saw inflated numbers.

HOW TO REPRODUCE

1. Open a share link.
2. Reload it.

One person reloads a link five times

AS RECEIVED

5 opens

AFTER THE FIX

1 open

THE FIX

Repeated opens within a short time are not counted; abuse protection is a setting for production.

Check: repeated requests to share links. **Fixed.** Share links · affects: Studio

20 **LOW** Answers told a missing link from someone else's and from a suspended studio

WHAT HAPPENS

"Doesn't exist", "not yours" and "suspended" got different answers, so a stranger could learn which links existed and which studios were suspended.

HOW TO REPRODUCE

1. Open a made-up link code.
2. Open a real one from a suspended studio.

Three link codes: made up, real, suspended studio

AS RECEIVED

Three different answers

AFTER THE FIX

One and the same refusal

THE FIX

One answer for all three cases.

Check: compared answers for made-up, foreign and suspended links. **Fixed.** Share links · affects: Anyone with a link

21 **LOW** A freelancer could read the owner's email

WHAT HAPPENS

The owner's team record, with the email, was readable by freelancers.

HOW TO REPRODUCE

1. Sign in as a freelancer.
2. Read the owner's team record.

A freelancer reads the team list

AS RECEIVED

The owner's email

AFTER THE FIX

Names of people on their project only

THE FIX

Freelancers see only the names of people on their project.

Check: read team records as a freelancer. **Fixed.** Access · affects: Studio

22 LOW People without a seat kept working after the trial ended

WHAT HAPPENS

Until the server recorded the end of a trial, people over the Free plan's seats kept working.

HOW TO REPRODUCE

1. Let a trial run out with more people than Free allows.
2. Work as the extra person.

The day a trial ends with 3 people

AS RECEIVED

All 3 keep working

AFTER THE FIX

Seats counted as Free at once

THE FIX

Seats are counted as Free as soon as the trial ends.

Check: worked as an extra person after the trial ended. **Fixed.** Plans · affects: Studio

23 LOW The team could change while the studio was suspended

WHAT HAPPENS

During a suspension people could leave and join by invitation.

HOW TO REPRODUCE

1. Suspend a studio.
2. Leave or accept an invitation.

A member leaves a suspended studio

AS RECEIVED

Left

AFTER THE FIX

Team frozen while suspended

THE FIX

The team does not change during a suspension.

Check: left and joined while suspended. **Fixed.** Team · affects: Studio

24 LOW Removing two people freed only one seat

WHAT HAPPENS

Removing several people at once moved the seat counter by one.

HOW TO REPRODUCE

1. Remove two people at once.
2. Look at the seat counter.

The owner removes two people

AS RECEIVED

Seat counter -1

AFTER THE FIX

Seat counter -2

THE FIX

The counter moves by the number of people removed.

Check: removed several people at once. **Fixed.** Team · affects: Studio

25 LOW A team record without a role could not be removed

WHAT HAPPENS

A record without a role was stuck: nobody could remove it.

HOW TO REPRODUCE

1. Create a team record without a role.
2. Try to remove it.

A broken team record

AS RECEIVED

Can't be removed

AFTER THE FIX

Removed like a member's

THE FIX

A record without a role is removed like a member's.

Check: removed records without a role. **Fixed.** Team · affects: Studio

26 LOW Plan and trial changes were missing from the founder's log

WHAT HAPPENS

An owner's choice of plan was not logged, and ending a trial was logged as "automatic" with no name.

HOW TO REPRODUCE

1. Pick a plan as the owner.
2. Open the founder's log.

The owner picks a plan

AS RECEIVED

Nothing in the log

AFTER THE FIX

Logged by the server, with who did it

THE FIX

The server logs every plan and trial change with who made it.

Check: changed plans and trials and read the log. **Partly fixed**: When the founder changes the plan during a trial, the log doesn't say the trial ended (low). Founder's admin · affects: Founder

27 LOW A "changes requested" message could exist without the decision

WHAT HAPPENS

The client's main contact could add the message that goes with a decision without making the decision.

HOW TO REPRODUCE

1. Sign in as the main contact.
2. Write the decision message on its own.

A decision message alone

AS RECEIVED

Message in the thread, stage unchanged

AFTER THE FIX

Accepted only with the decision

THE FIX

The message is accepted only together with the decision.

Check: wrote decision messages alone. **Fixed**. Messages · affects: Clients

28 LOW People outside a studio could mark its notifications read

WHAT HAPPENS

The founder and strangers could write "read" marks.

HOW TO REPRODUCE

1. Sign in as someone outside the studio.
2. Write a read mark.

A stranger marks notifications read

AS RECEIVED

Accepted

AFTER THE FIX

Refused

THE FIX

Only people with a studio or client access write read marks.

Check: wrote read marks from outside. **Fixed**. Notifications · affects: Founder

29 LOW A client could be deleted without typing its name

WHAT HAPPENS

Deleting a client for good asked to type its name, except when it had no projects.

HOW TO REPRODUCE

1. Open a client with no projects.
2. Delete it for good.

Deleting a client with no projects

AS RECEIVED

Deleted on one click

AFTER THE FIX

Name typed first, always

THE FIX

Deleting for good always asks for the client's name.

Check: deleted clients with and without projects. **Fixed**. Clients · affects: Studio

Brought or shown by the fixes

Fixes change code, and each round was checked again for what it broke. These came up in those checks and are not among the 29.

HIGH	Moving a project to another client left the old client's share links working, showing files added for the new client.	Fixed
HIGH	Names with a capital letter outside Latin ("Мария Смирнова", "Émile Durand") could no longer sign up or accept an invitation.	Fixed
MEDIUM	After a project moved, the new client's main contact could delete files the old client had sent.	Left: the owner's choice
MEDIUM	An owner could delete their account while their studio was half-deleted, leaving it without an owner.	Fixed
MEDIUM	"Add client" on the Clients page stopped working.	Fixed
MEDIUM	Anyone signed in could ask whether a person with a given name was in a studio.	Partly: the main contact can still ask by inviting themselves
MEDIUM	The update script for existing data stopped on an old name with a slash and skipped the next studios.	Fixed
MEDIUM	An old permission for a name (over an hour) let a person join under a name someone else had taken.	Open
LOW	Six smaller ones fixed: an over-full plan accepted, clients' own contacts hidden from them, a deleted message's text left in the feed, an endless spinner, old projects signed by the wrong person, a name with a no-break space refused.	Fixed
LOW	A name stays reserved after its person leaves; empty files can't be uploaded; the founder's numbers count file records without bytes; a client can't send a file into a completed project; one name check closes the name for an hour; nobody can change their own name in a studio.	Open

Only on the real Firebase

The portal was then put on a real Firebase project and checked again, signed out and by hand in all four roles. These did not show on the local copy.

-	Every upload was refused: the storage rules read more records than Firebase allows in one check.	Fixed
-	An uploaded file would never have shown up: the server waited for a second upload event that only the local copy sends.	Fixed
-	The founder's admin failed: a database index was missing.	Fixed
-	A file a client sent hid behind a filter, so it looked as if the upload hadn't worked.	Fixed
LOW	Server functions take requests from any website (they still need the person's sign-in).	Open
LOW	Share link counters have no protection against automated opening (on the demo they reset every night).	Open
LOW	localhost was still allowed to sign in to the live project.	Fixed

Requirements the founder changed

Places where the builder made a reasonable choice and the founder later decided otherwise. They were changed too, and they are not counted as mistakes.

-	The client's main contact sees and changes only their own share links.	Done
-	"Your copy" for the client's main contact works while the studio is suspended.	Done
-	New share links can be made in read-only projects.	Done
-	Share links can be deleted by whoever can turn them off.	Done
-	The owner can delete any ordinary message in the studio.	Done
-	The client's main contact can delete files sent by their colleagues.	Done
-	A freelancer can't change a project's name, description or due date.	Done
-	The team can move a project to another client.	Done
-	A share link's page doesn't show the client's company.	Done
-	Pending team invitations are visible only to the owner and the founder.	Done
-	Pending invitations count against free seats.	Done
-	The founder doesn't create studios or join teams; a client's people don't join the studio's team.	Done

Checked and fine

- Signed out, the database, file storage and server functions refuse every read and write, on the local copy and live.
- A share link gives only its own files; turned-off, expired and suspended studios' links don't open.
- The live pages match the checked build file for file and carry only public settings: no private keys, no source maps.
- Sign-in by email link for unknown addresses is off, and password reset doesn't reveal whether an account exists.

Left to the founder

- 3 medium, each needing deliberate odd steps: look-alike letters in a name, the main contact asking about names by inviting themselves, an hour-old name permission.
- The low items marked Open above and the rest of the 3 partly fixed.
- Before real studios: App Check and rate limits on server functions and share links, functions answering only the portal's own address, real email for invitations, payments, legal pages, backups and alerts.

How it was checked

- The founder's rules written down first: for every person in the portal, what they may see and change in each part of it; the founder decided the unclear cases.
- Each rule tried as that person on a local copy with test data, straight against the database, file storage and server functions, not only through the pages.
- Fixes sent to the builder in plain words, in three rounds; each round checked again for what it fixed and what it broke.
- Then the portal was put on a real Firebase project and checked again there.

Limits

- One portal, built once: the numbers describe this portal, not a rate for such apps.

- Two people racing for the last seat or project at the same moment was not checked: the local copy does not run truly in parallel.
- The live check signed in only with the four demo logins; a stranger's account could not be created there.
- Each finding shows one example; a check usually covered every role the rule applies to.

Sample engagement: the portal and its studios are fictional and hold test data; it was built with Claude Code for this case; every finding and fix is a real run.