

CODE REVIEW · PR #1842

Workspace export needs an ownership check

One blocking security issue, two reliability findings, and a focused verification plan.

VERDICT

Changes required

1 blocker

FILES REVIEWED

14

+612 / -88

FINDINGS

3

evidence-linked

TESTS REQUESTED

4

targeted

EXECUTIVE READ

The export endpoint accepts a workspace identifier from the request and passes it to the job layer without proving that the authenticated user belongs to that workspace. This creates a cross-workspace access risk.

01

BLOCKER · Ownership

routes/exports.ts:88
uses body.workspaceId
after authentication

02

HIGH · Retry duplication

jobs/export.ts:142
creates a new object
key on each retry. Use

03

MEDIUM · Unbounded selection

The request can select
every artifact without

CODE REVIEW · PR #1842

Evidence, decisions, and a usable handoff

The complete file keeps the working structure editable and the review points visible.

TEST	EXPECTED RESULT	LEVEL	STATUS
Other workspace ID	403 before job creation	Integration	Required
Valid member	Export created	Integration	Required
Retry same request	One object key	Worker	Required
Over size cap	Validation error	Route	Required

DECISION / NEXT REVIEW

Block merge until workspace ownership is enforced and the four focused regression tests pass.

QUALITY NOTE

Illustrative sample · fictional company and data. Values, names, and links in this sample must not be treated as production facts.