FINETIC TRUST CENTRE

RELEASE SECURITY EVIDENCE

Finetic v0.1.92

A readable companion to the raw CycloneDX inventory, Trivy vulnerability feed, release manifest and application penetration-test record.

EVIDENCE-BACKED RESULT

35/35 application checks passed; no fixable High or Critical package records reported.

ASSESSMENT

FIN-REL-2026-07-28

PUBLISHED

28 July 2026

SCOPE

Published Linux amd64 and arm64 preview image

EVIDENCE CLASS

Owner-authorised first-party assessment

Decision summary

> **This is evidence, not certification.**
> This report is an owner-authorised first-party assessment. It does not prove that Finetic is vulnerability-free and should not be described as an independent security audit.

RELEASE TESTS	APPLICATION CHECKS	SBOM INVENTORY	FIXABLE HIGH / CRITICAL
460	**35**	**428**	**0**
passed · 0 failed	of 35 passed	components	scanner records

QUESTION	PUBLISHED EVIDENCE
Which exact image was assessed?	OCI index `sha256:f755291c2e21c6e91548853b8e2a4a02bc18880b40fd6fe59f0383b7c447923d`, produced from source revision `b456ca9f4e51d41f1aa392968b7fa01bb3d8e149`.
What software is present?	A CycloneDX inventory of 428 components accompanies this report as raw JSON.
What did the package scanner report?	718 package-to-advisory records. None had a vendor-provided fixed version in the installed distribution at scan time.
Was the application boundary tested?	35/35 checks passed across anonymous, administrator and restricted-user flows.
Were embedded secrets found?	0 findings in the published image secret scan.

Vulnerability results, without hiding inconvenient data

Trivy reported 718 package-to-advisory records: 23 Critical, 89 High, 223 Medium, 228 Low and 155 Unknown. These counts include duplicate relationships across related packages and advisories for which the installed Debian distribution currently provides no fixed version.

Zero fixable High or Critical records does not mean zero risk. A package scan compares versions with vulnerability feeds. It does not establish whether a vulnerable function is reachable, whether an advisory is disputed, or whether an unreported vulnerability exists. The complete unfiltered scanner output remains available beside this report.

Application-boundary coverage

- Unauthenticated application boundary and protected administrator routes.
- Initial administrator bootstrap, session rotation and cross-site request-forgery controls.
- Restricted household-user authorization.

- Selected injection, parser, CORS, upload, SSRF, media authorization, artifact-exposure and body-limit checks.

Application checks

ID	AREA	RESULT	OBSERVED TEST
PT-001	release identity	PASS	The running candidate reports v0.1.92.
PT-002	browser boundary	PASS	The HTML shell supplies restrictive browser security headers and suppresses framework disclosure.
PT-003	privacy	PASS	The public preview status omits installation, customer, payment, token, and lease identifiers.
PT-004	session	PASS	Anonymous application sessions use an opaque cookie and a separate CSRF token.
PT-005	authorization	PASS	A request without an application session cannot read /api/system/health.
PT-006	authorization	PASS	A request without an application session cannot read /api/auth/users.
PT-007	authorization	PASS	A request without an application session cannot read /api/system/backups.
PT-008	authorization	PASS	A request without an application session cannot read /api/native/diagnostics.
PT-009	authorization	PASS	A request without an application session cannot read /api/analytics/export.
PT-010	authorization	PASS	An anonymous application session still cannot read administrator health data.
PT-011	csrf	PASS	Initial administrator creation is rejected without the session CSRF token.
PT-012	bootstrap	PASS	The first administrator is created only through the session-bound bootstrap flow and the session identifier rotates.
PT-013	bootstrap	PASS	A second client cannot bootstrap another initial administrator.
PT-014	authorization	PASS	The authenticated administrator can read system health.
PT-015	csrf	PASS	An authenticated mutation without CSRF is rejected.
PT-016	csrf	PASS	A CSRF token issued to another session cannot authorize an administrator mutation.
PT-017	session	PASS	A forged session cookie does not grant access.
PT-018	injection	PASS	SQL-style login input does not authenticate.
PT-019	injection	PASS	Object/operator login input does not authenticate.
PT-021	role boundary	PASS	An administrator can create a restricted household account.
PT-022	role boundary	PASS	A restricted household account cannot list or manage users.
PT-020	rate limiting	PASS	Repeated invalid sign-ins are throttled without revealing whether a username exists.
PT-023	body limits	PASS	A 17 MiB JSON request is rejected before application processing.
PT-024	upload boundary	PASS	SVG avatar payloads are rejected rather than interpreted as active content.

ID	AREA	RESULT	OBSERVED TEST
PT-025	ssrf boundary	PASS	Metadata artwork proxying rejects a loopback URL.
PT-026	artifact exposure	PASS	/.env does not disclose a source or configuration artifact.
PT-027	artifact exposure	PASS	/.git/config does not disclose a source or configuration artifact.
PT-028	artifact exposure	PASS	/server.ts does not disclose a source or configuration artifact.
PT-029	artifact exposure	PASS	/dist/server.cjs.map does not disclose a source or configuration artifact.
PT-030	cors	PASS	A hostile web origin is not granted cross-origin credential access.
PT-031	licensing boundary	PASS	Commercial billing remains disabled in the public-preview runtime.
PT-032	media authorization	PASS	An unsigned native media route cannot read a guessed media identifier.
PT-033	guest capability	PASS	A guessed guest-share token discloses no media.
PT-034	http parser	PASS	A CL.TE request-smuggling probe is rejected without serving a second protected response.
PT-035	websocket/sse	PASS	An unauthenticated WebSocket upgrade to administrator events is not accepted.

Limitations

- The application assessment and release evidence are first-party, not independent certification.
- The published vulnerability report is a package inventory comparison and does not prove or disprove exploitability.
- The amd64 published image was rescanned directly; the arm64 image was produced from the same context by the attested multi-platform workflow.
- Ten fixture-dependent media tests were explicitly skipped because their external test corpus was not mounted into the isolated release gate.

Raw evidence and integrity

The Trust Centre retains machine-readable sources for independent inspection and automation. Paths are relative to **https://youngstudio.uk**.

CYCLONEDX SBOM

`/trust/releases/0.1.92/finetic-0.1.92-sbom.cdx.json`

`SHA-256 befe7713c79e72e7d6dd7097623ccafa8e5d70b5d8b37ba21d2df4eabac8cea0`

TRIVY VULNERABILITY REPORT

/trust/releases/0.1.92/finetic-0.1.92-vulnerability-report.json

SHA-256 1bacd28f9b60555a1e060915ca512e09fe6a3e4e54984a51c575c7c487d1fdc0

APPLICATION ASSESSMENT

/trust/assessments/finetic-0.1.92-application-pentest.json

SHA-256 e109959dc2da0e6f15e25708e6faaaf6719c27a2627eac7fba35de650443d398

IMMUTABLE OCI IMAGE

ghcr.io/360john360/finetic@sha256:f755291c2e21c6e91548853b8e2a4a02bc18880b40fd6fe59f0383b7c447923d

Finetic Trust Centre · FIN-REL-2026-07-28 · Public evidence at youngstudio.uk/trust/