

FalseGreen Verification Report

INSUFFICIENT EVIDENCE

The required evidence could not be established for the exact source tree verified by FalseGreen.

This does not prove universal correctness. Assurance is limited to the explicit formal properties, assumptions, models, summaries, and scope recorded in this report.

This is record 5 of this Job, re-issued from the evidence its run stored. The verdict was decided by the Job itself, under the rules that run shipped with (the policy digest and witness versions in the Security section); re-issuing re-presents the evidence and NEVER re-decides it. Record 1 stays immutable.

THE WORK

Job	520d2155-f6c4-43c6-953c-1829b6dd5cc3
Language	rust
Toolchain	rustc 1.99.0 (rustc) (1.99.0)
Verifier environment	rust - rustc 1.99.0 (rustc) (1.99.0)

THE FROZEN BOUNDARY

Source tree	e8006c3f8784d4f439eff39ce6354cbd256c987bb17243c3a45c57f92726d25d
Contract SHA-256	e5994e7c7513719eb7bbc8e71819af12bee6973055b2cb3c5f458f5e4b1f12b7
Criteria SHA-256	d34458a3179d885efdb609b2971179f2f58aabd17860731a25031594a5d329cb
Criteria	3 / 3 PASSED

WHAT FALSEGREEN DID

Attempts	7
Duration	27.ls
Report schema	v13
Report record	5 (re-issued 2026-10-26)
Signed	2026-10-26 05:58:17 UTC

Contract (frozen)

(contract embedding unavailable — schema v2 report)

Plan (frozen)

Objective

Re-smoke FalseGreen 0.10.0 end-to-end on the ledger demo: the falsegreen.toml invariant set captures every implemented behavior claim (DE SIGN.md sections 1-10 + README exit-code contract + threat-model scope), the baseline run is accepted with all five security witnesses carrying real evidence, and three dedicated break workspaces prove the SCA (#10), SAST (#14), and secret (#12) classes now actually gate the verdict; the HTML/PDF report parity (#13) and the invariant carry (#7) are re-observed on the signed artifacts.

Plan digest

fc5315fcb0033384496bdcf05184fb8aaf2768ad689e9f045a968c93cd8aa2bf

Work items

7

Work items, in dependency order:

Work item	Outcome	Depends on	Omission risk
contract-invariants	falsegreen.toml carries ten [[invariant]] sections mapping 1:1 to the implemented behavior: canonical form, validation, hash chain, append-only store, Merkle/Ed25519 seals, compaction, policy evaluation, exit-code precedence, export/import round-trips, and the threat-model scope	-	-
behavior-tests	the workspace test suite (run by the frozen contract criteria) pins each behavior the invariants claim	-	-
green-baseline	one accepted Job over the clean tree with real (never-empty) evidence from all five witnesses	contract-invariants, behavior-tests	-
sca-break	a pinned CRITICAL advisory (smallvec 1.6.0) yields a signed critical finding and a failed verdict	green-baseline	-
sast-break	a payload matching a SARIF rule whose defaultConfiguration.level is error yields a high finding and a failed verdict	green-baseline	-
secret-break	a planted below-DO-threshold secret token in-tree is found by the file-scanning gitleaks witness and fails the secret class	green-baseline	-
inventory-evidence	supply_chain and license classes carry real SBOM facts (component rows + license facts) and are recorded severity-less — they inform, never severity-gate	green-baseline	-

Acceptance conditions, and the evidence that decides each:

Scope	Condition	Evidence
contract-invariants	every DESIGN.md section and the README exit-code contract is claimed by exactly one invariant: the signed	inspection

Evidence manifest

ATTEMPT 1 - PASSED - 2026-10-21 17:51:56 UTC - WALL 42.2S

source sha256: c29cc78fa67a8ad57fe6b25c3b42fd29f5d6cfb4d9fcfcf06263ce8e4686811e

env sha256: f94232bb359ccba42a8dbf82c6ce4ee702015af403e42ac2920c636e91ab6552

ATTEMPT 2 - PASSED - 2026-10-21 17:54:42 UTC - WALL 29.2S

source sha256: 4db442db0b30ff15694e4c46da2b8be04d9c388e312903c3b3b69144543dcccdd

env sha256: f94232bb359ccba42a8dbf82c6ce4ee702015af403e42ac2920c636e91ab6552

ATTEMPT 3 - PASSED - 2026-10-21 17:55:50 UTC - WALL 29.2S

source sha256: bdfbca2b16dfbe856fb4b96879974d70b50882791902d790ae24e85e8e8640b7

env sha256: f94232bb359ccba42a8dbf82c6ce4ee702015af403e42ac2920c636e91ab6552

ATTEMPT 4 - PASSED - 2026-10-21 17:57:04 UTC - WALL 34.8S

source sha256: 0f803b6e96e7060ae83e7e589cfac7c1eda124872402cc22dcd2ee43df2c0067

env sha256: f94232bb359ccba42a8dbf82c6ce4ee702015af403e42ac2920c636e91ab6552

ATTEMPT 5 - PASSED - 2026-10-21 17:59:09 UTC - WALL 28.5S

source sha256: 0d0034d14e791fcb13b7db8875d18e7f884f2a4da9c393040ced7f5d2f34178e

env sha256: f94232bb359ccba42a8dbf82c6ce4ee702015af403e42ac2920c636e91ab6552

ATTEMPT 6 - PASSED - 2026-10-21 18:00:14 UTC - WALL 28.0S

source sha256: 0cb7c13b10d359ba5965e6dc9285a64043fa73a95985c7facde439fecdb6b1e86

env sha256: f94232bb359ccba42a8dbf82c6ce4ee702015af403e42ac2920c636e91ab6552

ATTEMPT 7 - PASSED - 2026-10-21 18:01:22 UTC - WALL 29.4S

source sha256: de6b2e18c7c9cf41b4b6389af49aac4728bb34db020bfe3fa770ceb6b17f6872

env sha256: f94232bb359ccba42a8dbf82c6ce4ee702015af403e42ac2920c636e91ab6552

ATTEMPT 8 - PASSED - - WALL 27.1S

source sha256: not recorded

env sha256: f94232bb359ccba42a8dbf82c6ce4ee702015af403e42ac2920c636e91ab6552

Security Findings

The bar these findings are judged against (the frozen policy): **fail on:** critical, high · **unknown severity:** insufficient_evidence.

Finding	Subject	Class	Severity	State
5046f75b49bcc91e972 fe6e37dff89bd730aca c66b5c0835cdf5961 0c6a9a5 osv/RUSTSEC-2021-0003	pkg:crates.io/smallvec@1.6.0	Dependency/SCA	high	OPEN
538efbca6ab37d1de72 06475fd690628e0d69c bb5b3b1d27719f69b6c aaf43f7 osv/GHSA-43w2-9j62-hq99	pkg:crates.io/smallvec@1.6.0	Dependency/SCA	high	OPEN

The full SBOM and VEX are in the signed JSON report.

JSON report: <https://falsegreen.com/report/520d2155-f6c4-43c6-953c-l829b6dd5cc3/json>

Invariant Checks

no invariants (machine-discharged propositions) were frozen for this Job

Security

Policy	falsegreen-platform
Policy digest	372d3c74758acb113c1bef14b20b08b326a7703dd57d943247de6541743c0fad
Result	NOT SATISFIED

Evidence class	Required	Status	Reasons
Dependency/SCA	yes	FAIL	vulnerability snapshot is stale (observed 2026-10-21T17:30:12Z, freshness bound 24h); finding 5046f75b49bcc91e972fe6e37dff89bd730acac66b5c0835cdf5a59610c6a9a5 severity 'high' is frozen-fail (osv/RUSTSEC-2021-0003); finding 538efbca6ab37d1de7206475fd690628e0d69cbb5b3b1d27719f69b6caaf43f7 severity 'high' is frozen-fail (osv/GHSA-43w2-9j62-hq99)
Static analysis	yes	PASS	
Secrets	yes	PASS	
Supply chain	yes	PASS	75 components inventoried (evidence, in the signed JSON report)
License policy	yes	NOT ASSESSED	no licence policy frozen — the licence facts are inventory, nothing was asserted · 73 licence facts inventoried (evidence, in the signed JSON report)

How to read this table. **PASS** — the evidence was collected and nothing in it violated the frozen policy. **FAIL** — the evidence showed a violation the policy forbids; that alone fails the Job. **INSUFFICIENT EVIDENCE** — the evidence could not be collected, or could not be decided for a reason outside the code (a stale snapshot, an unavailable tool, output the parser could not read). It is never a pass, and it holds the Job at *insufficient_evidence* rather than accepting it. **NOT ASSESSED** — no policy is frozen for this class, so nothing was asserted about it; the facts are recorded as inventory and the class does not hold the Job. The findings table lists only what the frozen policy **JUDGED** — a graded severity, supply-chain drift, or a licence breaking the frozen policy. Everything else the tools recorded (components, licence facts) is inventory: not a finding, counted on the class row above, kept in the signed JSON report. A finding is **OPEN** unless it is resolved, not affected, or covered by a recorded exception.

Attempt security history (the full per-attempt sections are in the signed JSON report):

Attempt	Result	Open findings	Demonstrated violations
#1	NOT SATISFIED	2	vulnerability snapshot is stale (observed 2026-10-21T17:30:12Z, freshness bound 24h); finding 5046f75b49bcc91e972fe6e37dff89bd730acac66b5c0835cdfea59610c6a9a5 severity 'high' is frozen-fail (osv/RUSTSEC-2021-0003); finding 538efbca6ab37d1de7206475fd690628e0d69cbb5b3b1d27719f69b6caaf43f7 severity 'high' is frozen-fail (osv/GHSA-43w2-9j62-hq99)
#2	NOT SATISFIED	2	vulnerability snapshot is stale (observed 2026-10-21T17:30:12Z, freshness bound 24h); finding 5046f75b49bcc91e972fe6e37dff89bd730acac66b5c0835cdfea59610c6a9a5 severity 'high' is frozen-fail (osv/RUSTSEC-2021-0003); finding 538efbca6ab37d1de7206475fd690628e0d69cbb5b3b1d27719f69b6caaf43f7 severity 'high' is frozen-fail (osv/GHSA-43w2-9j62-hq99)
#3	NOT SATISFIED	2	vulnerability snapshot is stale (observed 2026-10-21T17:30:12Z, freshness bound 24h); finding 5046f75b49bcc91e972fe6e37dff89bd730acac66b5c0835cdfea59610c6a9a5 severity 'high' is frozen-fail (osv/RUSTSEC-2021-0003); finding 538efbca6ab37d1de7206475fd690628e0d69cbb5b3b1d27719f69b6caaf43f7 severity 'high' is frozen-fail (osv/GHSA-43w2-9j62-hq99)
#4	NOT SATISFIED	2	vulnerability snapshot is stale (observed 2026-10-21T17:30:12Z, freshness bound 24h); finding 5046f75b49bcc91e972fe6e37dff89bd730acac66b5c0835cdfea59610c6a9a5 severity 'high' is frozen-fail (osv/RUSTSEC-2021-0003); finding 538efbca6ab37d1de7206475fd690628e0d69cbb5b3b1d27719f69b6caaf43f7 severity 'high' is frozen-fail (osv/GHSA-43w2-9j62-hq99)
#5	NOT SATISFIED	2	vulnerability snapshot is stale (observed 2026-10-21T17:30:12Z, freshness bound 24h); finding 5046f75b49bcc91e972fe6e37dff89bd730acac66b5c0835cdfea59610c6a9a5 severity 'high' is frozen-fail (osv/RUSTSEC-2021-0003); finding 538efbca6ab37d1de7206475fd690628e0d69cbb5b3b1d27719f69b6caaf43f7 severity 'high' is frozen-fail (osv/GHSA-43w2-9j62-hq99)

Attempt	Result	Open findings	Demonstrated violations
#6	NOT SATISFIED	2	vulnerability snapshot is stale (observed 2026-10-21T17:30:12Z, freshness bound 24h); finding 5046f75b49bcc91e972fe6e37dff89bd730acac66b5c0835cdfea59610c6a9a5 severity 'high' is frozen-fail (osv/RUSTSEC-2021-0003); finding 538efbca6ab37d1de7206475fd690628e0d69cbb5b3b1d27719f69b6caaf43f7 severity 'high' is frozen-fail (osv/GHSA-43w2-9j62-hq99)
#7	NOT SATISFIED	2	vulnerability snapshot is stale (observed 2026-10-21T17:30:12Z, freshness bound 24h); finding 5046f75b49bcc91e972fe6e37dff89bd730acac66b5c0835cdfea59610c6a9a5 severity 'high' is frozen-fail (osv/RUSTSEC-2021-0003); finding 538efbca6ab37d1de7206475fd690628e0d69cbb5b3b1d27719f69b6caaf43f7 severity 'high' is frozen-fail (osv/GHSA-43w2-9j62-hq99)

Witnesses (tool provenance)

osv-scanner 2.7.0 (Dependency/SCA) – invocation sha256:
ccd91f56f4900e7561b4ac09ffcd8f32a89fd4ee9a01d47d046ffe8a44d6b13d –
f94232bb359ccba42a8dbf82c6ce4ee702015af403e42ac2920c636e91ab6552

semgrep 1.181.0 (Static analysis) – invocation sha256:
f3dfe0ed2197c2c55812c31eb6a20c881e8fc0e28e8e6fdc69e149337e14a88f –
f94232bb359ccba42a8dbf82c6ce4ee702015af403e42ac2920c636e91ab6552

gitleaks 8.30.1 (Secrets) – invocation sha256:
497dd2010d6a321cfa4645d9c366e8d2e8bc923e320c1bed1834e7c3ec0c54e5 –
f94232bb359ccba42a8dbf82c6ce4ee702015af403e42ac2920c636e91ab6552

syft 1.54.1 (Supply chain) – invocation sha256:
22eee92de7a91a923a00982dc2fa798362f2df94202d1750cdc71125a0dddb5c –
f94232bb359ccba42a8dbf82c6ce4ee702015af403e42ac2920c636e91ab6552

dependency-manifest 1 (License policy) – invocation sha256:
41dd72d0f0c625cedddfffd7035ef794b142f250ac3553faa884b254c6bb66b42 –
f94232bb359ccba42a8dbf82c6ce4ee702015af403e42ac2920c636e91ab6552

Tools & provers used

Tool	Version	What it did in this run
osv-scanner	2.7.0	Dependency/SCA evidence witness
semgrep	1.181.0	Static analysis evidence witness
gitleaks	8.30.1	Secrets evidence witness
syft	1.54.1	Supply chain evidence witness
dependency-manifest	1	License policy evidence witness

Exports

Full content is embedded in the signed JSON report (report schema v13).

spdx-3.0 sha256:bbb47aae1a3bc88a815c3d1c5b8e0b84de6e8dc1b969bcc3bf99163a3166e8a3 embedded in the JSON report (55505 bytes)

cyclonedx-1.7 sha256:0b323f20f1fe10c6827e4e4f95eac74131f7b562796866974a89cf9e7a0ea6c7 embedded in the JSON report (26621 bytes)

cyclonedx-1.7-vex sha256:62942ce2646bffc3761f5ada87954ac7167299a394bf1632855ab300753e772a embedded in the JSON report (2153 bytes)

Signature

This report is cryptographically signed: Ed25519 over the canonical report content. The public key is embedded in the report — verification is offline and registry-free (falsegreen `verify-report`).

key id: fg-report-9fc1a2c5-134c-4ca1-a0f2-56b2d1bcde67-20261018-1

ed25519 public key: ie4eQdY1lt705aCCQz0+/192Yzc4pLQsGyVNqSKtImA=

ed25519 signature: ElwtGNIaWa+Pl93yIwHaGJFmvN7m569bNIPyjs9tF05AYA6PXBpJ1iozFt7nTeYbstLLpdcLJukLbLeBb4W0Aw==

digest: fbf0f1ad979580760474c065b21b6e3d149a77ca50a697c37717d42d7ad4f53a

This is a presentation of the signed canonical evidence (the JSON artifact). It is not an audit certificate. - FalseGreen v0.16.0