# ULMCode Report Writer

EXECUTIVE SNAPSHOT

| Total Findings | Critical | High | Medium | Low |
|---|---|---|---|---|
| 4 | 0 | 0 | 3 | 1 |

TABLE OF CONTENTS

Executive Summary

Methodology

Findings

- [FND-BP7A638K5S] CI workflow executes remote installer via curl|bash
- [FND-BWRDYG95XT] Tool permission policy blocks editing engagement artifacts (results/handoff)
- [FND-KRX5XQD0QP] CI uses TOFU ssh-keyscan and writes AUR deploy key to disk
- [FND-8PJK948RGC] Strict-isolation flags not set in current session; external skill directory present

Detection and Telemetry Notes

Remediation Plan

Primary Objective

30/60/90 Plan

- 0-30 Days
- 31-60 Days
- 61-90 Days

Validation Gates

Provenance Index

FINDINGS MATRIX

| ID | Title | Severity | Confidence |
|---|---|---|---|
| FND-BP7A638K5S | CI workflow executes remote installer via curl|bash | MEDIUM | 0.95 |
| FND-BWRDYG95XT | Tool permission policy blocks editing engagement artifacts (results/handoff) | MEDIUM | 0.9 |
| FND-KRX5XQD0QP | CI uses TOFU ssh-keyscan and writes AUR deploy key to disk | MEDIUM | 0.9 |
| FND-8PJK948RGC | Strict-isolation flags not set in current session; external skill directory pres | LOW | 0.75 |

## Executive Summary

- Session: ses_3c81e997bffeUeWcudNV7EeXJF
- Generated: 2026-02-07T11:37:31.906Z
- Total findings: 4
- Severity mix: critical=0, high=0, medium=3, low=1, info=0

## Methodology

- Authorized internal assessment with non-destructive-first posture.
- Evidence-backed validation, source traceability, and controlled execution.

## Findings

### [FND-BP7A638K5S] CI workflow executes remote installer via curl|bash

- Severity: medium
- Confidence: 0.95
- Asset: GitHub Actions workflow: .github/workflows/review.yml
- Evidence-backed statement: see source index references.

#### Impact

If the install endpoint, DNS/TLS path, or upstream hosting is compromised, an attacker can achieve arbitrary code execution in the CI runner context, potentially impacting build artifacts, secrets available to the job, and repository operations performed by the workflow.

#### Recommendation

Avoid `curl | bash` in CI. Prefer a pinned, integrity-verified install method (e.g., package manager with version pinning, checksum/signature verification, or vendoring the installer script at a pinned commit). If a script must be fetched, pin to an immutable version and verify a published checksum/signature before execution.

### [FND-BWRDYG95XT] Tool permission policy blocks editing engagement artifacts (results/handoff)

- Severity: medium
- Confidence: 0.9
- Asset: opencode cyber session tool permissions
- Evidence-backed statement: see source index references.

#### Impact

Cyber workflow audit trail can’t be maintained by subagents (cannot update results.md/handoff.md using the available editing mechanism). This can break engagement compliance requirements, reduce report quality, and prevent coordination updates from being captured in the canonical artifacts.

#### Recommendation

Adjust the runtime/tool permission policy for cyber sessions to allow editing/writing of engagement artifacts (at minimum: `handoff.md`, `agents/*/results.md`, and optionally `reports/*`), or provide a dedicated non-interactive write tool that is permitted for these paths. Ensure the permission layer distinguishes between project code edits vs. engagement-artifact updates.

### [FND-KRX5XQD0QP] CI uses TOFU ssh-keyscan and writes AUR deploy key to disk

- Severity: medium
- Confidence: 0.9
- Asset: GitHub Actions workflow: .github/workflows/publish.yml (AUR publishing)
- Evidence-backed statement: see source index references.

#### Impact

A MITM on the CI network path could feed a malicious host key during `ssh-keyscan`, enabling credential capture or malicious pushes to the AUR repo. Writing the deploy key to disk increases the blast radius if the runner is compromised during job execution.

#### Recommendation

Pin the expected AUR host key(s) (commit them in-repo or store as a protected secret) instead of `ssh-keyscan` TOFU. Prefer `ssh-agent` with an ephemeral key file and strict permissions, and consider using `known_hosts` with exact key material. Ensure secrets are least-privilege and job permissions are minimized.

### [FND-8PJK948RGC] Strict-isolation flags not set in current session; external skill directory present

- Severity: low
- Confidence: 0.75
- Asset: Operator runtime environment (local shell running cyber session)
- Evidence-backed statement: see source index references.

#### Impact

If strict-isolation mode is required for an engagement, running without the isolation flags can allow discovery/loading of skills or config outside the intended allowlist, increasing risk of skill/config leakage or unintended behavior drift between environments.

#### Recommendation

Use the isolated profile launcher (e.g., `tools/ulmcode-profile/scripts/bootstrap-ulmcode-profile.sh`) and run via the generated `ulmcode-launch.sh`, which exports `OPENCODE_DISABLE_EXTERNAL_SKILLS=1` and `OPENCODE_DISABLE_PROJECT_CONFIG=1` and pins config via `OPENCODE_CONFIG_DIR`/`OPENCODE_CONFIG`. Optionally add a startup preflight that fails closed if cyber sessions start without these flags when isolation is expected.

## Detection and Telemetry Notes

- Detection opportunities were mapped from validated exploitation paths and observed control gaps.
- Prioritize alerting and response playbooks for high-impact findings.

## Remediation Plan

# Remediation Plan

## Primary Objective

Address highest-risk finding first: [FND-BP7A638K5S] CI workflow executes remote installer via curl|bash (medium).

## 30/60/90 Plan

### 0-30 Days

### 31-60 Days

- FND-BP7A638K5S: Avoid `curl | bash` in CI. Prefer a pinned, integrity-verified install method (e.g., package manager with version pinning, checksum/signature verification, or vendoring the installer script at a pinned commit). If a script must be fetched, pin to an immutable version and verify a published checksum/signature before execution.
- FND-BWRDYG95XT: Adjust the runtime/tool permission policy for cyber sessions to allow editing/writing of engagement artifacts (at minimum: `handoff.md`, `agents/*/results.md`, and optionally `reports/*`), or provide a dedicated non-interactive write tool that is permitted for these paths. Ensure the permission layer distinguishes between project code edits vs. engagement-artifact updates.
- FND-KRX5XQD0QP: Pin the expected AUR host key(s) (commit them in-repo or store as a protected secret) instead of `ssh-keyscan` TOFU. Prefer `ssh-agent` with an ephemeral key file and strict permissions, and consider using `known_hosts` with exact key material. Ensure secrets are least-privilege and job permissions are minimized.

### 61-90 Days

- FND-8PJK948RGC: Use the isolated profile launcher (e.g., `tools/ulmcode-profile/scripts/bootstrap-ulmcode-profile.sh`) and run via the generated `ulmcode-launch.sh`, which exports `OPENCODE_DISABLE_EXTERNAL_SKILLS=1` and `OPENCODE_DISABLE_PROJECT_CONFIG=1` and pins config via `OPENCODE_CONFIG_DIR`/`OPENCODE_CONFIG`. Optionally add a startup preflight that fails closed if cyber sessions start without these flags when isolation is expected.

## Validation Gates

- Re-test all critical/high findings after remediation implementation.
- Confirm detection coverage and incident response telemetry for exploitation paths.
- Update risk register with accepted residual risk and ownership.

## Provenance Index

- SRC-001: Canonical finding log
- SRC-002: Cross-agent coordination notes
- SRC-003: Evidence root directory
- SRC-004: Subagent summarized output
- SRC-005: Subagent summarized output
- SRC-006: Subagent summarized output
- SRC-007: Subagent summarized output
- SRC-008: Subagent summarized output