CMU spiral-software

Created by Scott A Hissam, last updated less than a minute ago • 6 minute read

> **WARNING: Do not hand edit, this page is subject to automatic updates.**

- Critical and High vulnerabilities
- Critical and High maliciousCodeRisk
- Critical and High engineeringRisk
- Critical and High authorsRisk
- Critical, High, Medium, and Low licenseRisk

<table>
<tr><th>OSS Project Report</th><th>Response</th></tr>
<tr><td>Overview</td><td></td></tr>
<tr><td>Background</td><td>spiral-software/spiral-software, Public source repository for the SPIRAL project</td></tr>
<tr><td>Application or Library</td><td>Manual (ask)</td></tr>
<tr><td>Current as of</td><td>Date: 08-12-2025 (project queried 0 days ago)</td></tr>
<tr><td>OSS-P4/R Outlook</td><td>
<table>
<tr><td>Overall</td><td>Project (4.5)</td><td>Product (10.0)</td><td>Protection (3.1)</td><td>Policy (7.0)</td></tr>
<tr><td>MY Checks</td><td>Project (10.0)</td><td></td><td></td><td>Policy (10.0)</td></tr>
<tr><td>OSSF Scorecard</td><td>Project (0.7)</td><td>Product (10.0)</td><td>Protection (3.1)</td><td>Policy (3.0)</td></tr>
<tr><td>MITRE Hipcheck</td><td>Project (2.7)</td><td>Product (10.0)</td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>DOD CIO Criteria</td><td>
<table>
<tr><td>Criteria</td><td>Security (8.1)</td><td>Integrity (0.4)</td><td>Dependencies (0.0)</td><td>Malicious Actors (10.0)</td><td>Long-Term Support (3.5)</td><td>Suitability (9.5)</td></tr>
<tr><td>MY Checks</td><td></td><td></td><td></td><td></td><td>Long-Term Support (10.0)</td><td>Suitability (10.0)</td></tr>
<tr><td>OSSF Scorecard</td><td>Security (6.2)</td><td>Integrity (0.8)</td><td>Dependencies (0.0)</td><td></td><td>Long-Term Support (0.4)</td><td>Suitability (9.0)</td></tr>
<tr><td>MITRE Hipcheck</td><td>Security (10.0)</td><td>Integrity (0.0)</td><td></td><td>Malicious Actors (10.0)</td><td>Long-Term Support (0.0)</td><td></td></tr>
</table>
</td></tr>
<tr><td>Summarized Scores By CIO Criteria</td><td>
<table>
<tr><td>Criteria:</td><td>Security</td><td>Integrity</td><td>Dependencies</td><td>Malicious Actors</td><td>Long-Term Support</td><td>Suitability</td></tr>
<tr><td>MY Checks:</td><td></td><td></td><td></td><td></td><td>Project Forked(false/false)
Problem Reporting(true/true)
Project Abandoned(false/false)
Dependent Projects Abandoned(0/0)</td><td>Restrictive License(s)(0/0)</td></tr>
<tr><td>OSSF Scorecard: (higher's better) ❌ 3.2/10.0</td><td>Binary Artifacts(10/3.3)
❌Branch Protection(0/3.3)
Dangerous Workflow(10/3.3)
❌Token Permissions(0/3.3)
Vulnerabilities(10/3.3)
⚠Webhooks(NaN/3.3)</td><td>❌Code Review(2/3.3)
❌CI Tests(0/3.3)
❌Fuzzing(0/3.3)
❌SAST(0/3.3)
⚠ Packaging(NaN/3.3)
⚠Signed Releases(NaN/3.3)</td><td>❌Dependency Update Tool(0/3.3)
❌Pinned Dependencies(0/3.3)</td><td></td><td>❌Contributors(3/3.3)
❌Maintained(0/3.3)
❌CII Best Practices(0/3.3)
❌Security Policy(0/3.3)</td><td>License(9/3.3)</td></tr>
<tr><td>MITRE Hipcheck: (score ≤ threshold) ❌ INVESTIGATE risk rated as 0.75, acceptable below or equal to 0.50</td><td>Binary Artifacts(0.0/0)
Large Commits(0.0/0.02)
Malware Entropy(0.0/0)
⚠ Typosquatting(NaN/true)</td><td>❌Self Reviews(0.7/0.2)
❌Fuzz Testing(false/true)
❌Pull Reviews(1.0/0.05)</td><td></td><td>Author Affiliation(0.0/0)</td><td>❌Commit Activity(86.0/71)</td><td></td></tr>
</table>
</td></tr>
<tr><td>Security</td><td></td></tr>
<tr><td>Trusted Source(s)</td><td>Source: https://github.com/spiral-software/spiral-software
D-U-N-S Availability: Manual
Repo or Mirror: Manual</td></tr>
<tr><td>Public or Private</td><td>Visibility is: public
Private is: false</td></tr>
<tr><td>Fully Unrestricted</td><td>Read-Only: manual
Write: manual</td></tr>
<tr><td>Login Credentials</td><td>Manual</td></tr>
<tr><td>Use of Repository Protections</td><td>❌0/10 as branch protection not enabled on development/release branches
10/10 as no dangerous workflow patterns detected
❌0/10 as detected GitHub workflow tokens with excessive permissions, and
⚠ check that webhooks is configured supporting secrets not run</td></tr>
<tr><td>Large Commits</td><td>Detected no unusually large commits being 0.000 found under or at the 0.02 permitted threshold (Churn)</td></tr>
<tr><td>Obfuscated Code</td><td>Detected no unusual-looking commits being 0.0 found under or at the 0 permitted threshold (Entropy)</td></tr>
<tr><td>Binary Artifact(s)</td><td>10/10 as no binaries found in the repo with binaries potentially containing code being 0 found under or at the 0 permitted threshold</td></tr>
<tr><td>Typosquatting Risk</td><td>⚠Failed to analyze for typos - can't identify a known language</td></tr>
<tr><td>Known Vulnerabilities</td><td>10/10 as 0 existing vulnerabilities detected (open, known unfixed vulnerabilities). And no additional dependent vul(s) detected</td></tr>
<tr><td>Integrity</td><td></td></tr>
</table>

Peer Reviews	Count pending; and activity is ❌2/10 as Found 3/15 approved changesets -- score normalized to 2 with change requests often lacking approving review prior to merge with 100.000% ❌over the 5.0% threshold and commits too often applied by the author with 69.77% ❌over the 20.0% threshold
Use of Code and Security Scanners	❌0/10 as project is not fuzzed with repository ❌not receiving regular fuzz testing ❌0/10 as SAST tool is not run on all commits -- score normalized to 0, and ❌0/10 as 0 out of 13 merged PRs checked by a CI test -- score normalized to 0
Signed Commits	Manual
Cryptographically Signed Commits	38 of the last 100 commits have a valid cryptographic signature.
Cryptographically Signed Releases & Artifacts	⚠️-1/10 as no releases found, and ⚠️-1/10 as packaging workflow not detected; investigate if any such signing(s) are crytopgraphic
Dependencies	
Published Software Bill of Materials	SPDX-2.3,Tool: protobom-v0.0.0-20250805170613-cf5b071169fb+dirty,Tool: GitHub.com-Dependency-Graph Language package managers detected: 2 githubactions, 1 github
Dependencies Pinned to Version	❌0/10 as dependency not pinned by hash detected -- score normalized to 0
Dependencies Up to Date	❌No with no update tool detected; investigate if any dependencies apply to more than the pipeline
Number OSS Dependencies	Primary: Total found: 3, dependencies pulled: 3, dependencies unknown: 0 Secondary: Total found: ⚠️0, dependencies pulled: ⚠️0, dependencies unknown: 0 Tertiary and greater (Max search depth realized 1): Total found: ⚠️0, dependencies pulled: ⚠️0, dependencies unknown: 0
Number Proprietary Dependencies	Primary: Manual Secondary and tertiary: Manual
Malicious Actors	
Author(s) Known to Commit Vulnerabilities	Manual
Author(s) Known to Commit Malicious Code	Hipcheck contributors affiliations being 0 found at or under the 0 permitted threshold
Long Term Support	
Project Summary	spiral-software/spiral-software, Public source repository for the SPIRAL project
Individual or Organization	Organization Details: Name: Not Reported Company: Not Reported Bio: Not Reported Email: Not Reported Blog: Not Reported Geo: Not Reported Source: GitHub
Organization Type	Pending, see: https://api.github.com/users/spiral-software/orgs logistics database D-U-N-S code: Manual
SLSA Level	Pending: (ask)
Best Practices	❌0/10 as no effort to earn an OpenSSF best practices badge detected
Number of Abandoned Project(s)	spiral-software is not archived; 0 of the primary dependencies are abandoned; ⚠️tertiary (other) dependencies are not checked at this time
OSSF's Activity (criticality) Score (work in progress)	0.28/1.0 (higher's better)
Commits	Days since last commit: 32 days, on Fri Jul 11 20:17:02 UTC 2025, reported 0 days ago Days since first commit: 2184 days, on Tue Aug 20 18:26:20 UTC 2019, reported 0 days ago Activity: ❌0/10 with 0 commit(s) and 0 issue activity found in the last 90 days -- score normalized to 0 with most recent activity being 86 weeks ❌over the 71 week threshold
Number of Contributors	Core: Count pending Other: 4 Organizational diversity: ❌3/10 as project has 1 contributing companies or organizations -- score normalized to 3
Problem Reporting Process	Yes with 11 open issues
Vulnerability Reporting Process	❌0/10 as security policy file not detected
Suitability	
License	License: Other SPDX_ID: NOASSERTION
License Risk	No restrictive license detected Found ⚠️1 license(s) yet to be determined suitable: NOASSERTION. Detected no product or dependent license(s) detected and no impacts potentially reported from dependencies
About this report	
Created	Tue Aug 12 21:56:11 UTC 2025
Version	pubRel 250516evie (branch: publicRelease)
Analysis Source	Package SBOM: spiral-software_ghapi_sbom.json, 71bdba722fb03337a155610e9f23f8de
Analysis ID	SBOM created on 2025-08-12T21:55:32Z (complete)
Runtime	Approximately 0 minute(s) (this run), for a total of 0 minute(s) over 1 run(s)

Command line	/home/hc_user/.local/bin/scir-oss.sh -l -v -C spiral-software -G spiral-software/spiral-software -P github:sbom
Dependency and Scoring depth	1, 0
Comment/Caveats	I: config image _OSSFSC=/home/hc_user/.local/bin/scorecard I: config image _MITRHC=/home/hc_user/.local/bin/hc I: config setting _OSSSCIRsettings=/home/hc_user/.local/bin/settings I: config setting _MITRHCconfig=/home/hc_user/.local/bin/settings/hipcheck/config I: config setting _MITRHCscripts=/home/hc_user/.local/bin/settings/hipcheck/scripts I: config setting _OSSSCIRlicenseDB=/home/hc_user/.local/bin/settings/mychecks/licenseDB.json I: config setting _OSSSCIRrepoResolveDB= I: env setting _TERTIARY_BLACKLIST='pkg:npm|^npm:' W: could not determine OSSF/criticality_score version I: CA Certificate Trust Store () I: SBOM dependencies in 'github' are declared to include transitive dependencies - issue depth is 0 (change with -i) I: Thresholds for OSSF Scorecard scores set at 3.3 I: Threshold for OSSF Criticality Score set at 0.2 I: Local cache tolerance set to 2 days I: Days active tolerance set to 497 days I: Days for a new project set to 245 days I: Contributors tolerance set to 3 ids W: Some responses may require manual investigation if necessary (look for 'manual')
Powered by	OSSF/Scorecard v5.2.1, OSSF/Critical Score unknown, MITRE Hipcheck 3.4.0, grype 0.93.0 db v6.0.3 built on 2025-08-12T04:13:42Z
footnotes	****Data in this report is from public sources and with some being self-reported (e.g., emails, country of origin, names)****. **Pending/manual**: *Check requires manual intervention.* **Restrictive license**: *A license that requires code changes be openly published (i.e., copyleft).* ⚠**-1/n**: *Score could not be valued due to source data.* ⚠**NaN**: *Score could not be computed due to source data.* ⚠**n**: *Score indicated a possible risk which requires investigation.* ⚠ **not checked**: *Check is coming soon.* ❌**m/n**: *Score did not meet goals and/or thresholds.* ❌**n**: *Score did not meet goals and/or thresholds.* ❌**Yes/No**: *Score did not meet goals and/or thresholds.* ❌**true/false**: *Score did not meet goals and/or thresholds.*

Critical and High vulnerabilities

Package	Impact	Description

Critical and High maliciousCodeRisk

Package	Impact	Description

Critical and High engineeringRisk

Package	Impact	Description

Critical and High authorsRisk

Package	Impact	Description

Critical, High, Medium, and Low licenseRisk

Package	Impact	Description

> Created by pub-scir pubRel 250516evie (branch: publicRelease) on Wed Aug 13 12:55:39 UTC 2025

No labels

Terms of Use