CMU temoa

Created by Scott A Hissam, last updated less than a minute ago • 7 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

OSS Project Report	Response
Overview	
Background	TemoaProject/temoa, Tools for Energy Model Optimization and Analysis ❌ATTENTION: this is a fork of hunteke/temoa
Application or Library	Manual (ask)
Current as of	Date: 08-12-2025 (project queried 0 days ago)

OSS-P4/R Outlook					
	Overall	Project (5.0)	Product (7.5)	Protection (0.0)	Policy (1.4)
	MY Checks	Project (7.3)			Policy (0.0)
	OSSF Scorecard	Project (3.1)	Product (5.0)	Protection (0.0)	Policy (3.3)
	MITRE Hipcheck	Project (4.5)	Product (10.0)		

DOD CIO Criteria						
	Criteria	Security (6.7)	Integrity (1.9)	Dependencies (0.0)	Malicious Actors (10.0)	Long-Term Support (5.9)	Suitability (5.0)
	MY Checks					Long-Term Support (7.3)	Suitability (0.0)
	OSSF Scorecard	Security (3.3)	Integrity (3.8)	Dependencies (0.0)		Long-Term Support (1.4)	Suitability (10.0)
	MITRE Hipcheck	Security (10.0)	Integrity (0.0)		Malicious Actors (10.0)	Long-Term Support (9.0)	

Summarized Scores By CIO Criteria

Criteria:	Security	Integrity	Dependencies	Malicious Actors	Long-Term Support	Suitability
MY Checks:					❌Project Forked(true/false) Problem Reporting(true/true) Project Abandoned(false/false) Dependent Projects Abandoned(0/0)	❌Restrictive License(s)(1/0)
OSSF Scorecard: (higher's better) ❌ 2.9/10.0	Binary Artifacts(10/3.3) ❌Branch Protection(0/3.3) ⚠️Dangerous Workflow(NaN/3.3) ⚠️Token Permissions(NaN/3.3) ❌Vulnerabilities(0/3.3) ⚠️Webhooks(NaN/3.3)	Code Review(10/3.3) ❌CI Tests(0/3.3) ❌Fuzzing(0/3.3) ❌SAST(0/3.3) ⚠️Packaging(NaN/3.3) ⚠️Signed Releases(NaN/3.3)	❌Dependency Update Tool(0/3.3) ⚠️Pinned Dependencies(NaN/3.3)		Contributors(10/3.3) ❌Maintained(0/3.3) ❌CII Best Practices(0/3.3) ❌Security Policy(0/3.3)	License(10/3.3)
MITRE Hipcheck: (score ≤ threshold) ❌ INVESTIGATE risk rated as 0.55, acceptable below or equal to 0.50	Binary Artifacts(0.0/0) Large Commits(0.0/0.02) Malware Entropy(0.0/0) ⚠️Typosquatting(NaN/true)	❌Self Reviews(0.9/0.2) ❌Fuzz Testing(false/true) ❌Pull Reviews(1.0/0.05)		Author Affiliation(0.0/0)	Commit Activity(7.0/71)	

Security	
Trusted Source(s)	Source: https://github.com/TemoaProject/temoa D-U-N-S Availability: Manual Repo or Mirror: Manual
Public or Private	Visibility is: public Private is: false
Fully Unrestricted	Read-Only: manual Write: manual
Login Credentials	Manual
Use of Repository Protections	❌0/10 as branch protection not enabled on development/release branches ⚠️-1/10 as no workflows found ⚠️-1/10 as No tokens found, and ⚠️ check that webhooks is configured supporting secrets not run
Large Commits	Detected no unusually large commits being 0.000 found under or at the 0.02 permitted threshold (Churn)
Obfuscated Code	Detected no unusual-looking commits being 0.0 found under or at the 0 permitted threshold (Entropy)
Binary Artifact(s)	10/10 as no binaries found in the repo with binaries potentially containing code being 0 found under or at the 0 permitted threshold
Typosquatting Risk	⚠️Failed to analyze for typos - can't identify a known language
Known Vulnerabilities	❌0/10 as 12 existing vulnerabilities detected (open, known unfixed vulnerabilities). Other detected vuls including other dependencies identified potentially: 1 critical; 4 high; 7 medium criticals: ❌1 GHSA-vqfr-h8mv-ghfj

Integrity	
Peer Reviews	Count pending; and activity is 10/10 as all changesets reviewed with change requests often lacking approving review prior to merge with 96.923% ❌over the 5.0% threshold and commits too often applied by the author with 93.20% ❌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 9 merged PRs checked by a CI test -- score normalized to 0
Signed Commits	Manual
Cryptographically Signed Commits	❌18 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: 1196 pypi, 349 githubactions, 159 github, 100 cargo, 1 null
Dependencies Pinned to Version	⚠️-1/10 as no dependencies found
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: 196, dependencies pulled: 196, dependencies unknown: 0 Secondary: Total found: 1339, dependencies pulled: 45, dependencies unknown: ⚠️1294 Tertiary and greater (Max search depth realized 3): Total found: 270, dependencies pulled: 2, dependencies unknown: ⚠️268
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	TemoaProject/temoa, Tools for Energy Model Optimization and Analysis ❌ATTENTION: this is a fork of hunteke/temoa
Individual or Organization	Organization Details: Name: Temoa (Tools for Energy Model Optimization and Analysis) Company: Not Reported Bio: An open source energy system model Email: Not Reported Blog: http://temoaproject.org Geo: Raleigh NC Source: GitHub
Organization Type	Pending, see: https://api.github.com/users/TemoaProject/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)	temoa 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)	0.42/1.0 (higher's better)
Commits	Days since last commit: 4 days, on Fri Aug 8 18:17:00 UTC 2025, reported 0 days ago Days since first commit: 3867 days, on Sat Jan 10 19:22:06 UTC 2015, reported 0 days ago Activity: ❌0/10 with 1 commit(s) and 0 issue activity found in the last 90 days -- score normalized to 0 with most recent activity being 7 weeks under or at the 71 week threshold
Number of Contributors	Core: Count pending Other: 12 Organizational diversity: 10/10 as project has 8 contributing companies or organizations
Problem Reporting Process	Yes with 7 open issues
Vulnerability Reporting Process	❌0/10 as security policy file not detected
Suitability	
License	License: GNU General Public License v2.0 SPDX_ID: GPL-2.0
License Risk	Detected ❌1 restrictive license(s) being: GPL-2.0-only 2 //github.com/TemoaProject/temoa has a copyleft, restricted, license and (2 high) potentially reported from dependencies
About this report	
Created	Tue Aug 12 22:34:05 UTC 2025
Version	pubRel 250516evie (branch: publicRelease)
Analysis Source	Package SBOM: TemoaProject___temoa.spdx.json, bf4ebd75372d367cbf4d87ca19b66f4e
Analysis ID	SBOM created on 2025-08-12T22:14:17Z (complete)
Runtime	Approximately 13 minute(s) (this run), for a total of 13 minute(s) over 1 run(s)

Command line	/home/hc_user/.local/bin/scir-oss.sh -l -v -C temoa -G TemoaProject/temoa -P TemoaProject___temoa.spdx.json:sbom
Dependency and Scoring depth	3, 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 'TemoaProject___temoa.spdx.json' are declared to include transitive dependencies - issue depth is 0 (change with -i) I: dependency depth limit '(-d 3)': skipped deeper dependencies... W: coalesce_scorecards: counted 165 missing project scorecard(s) 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
pkg:pypi/h11@0.14.0 version <0.16.0 (python)	CV-GHSA-vqfr-h8mv-ghfj	**Overview** h11 accepts some malformed Chunked-Encoding bodies **Grype Data Source**: https://github.com/advisories/GHSA-vqfr-h8mv-ghfj **Recommendation** Fix available in 0.16.0 **References** https://github.com/python-hyper/h11/commit/114803a29ce50116dc47951c690ad4892b1a36ed https://github.com/python-hyper/h11/security/advisories/GHSA-vqfr-h8mv-ghfj **CVE:** CVE-2025-43859 - **CVSS**: 9.1
pkg:pypi/jupyter-core@5.7.2 version <5.8.0 (python)	HV-GHSA-33p9-3p43-82vq	**Overview** Jupyter Core on Windows Has Uncontrolled Search Path Element Local Privilege Escalation Vulnerability **Grype Data Source**: https://github.com/advisories/GHSA-33p9-3p43-82vq **Recommendation** Fix available in 5.8.1 **References** https://github.com/jupyter/jupyter_core/security/advisories/GHSA-33p9-3p43-82vq **CVE:** CVE-2025-30167 - **CVSS**: 7.3
pkg:pypi/tornado@6.4.1 version <6.5 (python)	HV-GHSA-7cx3-6m66-7c5m	**Overview** Tornado vulnerable to excessive logging caused by malformed multipart form data **Grype Data Source**: https://github.com/advisories/GHSA-7cx3-6m66-7c5m **Recommendation** Fix available in 6.5 **References** https://github.com/tornadoweb/tornado/commit/b39b892bf78fe8fea01dd45199aa88307e7162f3 https://github.com/tornadoweb/tornado/security/advisories/GHSA-7cx3-6m66-7c5m https://lists.debian.org/debian-lts-announce/2025/05/msg00038.html **CVE:** CVE-2025-47287 - **CVSS**: 7.5
pkg:pypi/tornado@6.4.1 version <=6.4.1 (python)	HV-GHSA-8w49-h785-mj3c	**Overview** Tornado has an HTTP cookie parsing DoS vulnerability **Grype Data Source**: https://github.com/advisories/GHSA-8w49-h785-mj3c **Recommendation** Fix available in 6.4.2 **References** https://github.com/advisories/GHSA-7pwv-g7hj-39pr https://github.com/tornadoweb/tornado/commit/d5ba4a1695fbf7c6a3e54313262639b198291533 https://github.com/tornadoweb/tornado/security/advisories/GHSA-8w49-h785-mj3c **CVE:** CVE-2024-52804 - **CVSS**: 7.5
pkg:pypi/starlette@0.38.2 version <0.40.0 (python)	HV-GHSA-f96h-pmfr-66vw	**Overview** Starlette Denial of service (DoS) via multipart/form-data **Grype Data Source**: https://github.com/advisories/GHSA-f96h-pmfr-66vw **Recommendation** Fix available in 0.40.0 **References** https://github.com/encode/starlette/commit/fd038f3070c302bff17ef7d173dbb0b007617733

| | | https://github.com/encode/starlette/security/advisories/GHSA-f96h-pmfr-66vw

CVE:
CVE-2024-47874 - **CVSS**: 0 |
| --- | --- | --- |

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
//github.com/TemoaProject/temoa has a copyleft, restricted, license	HL0001	**Summary** Package owners declare a copyleft open source software license GPL-2.0. **Impact** Use and/or modification could compel disclosure of source code back to the open source software community. **References** https://github.com/TemoaProject/temoa from git://github.com/TemoaProject/temoa.git **Recommendation** Do not modify code in this module without understanding the open source software license and any disclosure requirements.
//github.com/TemoaProject/temoa has a copyleft, restricted, license	HL0002	**Summary** Package owners declare a copyleft open source software license GPL-2.0. **Impact** Use and/or modification could compel disclosure of source code back to the open source software community. **References** https://github.com/TemoaProject/temoa from git://github.com/TemoaProject/temoa.git **Recommendation** Do not modify code in this module without understanding the open source software license and any disclosure requirements.

No labels

Terms of Use