

drawio-mcp

github.com/jgraph/drawio-mcp

Scanned 24 September 2026 at 10:28 · Report generated 29 October 2026 · JavaScript · 5,504 stars

OVERALL ASSESSMENT

Medium

Combined score 48 · 29 findings after filtering

Summary

This repository has a medium vulnerability score of 45, which means there are several insecure coding patterns that an attacker could exploit to steal secrets or code. However, the scan also found signs of potentially malicious intent with a low score of 3, suggesting the code might be intentionally harmful rather than just poorly written. Most of these issues relate to common mistakes like using unescaped user input in logs or allowing variable interpolation in scripts, which are typical errors that can be fixed by developers. There is only one high-severity finding involving an encoded payload being decoded and executed, but this appears to be a specific edge case rather than widespread malicious behavior. Overall, while the code contains some risky patterns that need attention, it does not look like a repository designed to cause harm, so you can proceed with caution if you are comfortable addressing the identified issues.

Written by a language model running locally on the scanning machine, from the findings in this report. The risk levels above and below were decided by the scoring model, not by this summary.

Risk, by type

MalDet scores two different questions separately, because they call for different responses: code can be badly written without being hostile, and hostile code is not always badly written.

VULNERABILITY

Medium (45)

Insecure coding an attacker could exploit. Usually mistakes, and usually fixable in place.

MALICIOUS PATTERN

Low (3)

Signs the code may be trying to do harm: hidden payloads, credential access, persistence, exfiltration.

What each detector found

DETECTOR	LOOKS FOR	HIGH	MEDIUM	LOW	TOTAL
semgrep	Insecure coding patterns across many languages	2	20	2	24
yara	Signatures of malicious behaviour in source files	3	0	1	4
guarddog	Malicious package and install-time behaviour	0	1	0	1

21 of 29 findings were rated more likely genuine than noise by the classifier.

Evidence

Identical findings are grouped, so a single rule firing many times takes one row. Ordered worst first. “Seen” is how many times that finding occurred.

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
HIGH	semgrep	Using variable interpolation `\${{...}}` with `github` context data in a `run:` step could allow an attacker to inject their own code into the runner. This would allow them to steal secrets and code. `github` context data can have arbitrary user input and should be treated as untrusted. Instead, use	2	/.github/workflows/publish-tool-server.yml:80
HIGH	yara	YARA rule matched: detect_base64_exec — Encoded payload decoded and then executed	1	/mcp-tool-server/src/pages.js
HIGH	yara	YARA rule matched: detect_obfuscated_string_execution — Reconstructs a string character-by-character or from hex escapes, then immediately executes it - fromCharCode/chr() alone are common in ordinary text-processing code, so this requires both the reconstruction and an execution call together	2	/mcp-app-server/src/shared.js
MEDIUM	semgrep	User data flows into the host portion of this manually-constructed HTML. This can introduce a Cross-Site-Scripting (XSS) vulnerability if this comes from user-provided input. Consider using a sanitization library such as DOMPurify to sanitize the HTML within.	1	/mcp-tool-server/src/libavoid-pass.js:289

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	guarddog	Detects LOLBAS usage in install hooks (execution and network tools) [threat-process-hooks]	1	/mcp-tool-server/package.json:15
MEDIUM	semgrep	RegExp() called with a `name` function argument, this might allow an attacker to cause a Regular Expression Denial-of-Service (ReDoS) within your application as RegExP blocks the main thread. For this reason, it is recommended to use hardcoded regexes instead. If your regex is run on user-controlled	1	/shared/mx-xml.js:391
MEDIUM	semgrep	GitHub Actions step uses a mutable tag or branch reference. Tags and branch names can be silently repointed by the action owner, enabling supply-chain attacks — as seen in the trivy-action and kics-github-action compromises. Pin the reference to a full 40-character commit SHA instead, e.g. `uses: ac	14	/.github/workflows/publish-tool-server.yml:38
MEDIUM	semgrep	Detected possible user input going into a `path.join` or `path.resolve` function. This could possibly lead to a path traversal vulnerability, where the attacker can access arbitrary files stored in the file system. Instead, be sure to sanitize or validate user input first.	4	/mcp-tool-server/src/cdn-cache.js:128
LOW	semgrep	Detected a logger that logs user input without properly neutralizing the output. The log message could contain characters like `` and `` and cause an attacker to forge log entries or include malicious content into the logs. Use proper input validation and/or output encoding to prevent log entries	2	/mcp-app-server/src/index.js:227
LOW	yara	YARA rule matched: detect_downloader — Downloads a remote resource - common and low-signal alone; see detect_download_and_execute for the composite version	1	/mcp-tool-server/vendor/libavoid/libavoid-node.mjs

How to read this report

- **This is a static scan.** The code was read, never executed. Behaviour that only appears at runtime is outside what any of these detectors can see.
- **Findings are not all equally real.** A classifier rates each finding on how likely it is to be genuine rather than noise, and that rating weights the scores. Measured against a hand-reviewed sample it reached precision 0.52 and recall 0.62 — useful for ranking, not a verdict on any single finding.
- **A high score is not proof of malice.** Security tools, penetration-testing frameworks and malware research repositories contain the same patterns as real malware by design. The two risk types above exist to keep that distinction visible.
- **Absence of findings is not proof of safety.** A detector that is not installed, or a language none of them parse, produces silence rather than a warning.
- **This scan is a snapshot.** The repository may have changed since 24 September 2026.