

chamilo-lms

github.com/chamilo/chamilo-lms

Scanned 24 September 2026 at 06:09 · Report generated 29 October 2026 · PHP · 1,006 stars

OVERALL ASSESSMENT

High

Combined score 104 · 206 findings after filtering

Summary

The repository has a score of 0.0 for insecure coding patterns, which means there are no obvious bugs or unsafe code that an attacker could exploit right now. However, the scan also found a critical risk score of 104.0, indicating strong signs that the code might be intentionally malicious rather than just poorly written. The most concerning issues involve hidden malware techniques like base64 decoding and steganography used to hide dangerous payloads within files such as yarn-4.17.1.cjs and ViewerJS webodf.js. These patterns are often used by attackers to bypass security checks, so the code should be treated with extreme caution until it is thoroughly reviewed and cleaned by a professional security team. While some findings relate to suspicious dependencies or obfuscation tricks that could indicate past malicious activity, they do not necessarily mean the entire project is compromised.

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

Safe

 (0)

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

MALICIOUS PATTERN

Critical

 (104)

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
dep_checker	Vulnerable, unpinned or typosquatted dependencies	1	0	124	125
yara	Signatures of malicious behaviour in source files	56	0	8	64
guarddog	Malicious package and install-time behaviour	7	6	4	17

18 of 206 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	guarddog	Detects a payload hidden by excessive whitespace or require aliased through a global to evade static analysis [threat-runtime-obfuscation-hidden-code]	1	/public/ plugin/ CStudio/ editor/dist/ js/ grapes.js:4259
HIGH	guarddog	Detects access to sensitive files (credentials, configs, keys) [threat-filesystem-read]	5	/.yarn/ releases/ yarn-4.17.1. cjs:4
HIGH	guarddog	Detects download-and-execute patterns: fetching a remote file then executing it [threat-process-download-exec]	3	/.yarn/ releases/ yarn-4.17.1. cjs:140
HIGH	guarddog	Detects steganography decode followed by code execution [threat-runtime-obfuscation-steganography]	1	/public/main/ inc/lib/ javascript/ ViewerJS/ webodf.js:31
HIGH	guarddog	Detects base64 decoding followed by code execution [threat-runtime-obfuscation-base64exec]	1	/.yarn/ releases/ yarn-4.17.1. cjs:164
HIGH	dep_checker	Typosquatting: 'vuex' is suspiciously similar to 'vue'	1	package.json

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
HIGH	yara	YARA rule matched: detect_base64_exec — Encoded payload decoded and then executed	7	/public/ plugin/ CStudio/ editor/jscss/ oel- teachdoc.js
HIGH	yara	YARA rule matched: detect_download_and_execute — Downloads a remote resource AND executes it - the actually dangerous combination, not just downloading alone	7	/public/ plugin/ ExtraMenuFromWeb service/ lib/ extramenufrom mweb service_ plugin.class. php
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	41	/public/ plugin/ CStudio/ resources/js/ jquery1.8.2. min.js
HIGH	yara	YARA rule matched: detect_persistence_mechanism — Modifies a startup/scheduling location - legitimate application code essentially never does this	1	/public/ documentation /legacy/ optimization. html
MEDIUM	guarddog	Detects unicode homoglyphs and uncommon characters used for obfuscation [threat-runtime-obfuscation-unicode]	1	/public/main/ inc/lib/ javascript/ d3/ d3.v3.5.4.js: 1261
MEDIUM	guarddog	Detects log/console suppression combined with obfuscated code, a common malware evasion pattern [threat-runtime-obfuscation-log-suppress]	1	/public/main/ inc/lib/ javascript/ ViewerJS/ compatibility .js:408
LOW	guarddog	Detects heavy obfuscation techniques commonly used by malware [threat-runtime-obfuscation]	1	/.yarn/ releases/ yarn-4.17.1. cjs:191

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	guarddog	Detects reading of environment variables (credential access, often contains secrets) [threat-runtime-environment-read]	3	/.yarn/releases/yarn-4.17.1.cjs:398
LOW	dep_checker	Loose version constraint: '@uppy/file-input^4.2.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'webpack-dev-server^5.2.4' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'jspdf^4.2.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'js-cookie^2.2.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'jsplumb^2.15.6' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'leaflet^1.9.4' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'litepicker^2.0.12' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'lodash^4.18.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'luxon^2.5.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'mathjax^4.1.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'mediaelement^7.1.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'mini-css-extract-plugin^2.10.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'moment^2.30.1' — attacker could push malicious update	1	package.json

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	dep_checker	Loose version constraint: 'multiselect-two-sides^2.5.7' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'nprogress^0.2.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'path^0.12.7' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'pinia^3.0.4' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'playwright-bdd^9.2.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'postcss-loader^8.2.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'postcss-prefix-selector^2.1.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'postcss^8.5.15' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'prettier-plugin-tailwindcss^0.7.4' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'pretty-bytes^5.6.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'primeicons^7.0.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'primevue^4.5.5' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'purgecss-webpack-plugin^8.0.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'qs^6.15.2' — attacker could push malicious update	1	package.json

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	dep_checker	Loose version constraint: 'readmore-js^2.2.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'recordrtc^5.6.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'video.js^8.23.8' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'webpack^5.107.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'webpack-notifier^1.15.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'webpack-cli^6.0.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'vuex^4.1.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'vuex-map-fields^1.4.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'vuedraggable^4.1.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'vue^3.5.35' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'vue-toastification^2.0.0-rc.5' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'vue-perfect-scrollbar^0.2.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'vue-multiselect^3.5.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'vue-loader^17.4.2' — attacker could push malicious update	1	package.json

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	dep_checker	Loose version constraint: 'vue-flatpickr-component^9.0.8' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'vue-eslint-parser^10.4.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'sweetalert2^11.26.25' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'sortablejs^1.15.7' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'signature_pad^3.0.0-beta.4' — attacker could push malicious update	1	package.json

Showing the 60 most significant of 139 distinct findings. The counts in the previous section cover all of them.

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.