

openstamanager

github.com/devcode-it/openstamanager

Scanned 24 September 2026 at 08:18 · Report generated 29 October 2026 · PHP · 150 stars

OVERALL ASSESSMENT

High

Combined score 183 · 189 findings after filtering

Summary

This repository shows high-risk issues that could allow attackers to run code, delete files, or steal data if they are not careful. The most serious problems involve dangerous operations like base64 decoding followed by execution and downloading remote files that are then run. These findings suggest the code may be intentionally malicious rather than just having poor security habits. While some issues appear to be ordinary insecure coding patterns, others indicate a deliberate attempt to bypass security checks or execute harmful payloads. The developer should treat this code as unsafe until it is thoroughly reviewed and fixed by a qualified security expert before any production use.

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

High (158)

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

MALICIOUS PATTERN

Medium (25)

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	7	50	33	90
dep_checker	Vulnerable, unpinned or typosquatted dependencies	0	2	75	77

DETECTOR	LOOKS FOR	HIGH	MEDIUM	LOW	TOTAL
yara	Signatures of malicious behaviour in source files	17	0	3	20
guarddog	Malicious package and install-time behaviour	2	0	0	2

42 of 189 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 destructive operations (recursive deletion, wiping) [threat-filesystem-destruction]	1	/assets/src/js/wacom/common/libs/signature_sdk.js:1
HIGH	semgrep	If unverified user data can reach the `exec` method it can result in Remote Code Execution	3	/gulpfile.js:684
HIGH	guarddog	Detects base64 decoding followed by code execution [threat-runtime-obfuscation-base64exec]	1	/assets/src/js/wacom/modules/digital-ink/workers/InkPathProvider.js:1
HIGH	semgrep	JWT token detected	1	/update/2_4_48.sql:41
HIGH	semgrep	Executing non-constant commands. This can lead to command injection.	3	/src/Util/XML.php:107
HIGH	yara	YARA rule matched: detect_base64_exec — Encoded payload decoded and then executed	9	/assets/src/js/wacom/modules/js-ext/js-ext-min.mjs
HIGH	yara	YARA rule matched: detect_download_and_execute — Downloads a remote resource AND executes it - the actually dangerous combination, not just downloading alone	1	/docker/Dockerfile.dev

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
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	7	/assets/src/js/wacom/modules/js-ext/js-ext-min.mjs
MEDIUM	semgrep	RegExp() called with a `searchTerm` 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-cont	1	/assets/src/js/base/supersearch.js:82
MEDIUM	semgrep	RegExp() called with a `find` 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	/assets/src/js/functions/functions.js:436
MEDIUM	semgrep	User controlled data in a HTML string may result in XSS	3	/assets/src/js/functions/functions.js:344
MEDIUM	semgrep	`t.replace("[", ".").replace` method will only replace the first occurrence when used with a string argument ("]"). If this method is used for escaping of dangerous data then there is a possibility for a bypass. Try to use sanitization library instead or use a Regex with a global flag.	4	/assets/src/js/wacom/modules/digital-ink/workers/SplitPointsProvider.mjs:1
MEDIUM	semgrep	`t.replace` method will only replace the first occurrence when used with a string argument ("["). If this method is used for escaping of dangerous data then there is a possibility for a bypass. Try to use sanitization library instead or use a Regex with a global flag.	4	/assets/src/js/wacom/modules/digital-ink/workers/SplitPointsProvider.mjs:1

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	semgrep	<code>`e.replace("[", ".").replace`</code> method will only replace the first occurrence when used with a string argument (<code>"["</code>). If this method is used for escaping of dangerous data then there is a possibility for a bypass. Try to use sanitization library instead or use a Regex with a global flag.	1	<code>/assets/src/js/wacom/modules/digital-ink/workers/InkPathProvider.mjs:1</code>
MEDIUM	semgrep	<code>`e.replace`</code> method will only replace the first occurrence when used with a string argument (<code>"["</code>). If this method is used for escaping of dangerous data then there is a possibility for a bypass. Try to use sanitization library instead or use a Regex with a global flag.	1	<code>/assets/src/js/wacom/modules/digital-ink/workers/InkPathProvider.mjs:1</code>
MEDIUM	semgrep	This Dependabot configuration does not set a cooldown period. Newly published packages can be malicious or unstable. Add a <code>`cooldown`</code> block with <code>`default-days: 7`</code> to each <code>`package-ecosystem`</code> entry under <code>`updates`</code> to wait 7 days before proposing updates to newly published package versions. Reference:	3	<code>/.github/dependabot.yml:16</code>
MEDIUM	semgrep	Found direct access to a PHP variable without HTML escaping inside an inline PHP statement setting data from <code>`\$_REQUEST[...]</code> . When untrusted input can be used to tamper with a web page rendering, it can lead to a Cross-site scripting (XSS) vulnerability. XSS vulnerabilities occur when untrusted input	2	<code>/include/init/configuration.php:125</code>
MEDIUM	semgrep	This <code>.yarnrc.yml</code> does not set a minimal age gate or sets it too low. Newly published packages can be malicious or unstable. Add <code>`npmMinimalAgeGate: "7d"`</code> to wait 7 days before resolving newly published package versions. Added in: 4.10 Reference: https://yarnpkg.com/configuration/yarnrc#npmMinimalAge	1	<code>/.yarnrc.yml:8</code>
MEDIUM	semgrep	File name based on user input risks server-side request forgery.	1	<code>/src/Security/LaravelRateLimiter.php:55</code>

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	semgrep	Make sure comparisons involving md5 values are strict (use `===` not `==`) to avoid type juggling issues	4	/src/Auth0SM.php:1082
MEDIUM	semgrep	Access-Control-Allow-Origin response header is set to "*". This will disable CORS Same Origin Policy restrictions.	1	/api/index.php:51
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	10	/.github/workflows/codeql.yml:58
MEDIUM	semgrep	Possibility of prototype polluting function detected. By adding or modifying attributes of an object prototype, it is possible to create attributes that exist on every object, or replace critical attributes with malicious ones. This can be problematic if the software depends on existence or non-exis	5	/assets/src/js/wacom/modules/digital-ink/workers/InkPathProvider.mjs:1
MEDIUM	semgrep	Calling `unserialize()` with user input in the pattern can lead to arbitrary code execution. Consider using JSON or structured data approaches (e.g. Google Protocol Buffers).	2	/src/Models/OAuth2.php:153
MEDIUM	semgrep	Using user input when deleting files with `unlink()` is potentially dangerous. A malicious actor could use this to modify or access files they have no right to.	6	/modules/aggiornamenti/src/Controlli/IntegritaFile.php:137
MEDIUM	dep_checker	Loose version constraint: 'js-md5^0.9.0' — attacker could push malicious update	1	package.json
MEDIUM	dep_checker	Loose version constraint: 'md5-file^5.0.0' — attacker could push malicious update	1	package.json
LOW	semgrep	Detected string concatenation with a non-literal variable in a util.format / console.log function. If an attacker injects a format specifier in the string, it will forge the log message. Try to use constant values for the format string.	33	/assets/src/js/wacom/modules/js-ext/js-ext-min.js:1

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	dep_checker	Loose version constraint: '@babel/core^7.11.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@babel/preset-env^7.11.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@fullcalendar/moment^6.1.5' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@openapitools/openapi-generator-cli^2.25.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: '@ttskch/select2-bootstrap4-theme^1.5.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'admin-lte^3.2.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'archiver^8.0.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'autocomplete^6.1.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'autonumeric^4.6.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'autosize^6.0.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'bootstrap-colorpicker^3.4.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'bootstrap-daterangepicker^2.1.25' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'bootstrap-maxlength^2.0.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'bootstrap^4.3.1' — attacker could push malicious update	1	package.json

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	dep_checker	Loose version constraint: 'chart.js^4.5.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'clipper-lib^6.4.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'components-jqueryui^1.12.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'datatables.net-bs^1.10.15' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'datatables.net-buttons-bs^1.3.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'datatables.net-scroller-bs^2.4.3' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'datatables.net-select-bs^1.2.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'del^6.0.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'driver.js^1.0.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'dropzone^5.7.2' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'eonasdan-bootstrap-datetimepicker^4.17.49' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'font-awesome^4.7.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'fullcalendar-scheduler^6.1.5' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'geocomplete^1.7.0' — attacker could push malicious update	1	package.json

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	dep_checker	Loose version constraint: 'gl-matrix^3.4.3' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'globby^14.0.1' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'gulp-autoprefixer^10.0.0' — attacker could push malicious update	1	package.json
LOW	dep_checker	Loose version constraint: 'gulp-babel^8.0.0' — attacker could push malicious update	1	package.json

Showing the 60 most significant of 104 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.