

typo3

github.com/TYP03/typo3

Scanned 29 October 2026 at 10:13 · Report generated 29 October 2026 · PHP · 1,218 stars

OVERALL ASSESSMENT

Medium

Combined score 24 · 14 findings after filtering

Summary

4 findings likely need attention, 10 look like noise. Most notable: Detects download-and-execute patterns: fetching a remote file then executing it [threat... (95% confidence).

Generated from finding counts. A plain-English summary was not available for this scan.

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

Medium (24)

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
yara	Signatures of malicious behaviour in source files	10	0	0	10
guarddog	Malicious package and install-time behaviour	2	1	1	4

4 of 14 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 download-and-execute patterns: fetching a remote file then executing it [threat-process-download-exec]	2	/Build/Sources/TypeScript/filelist/context-menu-actions.ts:127
HIGH	yara	YARA rule matched: detect_base64_exec — Encoded payload decoded and then executed	1	/typo3/sysextrteckeditor/Resources/Public/Contrib/@ckeditor/ckeditor5-inspector.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	6	/typo3/sysextrbackend/Resources/Public/JavaScript/Contrib/@codemirror/view.js
HIGH	yara	YARA rule matched: detect_persistence_mechanism — Modifies a startup/scheduling location - legitimate application code essentially never does this	3	/typo3/sysextrcore/Documentation/Changelog/12.2/Feature-97700-AdoptSymfonyMessengerAsAMessageBusAndQueue.rst
MEDIUM	guarddog	Detects unicode homoglyphs and uncommon characters used for obfuscation [threat-runtime-obfuscation-unicode]	1	/typo3/sysextrteckeditor/Resources/Public/Contrib/translations/bg.js:1
LOW	guarddog	Detects heavy obfuscation techniques commonly used by malware [threat-runtime-obfuscation]	1	/typo3/sysextrbackend/Resources/Public/JavaScript/Contrib/@codemirror/view.js:1

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 29 October 2026.