

# zoneminder

github.com/ZoneMinder/zoneminder

Scanned 24 September 2026 at 06:48 · Report generated 29 October 2026 · PHP · 5,936 stars

OVERALL ASSESSMENT

Medium

Combined score 56 · 86 findings after filtering

## Summary

The repository has two medium-risk scores, both indicating that there are some insecure coding patterns and signs of potentially malicious behavior, but these issues do not necessarily mean the code is intentionally harmful. The most critical finding is that the project uses Telnet to connect to remote servers, which is an extremely dangerous practice because it transmits data without encryption and can be easily exploited by attackers. Additionally, the code contains several other security concerns such as downloading files from the internet and executing them, along with potential memory scraping vulnerabilities, but these are likely due to standard development habits rather than deliberate attacks. While some of the flagged items appear in legitimate software like jQuery or Beowulf documentation, the presence of Telnet usage and the download-and-execute pattern suggests that this codebase requires immediate attention before it can be used safely.

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 (22)

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

MALICIOUS PATTERN

Medium (34)

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     |
|-----------------|---------------------------------------------------|------|--------|-----|-----------|
| <b>yara</b>     | Signatures of malicious behaviour in source files | 51   | 0      | 15  | <b>66</b> |
| <b>bandit</b>   | Insecure coding patterns in Python source         | 2    | 1      | 13  | <b>16</b> |
| <b>guarddog</b> | Malicious package and install-time behaviour      | 3    | 0      | 1   | <b>4</b>  |

6 of 86 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                                       |
|-------------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|------|--------------------------------------------------------|
| <b>HIGH</b> | guarddog | Detects HTTP/HTTPS URL dependencies in package.json (dependency confusion, untrusted sources) [threat-npm-http-dependency]                                    | 3    | /web/skins/classic/js/jquery-ui-1.13.2/package.json:21 |
| <b>HIGH</b> | bandit   | Telnet-related functions are being called. Telnet is considered insecure. Use SSH or some other encrypted protocol.                                           | 1    | /scripts/zalarm-server.py:68                           |
| <b>HIGH</b> | bandit   | A telnet-related module is being imported. Telnet is considered insecure. Use SSH or some other encrypted protocol.                                           | 1    | /scripts/zalarm-server.py:38                           |
| <b>HIGH</b> | yara     | YARA rule matched: detect_base64_exec — Encoded payload decoded and then executed                                                                             | 4    | /web/js/hls-1.6.13/hls.min.js                          |
| <b>HIGH</b> | yara     | YARA rule matched: detect_download_and_execute — Downloads a remote resource AND executes it - the actually dangerous combination, not just downloading alone | 1    | /web/includes/monitor_probe.php                        |

| SEVERITY | DETECTOR | FINDING                                                                                                                                                                                                                                                                                                      | SEEN | EXAMPLE LOCATION                                                                             |
|----------|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|----------------------------------------------------------------------------------------------|
| HIGH     | yara     | YARA rule matched:<br>detect_obfuscated_string_execution —<br>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 | 39   | /web/skins/classic/assets/bootstrap-table/extensions/group-by-v2/bootstrap-table-group-by.js |
| HIGH     | yara     | YARA rule matched:<br>detect_persistence_mechanism — Modifies a startup/scheduling location - legitimate application code essentially never does this                                                                                                                                                        | 7    | /distros/ubuntu2004/README.Debian                                                            |
| MEDIUM   | bandit   | Possible binding to all interfaces.                                                                                                                                                                                                                                                                          | 1    | /scripts/zalarm-server.py:118                                                                |
| LOW      | guarddog | Detects memory scraping and credential dumping from process memory [threat-process-memory]                                                                                                                                                                                                                   | 1    | /web/js/hls-1.6.13/hls.min.js:1                                                              |
| LOW      | bandit   | Consider possible security implications associated with the subprocess module.                                                                                                                                                                                                                               | 4    | /scripts/zalarm-server.py:62                                                                 |
| LOW      | bandit   | Starting a process with a partial executable path                                                                                                                                                                                                                                                            | 3    | /scripts/zalarm-server.py:50                                                                 |
| LOW      | bandit   | subprocess call - check for execution of untrusted input.                                                                                                                                                                                                                                                    | 5    | /utils/check-shareddata-abi.py:80                                                            |
| LOW      | yara     | YARA rule matched: detect_downloader —<br>Downloads a remote resource - common and low-signal alone; see detect_download_and_execute for the composite version                                                                                                                                               | 15   | /dep/jwt-cpp/.github/actions/install/kazuho-picojson/action.yml                              |
| LOW      | bandit   | Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.                                                                                                                                                                                                             | 1    | /tools/zm_stream_socket_dump.py:88                                                           |

## 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.