f / **prompts.chat** Public

Code Issues 10 Pull requests 35 Actions Projects Models S

Commit `0f8d4c3`

mdisec committed 3 weeks ago · ✓ 2 / 3

```
  fix(security): harden skill zip packaging against path traversal and control
char injection
```

main (#1101)

1 parent 6d0bf7f commit 0f8d4c3

2 files changed +10 -9 lines changed

Top

Filter files…

- src
  - app/api/prompts/[id]/skill
    - route.ts
  - lib
    - skill-files.ts

2 files changed +10 -9 lines changed

Search within code

src/app/api/prompts/[id]/skill/route.ts

```
@@ -55,16 +55,16 @@ export async function GET(
55  55
56  56      // Add each file to the zip (sanitize filenames to prevent Zip Slip)
57  57      for (const file of files) {
58      -     const safeName = sanitizeFilename(file.filename)
59      -       ?? file.filename
60      -         .split("/")
61      -         .filter(segment => segment !== ".." && segment !== ".")
62      -         .join("/")
```

```
63      -         .replace(/^\/+/, "");
64      -
65      -     if (safeName) {
66      -       zip.file(safeName, file.content);
        58  +     const candidate = file.filename
        59  +       .replace(/\\/g, "/")
        60  +       .split("/")
        61  +       .filter((segment) => segment && segment !== "." && segment !== "..")
        62  +       .join("/");
        63  +     const safeName = sanitizeFilename(candidate);
        64  +     if (!safeName) {
        65  +       continue;
67      66        }
        67  +     zip.file(safeName, file.content);
68      68      }
69      69
70      70      // Generate the zip content as blob for Response compatibility
```

src/lib/skill-files.ts

```
        @@ -201,6 +201,7 @@ export function getLanguageFromFilename(filename:
        string): string {
201     201   export function sanitizeFilename(filename: string): string | null {
202     202     const trimmed = filename.trim();
203     203     if (!trimmed) return null;
        204 +   if (/[\x00-\x1F\x7F]/.test(trimmed)) return null;
204     205     if (trimmed.includes("..")) return null;
205     206     if (trimmed.startsWith("/") || trimmed.endsWith("/")) return null;
206     207     if (trimmed.includes("//")) return null;
```

Comments 0

Please sign in to comment.