

f / prompts.chat Public

<> Code Issues 9 Pull requests 33 Actions Projects Models Se

Commit 0f8d4c3



mdisec committed 2 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](#)

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

2 files changed +10 -9 lines changed

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);
67
68 +     const candidate = file.filename
69 +         .replace(/\\/g, "/")
70 +         .split("/")
71 +         .filter((segment) => segment && segment !== "." && segment !== "..")
72 +         .join("/");
73 +     const safeName = sanitizeFilename(candidate);
74 +     if (!safeName) {
75 +         continue;
76
77     }
78 +     zip.file(safeName, file.content);
79
80     }
81
82     // 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.