anthropics / **anthropic-sdk-typescript** Public

Code | Issues 79 | Pull requests 43 | Discussions | Actions | Security and

⚠ This commit does not belong to any branch on this repository, and may belong to a fork outside of the repository.

Commit `0ac69b3`

dtmeadows authored 4 days ago · ✓ 3 / 3 · Verified

```
fix(memory): append path separator in validatePath prefix check

## Changes

`validatePath` and `validateNoSymlinkEscape` used
`startsWith(resolvedRoot)` without a trailing path separator, so a
sibling directory like `/memories_backup/` would pass the `/memories`
prefix check. Appends `path.sep` so only actual children of the memory
root are accepted.
```

1 parent 284561f commit 0ac69b3

2 files changed +38 -2 lines changed

Top

Filter files...

- src/tools/memory
  - node.ts
- tests/lib/tools
  - BetaLocalFilesystemMemoryTool.test.ts

2 files changed +38 -2 lines changed

Search within code

src/tools/memory/node.ts

```
@@ -73,7 +73,7 @@ async function validateNoSymlinkEscape(targetPath: string,
memoryRoot: string):
```

```
73  73        while (true) {
74  74          try {
75  75            const resolved = await fs.realpath(current);
76      -         if (!resolved.startsWith(resolvedRoot)) {
    76  +         if (resolved !== resolvedRoot && !resolved.startsWith(resolvedRoot + path.sep)) {
77  77              throw new Error(`Path would escape /memories directory via symlink`);
78  78            }
79  79            return;
    @@ -141,7 +141,7 @@ export class BetaLocalFilesystemMemoryTool implements MemoryToolHandlers {
141 141
142 142         const resolvedPath = path.resolve(fullPath);
143 143         const resolvedRoot = path.resolve(this.memoryRoot);
144     -       if (!resolvedPath.startsWith(resolvedRoot)) {
    144 +       if (resolvedPath !== resolvedRoot && !resolvedPath.startsWith(resolvedRoot + path.sep)) {
145 145           throw new Error(`Path ${memoryPath} would escape /memories directory`);
146 146         }
147 147
```

...tools/BetaLocalFilesystemMemoryTool.test.ts

```
    @@ -510,6 +510,42 @@ describe('BetaLocalFilesystemMemoryTool', () => {
510 510       });
511 511     });
512 512
    513 +   describe('sibling directory prefix attack', () => {
    514 +     it('should reject symlink to a sibling directory whose name shares the memory root prefix', async () => {
    515 +       // Attack: create a sibling directory memories_backup next to memories,
    516 +       // then symlink from inside memories to it. Without the trailing separator
    517 +       // fix, validateNoSymlinkEscape's startsWith check would pass because
    518 +       // "/tmp/.../memories_backup".startsWith("/tmp/.../memories") is true.
    519 +       const memoriesDir = path.join(tempDir, 'memories');
    520 +       const siblingDir = path.join(tempDir, 'memories_backup');
    521 +       await fs.mkdir(siblingDir, { recursive: true });
    522 +       await fs.writeFile(path.join(siblingDir, 'secret.txt'), 'stolen data', 'utf-8');
```

```
523 +
524 +       // Symlink from inside memories to the sibling
525 +       await fs.symlink(siblingDir, path.join(memoriesDir, 'escape_link'),
    'dir');
526 +
527 +       await expect(
528 +         tool.view({
529 +           command: 'view',
530 +           path: '/memories/escape_link/secret.txt',
531 +         }),
532 +       ).rejects.toThrow('would escape /memories directory');
533 +     });
534 +
535 +     it('should reject path traversal to a sibling prefix-matching directory',
    async () => {
536 +       const siblingDir = path.join(tempDir, 'memories_backup');
537 +       await fs.mkdir(siblingDir, { recursive: true });
538 +       await fs.writeFile(path.join(siblingDir, 'secret.txt'), 'stolen data',
    'utf-8');
539 +
540 +       await expect(
541 +         tool.view({
542 +           command: 'view',
543 +           path: '/memories/../memories_backup/secret.txt',
544 +         }),
545 +       ).rejects.toThrow('would escape /memories directory');
546 +     });
547 +   });
548 +
513 549     describe('symlink validation', () => {
514 550       let outsideDir: string;
515 551
```

Comments 0

Please sign in to comment.