Gitlawb / **openclaude** Public

Code | Issues 83 | Pull requests 73 | Discussions | Actions | Projects

Commit 7002cb3

kevincodex1 authored 19 hours ago · ✓ 4 / 6 · Verified

```
fix: enforce Bash path constraints after sandbox allow (#777)
```

main (#777) · v0.5.2 v0.5.1

1 parent 739b8d1 commit 7002cb3

2 files changed +63 -1 lines changed

Top

Filter files...

- src/tools/BashTool
  - bashPermissions.test.ts
  - bashPermissions.ts

2 files changed +63 -1 lines changed

Search within code

src/tools/BashTool/bashPermissions.test.ts

```
@@ -0,0 +1,59 @@
+ import { afterEach, expect, test } from 'bun:test'
+
+ import { getEmptyToolPermissionContext } from '../../Tool.js'
+ import { SandboxManager } from '../../utils/sandbox/sandbox-adapter.js'
+ import { bashToolHasPermission } from './bashPermissions.js'
+
+ const originalSandboxMethods = {
+   isSandboxingEnabled: SandboxManager.isSandboxingEnabled,
+   isAutoAllowBashIfSandboxedEnabled:
+     SandboxManager.isAutoAllowBashIfSandboxedEnabled,
+   areUnsandboxedCommandsAllowed: SandboxManager.areUnsandboxedCommandsAllowed,
```

```
12  +   getExcludedCommands: SandboxManager.getExcludedCommands,
13  + }
14  +
15  + afterEach(() => {
16  +   SandboxManager.isSandboxingEnabled =
17  +     originalSandboxMethods.isSandboxingEnabled
18  +   SandboxManager.isAutoAllowBashIfSandboxedEnabled =
19  +     originalSandboxMethods.isAutoAllowBashIfSandboxedEnabled
20  +   SandboxManager.areUnsandboxedCommandsAllowed =
21  +     originalSandboxMethods.areUnsandboxedCommandsAllowed
22  +   SandboxManager.getExcludedCommands =
      originalSandboxMethods.getExcludedCommands
23  + })
24  +
25  + function makeToolUseContext() {
26  +   const toolPermissionContext = getEmptyToolPermissionContext()
27  +
28  +   return {
29  +     abortController: new AbortController(),
30  +     options: {
31  +       isNonInteractiveSession: false,
32  +     },
33  +     getAppState() {
34  +       return {
35  +         toolPermissionContext,
36  +       }
37  +     },
38  +   } as never
39  + }
40  +
41  + test('sandbox auto-allow still enforces Bash path constraints', async () => {
42  +   ;(globalThis as unknown as { MACRO: { VERSION: string } }).MACRO = {
43  +     VERSION: 'test',
44  +   }
45  +
46  +   SandboxManager.isSandboxingEnabled = () => true
47  +   SandboxManager.isAutoAllowBashIfSandboxedEnabled = () => true
48  +   SandboxManager.areUnsandboxedCommandsAllowed = () => true
49  +   SandboxManager.getExcludedCommands = () => []
50  +
```

```
+   const result = await bashToolHasPermission(
+     { command: 'cat ../../../../../etc/passwd' },
+     makeToolUseContext(),
+   )
+
+   expect(result.behavior).toBe('ask')
+   expect(result.message).toContain('was blocked')
+   expect(result.message).toContain('/etc/passwd')
+ })
```

src/tools/BashTool/bashPermissions.ts

```
@@ -1814,7 +1814,10 @@ export async function bashToolHasPermission(
1814 1814          input,
1815 1815          appState.toolPermissionContext,
1816 1816        )
1817      -     if (sandboxAutoAllowResult.behavior !== 'passthrough') {
     1817 +     if (
     1818 +       sandboxAutoAllowResult.behavior === 'deny' ||
     1819 +       sandboxAutoAllowResult.behavior === 'ask'
     1820 +     ) {
1818 1821          return sandboxAutoAllowResult
1819 1822        }
1820 1823      }
```

Comments 0

Please sign in to comment.