Command injection via server name in subprocess-backed install commands

Moderate **jlowin** published **GHSA-m8x7-r2rg-vh5g** last week

Package

FastMCP

Affected versions

<3.2.0

Patched versions

3.2.0

Description

Server names containing shell metacharacters (e.g., `&`) can cause command injection on Windows when passed to `fastmcp install claude-code` or `fastmcp install gemini-cli`. These install paths use `subprocess.run()` with a list argument, but on Windows the target CLIs often resolve to `.cmd` wrappers that are executed through `cmd.exe`, which interprets metacharacters in the flattened command string.

PoC:

```python
from fastmcp import FastMCP

mcp = FastMCP(name="test&calc")

@mcp.tool
def roll_dice(n_dice: int) -> list[int]:
    """Roll `n_dice` 6-sided dice and return the results."""
    return [random.randint(1, 6) for _ in range(n_dice)]
```

```
fastmcp install claude-code server.py   # or: fastmcp install gemini-cli server.py
```

On Windows, this opens Calculator via the `&calc` in the server name.

Impact:
Arbitrary command execution with the privileges of the user running `fastmcp install`. Affects Windows hosts where the target CLI (one of claude, gemini) is installed as a `.cmd` wrapper. Does not affect macOS/Linux, and does not affect config-file-based install targets (cursor, goose, mcp-json).

Patched in #3522 by validating server names to reject shell metacharacters.

Severity

Moderate 6.7 / 10

CVSS v3 base metrics

Attack vector	Local
Attack complexity	High
Privileges required	Low
User interaction	Required
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

Learn more about base metrics

CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H

CVE ID

CVE-2025-64340

Weaknesses

▶ CWE-78

Credits

nil340 Reporter