

Path-traversal staging in mcp-server-git git_add (CVE-2026-27735)

PRIMARY

Publisher	NVD
Published	2026-02-26
Retrieved	2026-10-19
Cite key	nvd2026pathtrave
URL	https://nvd.nist.gov/vuln/detail/CVE-2026-27735

Assessment. Primary vendor-adjacent record. Status Analyzed. Fixed in 2026.1.14, before the paper appeared.

Claims drawn from this source. CLAIM-2026-10-19-04, CLAIM-2026-10-19-06

NVD record, retrieved 2026-10-19. Published 2026-02-26. vulnStatus: Analyzed.

Description. "Model Context Protocol Servers is a collection of reference implementations for the model context protocol (MCP). In mcp-server-git versions prior to 2026.1.14, the git_add tool did not validate that file paths provided in the files argument were within the repository boundaries. Because the tool used GitPython's repo.index.add() rather than the Git CLI, relative paths containing ../ sequences that resolve outside the repository were accepted and staged into the Git index. Users are advised to upgrade to 2026.1.14 or newer to remediate this issue."

Scoring. CVSS v3.1 base 6.5 MEDIUM; CVSS v4.0 base 6.4 MEDIUM.

References. [github.com/modelcontextprotocol/servers pull/3164](https://github.com/modelcontextprotocol/servers/pull/3164); advisory GHSA-vjqx-cfc4-9h6v.