Trust Dialog Bypass via Git Worktree Spoofing Allows Arbitrary Code Execution

High **OctavianGuzu** published **GHSA-q5hj-mxqh-vv77** 2 weeks ago

Package

@anthropic-ai/claude-code (npm)

Affected versions

>= 2.1.63, < 2.1.84

Patched versions

2.1.84

Description

Claude Code used the git worktree `commondir` file when determining folder trust but did not validate its contents. By crafting a repository with a `commondir` file pointing to a path the victim had previously trusted, an attacker could bypass the trust dialog and immediately execute malicious hooks defined in `.claude/settings.json`. Exploiting this required the victim to clone a malicious repository and run Claude Code within it, and for the attacker to know or guess a path the victim had already trusted.

Users on standard Claude Code auto-update have received this fix already. Users performing manual updates are advised to update to the latest version.

Thank you to hackerone.com/masato_anzai for reporting this issue.

Severity

High 7.7 / 10

CVSS v4 base metrics

Exploitability Metrics

Attack Vector	Network
Attack Complexity	Low

Attack Requirements	Present
Privileges Required	None
User interaction	Passive
Vulnerable System Impact Metrics	
Confidentiality	High
Integrity	High
Availability	High
Subsequent System Impact Metrics	
Confidentiality	None
Integrity	None
Availability	None

Learn more about base metrics

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CVE ID

CVE-2026-40068

Weaknesses

- CWE-20
- CWE-77