Sandbox Escape via Symlink Following Allows Arbitrary File Write Outside Workspace

High **OctavianGuzu** published **GHSA-vp62-r36r-9xqp** 15 hours ago

Package

@anthropic-ai/claude-code (npm)

Affected versions

< 2.1.64

Patched versions

2.1.64

Description

Claude Code's sandbox did not prevent sandboxed processes from creating symlinks pointing to locations outside the workspace. When Claude Code subsequently wrote to a path within such a symlink, its unsandboxed process followed the symlink and wrote to the target location outside the workspace without prompting the user for confirmation. This allowed a sandbox escape where neither the sandboxed command nor the unsandboxed app could independently write outside the workspace, but their combination could write to arbitrary locations, potentially leading to code execution outside the sandbox. Reliably exploiting this required the ability to add untrusted content into a Claude Code context window to trigger sandboxed code execution via prompt injection.

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

Thank you to hackerone.com/philts 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-2026-39861

Weaknesses

- ▶ CWE-22
- ▶ CWE-61