Memory Tool Path Validation Race Condition Allows Sandbox Escape

Moderate **localden** published **GHSA-w828-4qhx-vxx3** 4 hours ago

Package

anthropic (pip)

Affected versions

>= 0.86.0, < 0.87.0

Patched versions

0.87.0

Description

The async local filesystem memory tool in the Anthropic Python SDK validated that model-supplied paths resolved inside the sandboxed memory directory, but then returned the unresolved path for subsequent file operations. A local attacker able to write to the memory directory could retarget a symlink between validation and use, causing reads or writes to escape the sandbox. The synchronous memory tool implementation was not affected.

Users on the affected versions are advised to update to the latest version.

Thank you to hackerone.com/kasthelord for reporting this issue!

Severity

Moderate 5.8 / 10

CVSS v4 base metrics

Exploitability Metrics

Attack Vector	Local
Attack Complexity	High
Attack Requirements	None
Privileges Required	Low
User interaction	None

Vulnerable System Impact Metrics	
Confidentiality	High
Integrity	Low
Availability	None
Subsequent System Impact Metrics	
Confidentiality	None
Integrity	None
Availability	None

Learn more about base metrics

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

CVE ID

CVE-2026-34452

Weaknesses

- CWE-59
- CWE-367