

# Loopjacking: When Your AI Agent Approves A, Runs B

## SECONDARY

|                  |                                                                                                                                                             |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Publisher</b> | byteiota                                                                                                                                                    |
| <b>Published</b> | 2026-09-24                                                                                                                                                  |
| <b>Retrieved</b> | 2026-09-24                                                                                                                                                  |
| <b>Cite key</b>  | byteiota2026loopjacki                                                                                                                                       |
| <b>URL</b>       | <a href="https://byteiota.com/loopjacking-when-your-ai-agent-approves-a-runs-b/">https://byteiota.com/loopjacking-when-your-ai-agent-approves-a-runs-b/</a> |

Published 24 September 2026. Reports the paper (arXiv 2609.21081, 17 September 2026): LangGraph Agent Server post-approval substitution 'reproduced across 12 tested versions, up through v0.14.0'; Agno AgentOS 'reproduced in seven releases from v2.5.6 through v3.0.9'; OpenAI Agents SDK v0.22.0 and v0.22.2 resistant. OpenClaw not mentioned.

Vendor response reported: 'The Agno team has merged nine authorization guard fixes in PR #10270', with a recommendation to verify 'whether your deployment has pulled that update'. No LangChain or OpenAI response reported.

Handling note: this is where the Agno pull request is placed beside the research. Reading the pull request shows its content is endpoint authorization, not approval binding, so the juxtaposition should not be read as a fix for the class.