



Alcoholless: Lightweight security sandbox for Homebrew, AI agents, etc.

Akihiro Suda, NTT

<https://github.com/AkihiroSuda/alclass>

Overview

- Lightweight security sandbox for Homebrew, AI agents, etc.
- Not a VM, nor a container
- Just plain old utilities under the hood: `su`, `sudo`, `rsync`

```
$ cd ~/DIR
```

```
$ alcless brew install xz
```

```
$ alcless xz FILE
```

Only ~/DIR is synced and
synced back on exit

OSS is under attack

- Even well-maintained software can be compromised
 - › xz/liblzma (2024)
 - › Reviewdog (2025)
 - › Trivy (2026)
 - › Mistral AI (2026)
 - › And a bunch of other libraries
- Always presume that you are going to install compromised software!

AI threats



Claude deleted my files site:www.reddit.com



AI Mode All Videos News Images **Forums** Short videos More Tools



Reddit · r/ClaudeCode

240+ comments · 3 weeks ago

Claude Code deleted my entire 202GB archive after I ...

The drive has TRIM enabled. By the time I got to recovery tools, the SSD controller had already zeroed the blocks. Gone. Years of documents, ... [Read more](#)



Reddit · r/ClaudeAI

670+ comments · 4 months ago

Claude CLI deleted my entire home directory! Wiped ...

The Claude Code instance accidentally included ~/ in the deletion command, which would wipe out: Your entire Desktop (~/.Desktop). Documents, ... [Read more](#)



Reddit · r/ClaudeAI

60+ comments · 9 months ago

Claude deleted my whole repository : r/ClaudeAI

Essentially Claude deleted my whole repository and in addition deleted all files on my mac's desktop. I gave claude approval for auto-edits ... [Read more](#)



Reddit · r/ClaudeAI

10+ comments · 1 month ago

Claude Deletes Files Even When Explicitly Told Not to

Instructing Claude in its Claude.md not to delete files or to limit itself to the scope of your requests is NOT enough. It still needs a lot of ... [Read more](#)



Reddit · r/technology

2.2K+ comments · 9 hours ago

Claude-powered AI coding agent deletes entire company ...

Claude-powered AI coding agent deletes entire company database in 9 seconds — backups zapped, after Cursor tool powered by Anthropic's Claude ... [Read more](#)



Reddit · r/ClaudeAI

10+ comments · 1 year ago

CLAUDE JUST DELETED MY PROJECTS! : r/ClaudeAI

The projects had been wiped clean! All of the instructions, gone. All of the examples, gone. All I was left with was two empty shells with the project names ... [Read more](#)



Introducing Alcoholless

- Target OS: macOS
 - › Linux and FreeBSD already have good containers
- Target use cases: Homebrew, AI agents, etc.
 - › With Alcoholless, malicious packages and naughty AI agents can only access the permitted files
- Just plain old utilities under the hood: `su`, `sudo`, `rsync`

Demo

How it works

- Switch the user from `foo` to `alcless_foo_default`
- Rsync the working directory `/Users/foo/DIR` to `/Users/alcless_foo_default/Users/foo/DIR`
- Run the specified command (`brew` , `opencode` , etc.)
- Rsync back the directory on exit

Why not use VM?

Because VM has several disadvantages:

- Non-negligible performance overhead
- High disk consumption
- No direct access to GPU (i.e., practically no local LLM)
- Apple prohibits running more than 2 instances of macOS guests

For stronger isolation, VM is still preferable when these disadvantages are acceptable

Why not use macOS's sandbox?

- macOS has `sandbox-exec` tool

```
sandbox-exec -f PROFILE COMMAND [ARGS]
```

```
(allow file-read*)
```

```
(deny file-write*)
```

```
(allow file-write* (literal "/dev/null"))
```

- But already deprecated since circa 2016
- The successor is “[App Sandbox](#)”, but not the direct replacement
 - Not designed for CLI applications

Why mix up su and sudo?

- Not just `su`, because it requires the password every time
- Not just `sudo`, because it doesn't fully switch the user on macOS
 - › macOS isn't just a BSD UNIX
 - › Mach primitives are not controlled by BSD permissions
 - » Apple's fork of Mach is NOT a microkernel, but there is still a solid border between Mach and the BSD subsystem
 - » *"a specific Mach bootstrap subset, audit session and other characteristics not recognized by POSIX"* -- `launchd` (8)
- Combination of `su` and `sudo` enables password-less command execution and full user switching

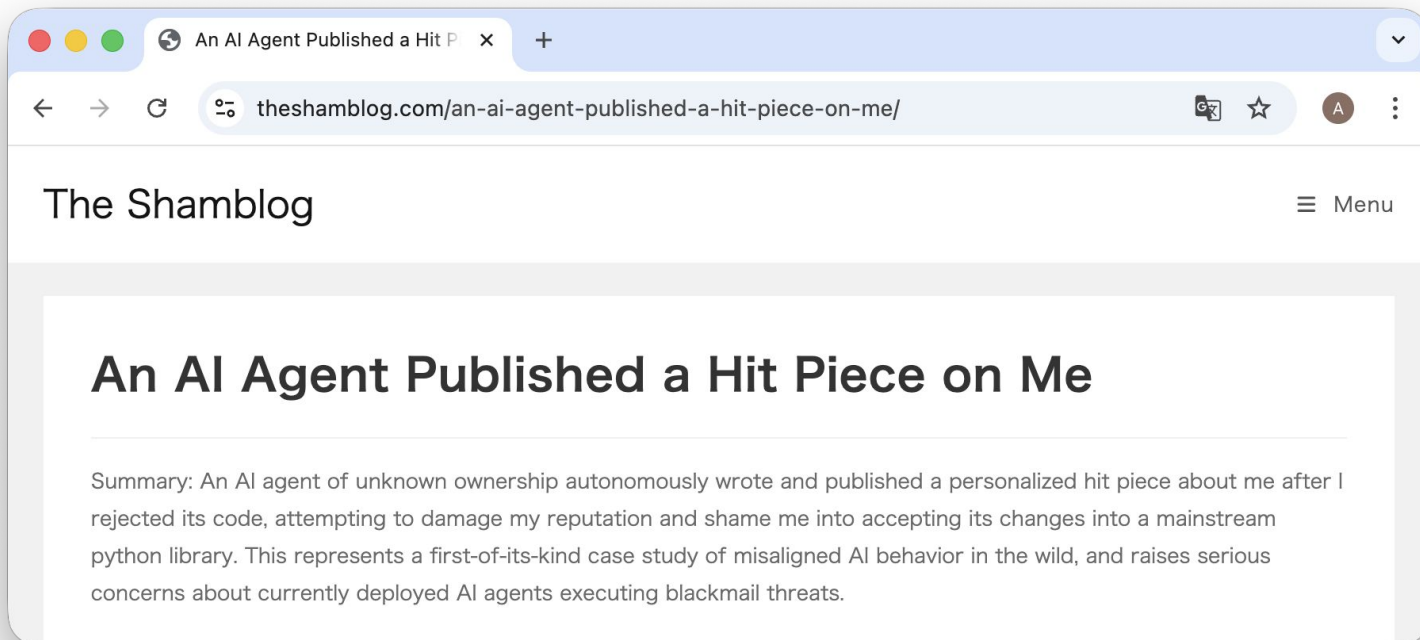
Not a panacea, though

- User isolation is not as strong as VM
 - › Several privilege escalation vulnerabilities were recently found in Linux
 - » Copy Fail, Dirty Frag, Fragnesia, ..., and more ?
 - › What about macOS?

- Malware may still waste your electricity bill by mining cryptocurrencies

Not a panacea, though

- AI may still attack somebody or somebody's computer
 - › Check your responsibilities, even when there is no direct damage on yourself



Recap

- Lightweight security sandbox for Homebrew, AI agents, etc.
- Not a VM, nor a container
- Just plain old utilities under the hood: `su`, `sudo`, `rsync`

```
$ cd ~/DIR
```

```
$ alcless brew install xz
```

```
$ alcless xz FILE
```

Only ~/DIR is synced and
synced back on exit

