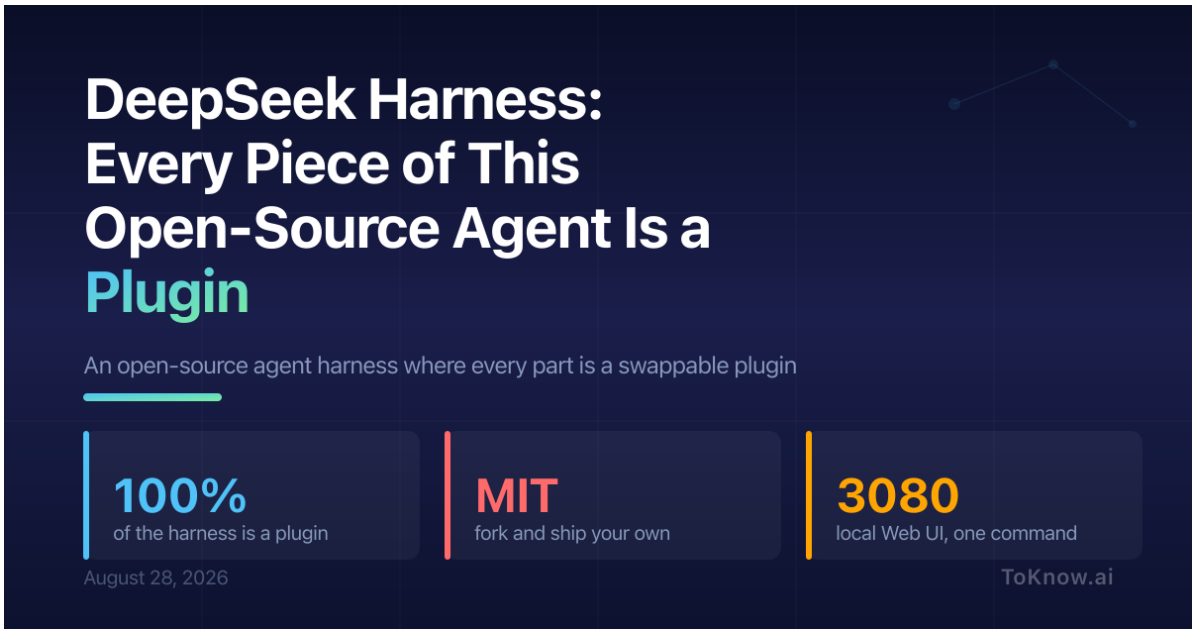
DeepSeek Harness: Every Piece of This Open-Source Agent Is a Plugin

Kabui, Charles

2026-08-28

Read at ToKnow.ai



DeepSeek Harness (`dsh`) is an open-source agent harness from DeepSeek AI where every part is a plugin. The model adapter, the tool registry, the session log, and the agent loop itself load as plugins into one context; none is privileged or baked in. The framework underneath is Cordis, described in a companion research paper. Remove a plugin and its effects fully undo; add a tool, model provider, or permission rule and it plugs in beside the rest. Run

`npx @deepseek-ai/dsh web` to get a local Web UI where the agent reads and edits files in a workspace, runs commands, and delegates work, asking before actions your policy blocks. It is MIT-licensed and in developer preview, with breaking changes expected.

Because the loop is replaceable, dsh is a direct answer to the "which agent do I build on" problem. Point it at any OpenAI-compatible model endpoint, drop in community plugins, and ship your setup as a bundle others can patch, all under MIT. A solo developer gets tooling that is no longer a black box, and a team can fork the whole stack. The security story is honest: the harness runs model-generated code and loads third-party plugins, and its safety notice says sandboxing reduces but does not guarantee isolation, so the recommended setup is least privilege in a disposable virtual machine.

DeepSeek open-sourcing the whole harness, not just a model, makes the scaffolding the thing teams can own. That is the direct counter to closed agent products, and it moves the real constraint from capability to running untrusted plugins safely.

Read More: see how the 2026 coding agent market splits between gateway-first and agent-first tools.

Sources:

- DeepSeek Harness: Everything Is a Plugin (GitHub)
- DeepSeek Harness documentation, Use the Web UI
- Cordis: Meta-Framework of Spatiotemporal Composability (GitHub)
- The design paper behind Cordis (arXiv)
- DeepSeek Harness Safety Notice (GitHub)

Disclaimer: *For information only. Accuracy or completeness not guaranteed. Illegal use prohibited. Not professional advice or solicitation.* ***Read more:*** */terms-of-service*