THE CYBER TOOLCHAIN

NO. 005

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED JULY 5, 2026 · EVERY WEEKDAY

The daily firehose — everything the toolchain shipped today, already filtered.

▸ // HOW THIS ISSUE IS MADE SHOW

VIEW

ISSUE VIEW

scroll



SCROLL | EXPAND IN PLACE | PREVIEW PANE

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 2 tools

BUILD

◆ AI Coding Agents

OpenAI Codex CLI `rust-v0.143.0-alpha.36` PRE-RELEASE

Lightweight coding agent that runs in your terminal

Codex CLI now exposes remote plugin marketplace versions in plugin listings.

└──▷ GET THIS VERSION

```
$ git clone --branch rust-v0.143.0-alpha.36
https://github.com/openai/codex.git
# already have the repo? check out this version:
$ git checkout rust-v0.143.0-alpha.36
```

- Adds `PluginSummary.version` field to surface version numbers advertised by remote plugin marketplaces.
- Preserves backend release version in `plugin/installed` responses alongside `localVersion` for the locally installed package.
- Supports object-valued buffering signals in streamed response events, enabling the buffering UI and using the faster-model field from the payload with fallback to existing response metadata.

WAS THIS USEFUL? 👍 👎

Windsurf snapshot-20260705

Windsurf is an AI-powered code editor that helps developers write, edit, and navigate code faster using intelligent autocomplete and agentic AI assistance.

Windsurf v3.4.22 adds sandbox command exclusions, MCP status panel, reviewable local-edit diffs, and enterprise CLI login policy enforcement.

└──▷ HOW TO FIND IT

Allow a specific build tool to run outside the agent sandbox so it has direct environment access — useful when the sandbox proxy breaks native toolchain behavior.

> 📍 In Devin Desktop, go to Settings and add an entry under sandbox.excluded with allow/ask/deny for the specific command (e.g., set the command to `make` with policy `allow` in the sandbox.excluded user or team config).

Check which MCP servers are live and their current status without leaving the chat interface.

```
$ /mcp
```

Review current ACU consumption at any point during a session to track quota usage.

```
$ /usage
```

- Adds a `sandbox.excluded` allow/ask/deny config (user and team settings) to run specific commands outside the agent sandbox, bypassing the sandbox proxy environment for those commands.
- Adds an `/mcp` slash command with a live MCP server status panel for inspecting connected MCP servers.
- ACU usage is now shown in the `/usage` command.
- Edits produced in Devin Local autonomous mode now produce reviewable diffs.
- Skill permissions: frontmatter now applies to auto-approvals.

+5 more

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · July 5, 2026

Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe