THE CYBER TOOLCHAIN

NO. 004

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED JULY 4, 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 3 tools

BUILD

◆ AI Coding Agents

Claude Code v2.1.200

Claude Code is an agentic coding tool that lives in your terminal, understands your codebase, and helps you code faster by executing routine tasks, explaining complex code, and handling git workflows - all through natural language commands.

Claude Code v2.1.200 makes Manual the default permission mode and adds opt-in idle timeout for user-question dialogs.

└──▷ GET THIS VERSION

```
$ git clone --branch v2.1.200 https://github.com/anthropics/claude-code.git
# already have the repo? check out this version:
$ git checkout v2.1.200
```

└──▷ TRY IT

Enforce Manual permission mode explicitly in automation or shared configs to match the new canonical name.

```
$ claude --permission-mode manual
```

- Changes `AskUserQuestion` dialogs to no longer auto-continue by default; opt into an idle timeout via `/config`.
- Renames the 'default' permission mode to 'Manual' across CLI, `--help`, VS Code, and JetBrains; accepts `--permission-mode manual` and `"defaultMode": "manual"` as canonical values.

└──▷ BREAKING ON UPGRADE

- ! The `AskUserQuestion` dialogs no longer auto-continue by default; auto-continue must be explicitly opted into via `/config`
- ! The default permission mode is renamed from "default" to "Manual" across the CLI, `--help`, VS Code, and JetBrains (though `--permission-mode default` and `"defaultMode": "default"` remain accepted alongside `manual`)

WAS THIS USEFUL? 👍 👎

Cline

cli-v3.0.37 · 2 RELEASES · 2026-07-03 → 2026-07-04 · LATEST · STABLE

Autonomous coding agent as an SDK, IDE extension, or CLI assistant.

Cline CLI now surfaces plan/act mode switches to the model and handles malformed tool calls from weaker LLMs.

└──▷ GET THIS VERSION

```
$ git clone --branch cli-v3.0.37 https://github.com/cline/cline.git
# already have the repo? check out this version:
$ git checkout cli-v3.0.37
```

- Adds plan/act mode-switch notices to the model's message stream, so it understands when you toggle modes mid-session instead of silently receiving a swapped system prompt.
- Supports graceful handling of malformed tool calls (wrong argument types, truncated JSON) from weaker models such as DeepSeek, allowing execution to continue rather than erroring out.

▾ 1 more release in this issue · 2026-07-03 → 2026-07-04

cli-v3.0.35 · STABLE

Cline CLI v3.0.35 adds ClinePass for all users, Tencent TokenHub provider, and updated model catalog.

└──▷ GET THIS VERSION

```
$ git clone --branch cli-v3.0.35 https://github.com/cline/cline.git
# already have the repo? check out this version:
$ git checkout cli-v3.0.35
```

- Enables ClinePass for all CLI users.
- Adds Tencent TokenHub as a supported AI provider.
- Refreshes the bundled model catalog with the latest provider models.
- Formats structured run_commands objects correctly in history exports.
- Recovers missing interactive sessions when reading messages.

WAS THIS USEFUL? 👍 👎

Windsurf snapshot-20260704

Windsurf is an AI-powered code editor that enhances developer productivity by integrating intelligent coding assistance, autocomplete, and agentic workflows directly into the development environment.

Windsurf v3.4.22 adds reviewable diffs, MCP status panel, sandbox exclusion controls, and ACU usage tracking.

└──▷ USE IT

Allowlist a specific command to run outside the agent sandbox — useful when a trusted internal tool must bypass sandbox proxy restrictions.

```yaml
# In team or user settings config:
sandbox:
  excluded:
    - command: "my-internal-scanner"
      policy: allow
```

Check live MCP server connectivity status directly from a Devin Local chat session.

```
$ /mcp
```

Review current ACU consumption without leaving the agent session.

```
$ /usage
```

- Adds reviewable diffs for edits produced in Devin Local autonomous mode, enabling practitioners to inspect and approve AI-generated changes before they land.
- New `/mcp` slash command surfaces a live MCP server status panel, giving visibility into connected MCP server health at a glance.
- ACU usage is now shown in the `/usage` command, letting users track agent compute consumption without leaving the session.
- New sandbox.excluded config (user and team level) allows specific commands to run outside the sandbox with allow/ask/deny controls — and excluded commands also bypass the sandbox proxy environment.
- Skill permissions: frontmatter now applies to auto-approvals, enabling fine-grained control over which skills can be auto-approved.

+4 more

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · July 4, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe