THE CYBER TOOLCHAIN

NO. 008

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED JULY 8, 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 10 tools

NETWORK SECURITY

◆ Firewalls & Network Defense

Cloudflare

Your Worker can now have its own cache in front of it (2026-07-06)

Cloudflare Blog is an official publication sharing updates, technical insights, and announcements about Cloudflare's internet security, performance, and networking products and services.

Cloudflare Workers Cache adds a tiered cache in front of Workers, configured via Wrangler and standard Cache-Control headers.

.
.
.
.

└──▷ USE IT

Enable Workers Cache for a Worker so Cloudflare's cache layer handles repeat requests before your code runs, eliminating CPU cost on cache hits.

```json
{
  "name": "my-worker",
  "main": "src/index.ts",
  "compatibility_date": "2026-05-01",
  "cache": {
    "enabled": true
  }
}
```

Serve a server-rendered page at cache speed for most visitors while keeping content fresh — fresh for 5 min, stale-served for up to 1 hour while background revalidation runs.

```javascript
return new Response(html, {
  headers: {
    "Content-Type": "text/html; charset=utf-8",
    "Cache-Control": "public, max-age=300, stale-while-
revalidate=3600",
  },
});
```

Purge cached entries for a specific product after an inventory update, without touching any other Worker's or zone's cached content.

```javascript
await ctx.cache.purge({ tags: ["product:123"] });
```

- New Workers Cache: a tiered cache that sits in front of a Worker, enabled with a single `cache.enabled` block in `wrangler.toml`, so cacheable requests never invoke Worker code or incur CPU billing.
- Supports `stale-while-revalidate` — stale responses are served instantly while the Worker re-renders in the background, so no user ever waits on a cache refresh.
- Supports standard `Vary` header for content negotiation, storing separate cache variants per distinct header combination (e.g., `Accept`, `Accept-Language`) with no allowlist restrictions.
- New ctx.cache.purge() API enables Workers to programmatically purge their own cache by tag (`tags: ["product:123"]`), path prefix, or everything — scoped to the Worker entrypoint, not the zone.
- Cache follows the Worker, not the hostname — a single Worker's cache is shared across custom domains, `workers.dev`, service bindings, preview URLs, and Workers for Platforms tenants.

+2 more

WAS THIS USEFUL? 👍 👎

CLOUD & CONTAINER SECURITY

◆ Cloud Security Posture

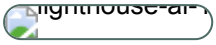
Prowler 5.33.0

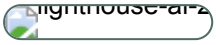
Prowler is the world's most widely used open-source cloud security platform that automates security and compliance across any cloud environment.

Prowler 5.33.0 adds agentic Lighthouse AI assistant, credential-free compliance PDFs, and scan queueing.

└──▷ GET THIS VERSION

```
$ git clone --branch 5.33.0 https://github.com/prowler-cloud/prowler.git
# already have the repo? check out this version:
$ git checkout 5.33.0
```





- New Lighthouse AI agentic assistant (Prowler Cloud/Enterprise) queries findings, compliance posture, and risky resources using configurable LLM providers (OpenAI, Amazon Bedrock, or any OpenAI-compatible endpoint).
- Persistent chat sessions with real-time streaming, session history, archiving, and a sidebar chat mode accessible from any page in the Prowler Cloud UI.
- Compliance PDF reports now generate without active provider credentials, drawing on provider metadata stored in the database.
- Overlapping scans for the same provider now queue behind the active scan instead of running concurrently, eliminating duplicate or racing scan workers.
- Kubernetes provider rejects kubeconfigs using `exec` authentication in Prowler Cloud, blocking user-supplied commands from executing on Cloud workers.

WAS THIS USEFUL? 👍 👎

EXPOSURE & VULNERABILITY MANAGEMENT

◆ Vulnerability Management

Rapid7 Insight Platform

Cloud Security (InsightCloudSec) Release Notes (2026-07-07)

Rapid7 Insight Platform is a cloud-based security operations platform that unifies vulnerability management, detection, response, and threat intelligence across an organization's IT environment.

InsightCloudSec 26.7.7 adds ASG/EBS/Security Group insights, enhanced credential cleanup, and CIS RHOCP v1.9.0 benchmark support.

- New Insights added for Auto Scaling Groups, EBS Volumes, and Security Groups.
- Enhanced credential cleanup capabilities.
- Adds support for CIS Red Hat OpenShift Container Platform Benchmark v1.9.0.

WAS THIS USEFUL? 👍 👎

defectdojo 3.1.0

Open-Source Unified Vulnerability Management, DevSecOps & ASPM

DefectDojo 3.1.0 adds new parsers, JIRA multi-component support, AES-256-GCM credential encryption, and import/deduplication sync control.

└──▷ GET THIS VERSION

```
$ git clone --branch 3.1.0 https://github.com/DefectDojo/django-DefectDojo.git
# already have the repo? check out this version:
$ git checkout 3.1.0
```

- Adds Garak (NVIDIA LLM vulnerability scanner) parser for AI/LLM security findings.
- Adds Govulncheck Scanner V2 parser for Go vulnerability results.
- Adds PICUS Breach and Attack Simulation CSV parser.
- Supports multiple JIRA components in project settings.
- Supports CVSS vector parsing and severity derivation in the cargo-audit parser.

+14 more

WAS THIS USEFUL? 👍 👎

BUILD

◆ AI Coding Agents

Claude Code v2.1.202

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 v2.1.202 adds dynamic workflow sizing, OTel workflow attributes, and a new `/code-review` command for multi-agent PR review.

└──▷ GET THIS VERSION

```
$ git clone --branch v2.1.202 https://github.com/anthropics/claude-code.git
# already have the repo? check out this version:
$ git checkout v2.1.202
```

└──▷ TRY IT

Run a thorough multi-agent review on a PR when you want deeper analysis than the default single-pass review.

```
$ /code-review high 4821
```

Tune agent parallelism for a complex workflow without hitting a hard cap — useful before kicking off a large refactor.

📍 `/config`

- Adds a 'Dynamic workflow size' setting in `/config` to guide how many agents Claude spawns for dynamic workflows (small/medium/large) — advisory, not an enforced cap.
- Adds `workflow.run_id` and `workflow.name` OpenTelemetry attributes to telemetry from workflow-spawned agents, enabling full reconstruction of a workflow run from OTel data.
- Introduces `/code-review <level> <pr#>` for multi-agent PR review at a chosen effort level; `/review <pr>` reverts to a fast single-pass review.
- Improves `/workflows` agent list layout with wider titles, a dedicated time column, and shorter model names.
- Improves MCP error messages to suggest `"type": "http"` when a server config has `url` but no `type`.

WAS THIS USEFUL? 👍 👎

Cline cli-v3.0.38

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

Cline CLI v3.0.38 refreshes the plan/act UI palette, rethinks chat input styling, and raises the default context window for under-specified models to 128K.

└──▷ **GET THIS VERSION**

```
$ git clone --branch cli-v3.0.38 https://github.com/cline/cline.git
# already have the repo? check out this version:
$ git checkout cli-v3.0.38
```

- New plan/act accent palette: act mode switches to blue (#79b8ff) and plan mode to amber, replacing the old cyan/yellow — applied across dialogs, model selector, config, onboarding, markdown, and syntax highlighting with light-theme contrast variants.
- Restyled chat input: minimal full-width horizontal-rule frame with a bold accent prompt glyph (❯) and slimmer user-message bubbles, replacing the tinted background.
- Assistant markdown accents are now tinted by the plan/act mode in which they were produced.
- Thinking-level picker now defaults its cursor to Medium instead of Off.
- Models in the live catalog that don't report a context window now default to a 128K input-token limit instead of 4K, giving under-specified models a usable context budget.

+1 more

WAS THIS USEFUL? 👍 👎

OpenHands

cloud-1.41.0 · 2 RELEASES · 2026-07-06 · LATEST · STABLE

OpenHands: AI-Driven Development

OpenHands 1.41 adds API key time windows, parallel tool calls, org admin dashboard, and semantic file chunking.

└──▷ GET THIS VERSION

```
$ git clone --branch cloud-1.41.0
https://github.com/OpenHands/OpenHands.git
# already have the repo? check out this version:
$ git checkout cloud-1.41.0
```

└──▷ TRY IT

Create an API key that is only valid within a specific time window — useful for temporary contractor access or scheduled automation.

```
$ curl -X POST https://app.openhands.ai/api/api-keys \
  -H 'Authorization: Bearer <your-token>' \
  -H 'Content-Type: application/json' \
  -d '{"name": "ci-bot", "not_before": "2026-08-01T00:00:00Z",
"expires_at": "2026-08-31T23:59:59Z"}'
```

Check what permissions your service account has within an organization before attempting privileged operations.

```
$ curl -X GET https://app.openhands.ai/api/organizations/<org-id>/me
\
  -H 'Authorization: Bearer <your-token>'
```

Enable parallel tool calls in agent settings to let the agent execute multiple tools concurrently and reduce round-trip latency on complex tasks.

> 📍 In the console, go to Settings › Agent and set tool_concurrency_limit to the desired maximum number of concurrent tool calls (e.g. 4).

- Adds semantic file chunking via tree-sitter AST parsing for more accurate code context in agent sessions.
- New organization conversation admin dashboard lets org admins review and manage all

conversations across their org.

- Captures production workspace state as an initial snapshot on start and archives it before deletion.
- Adds super roles via user.role_id with permission fallback for enterprise/auth authorization.
- Exposes caller permissions on GET `/organizations`/{id}`/me` so clients can check what actions they're allowed to take.

+6 more

▾ **1 more release in this issue** · 2026-07-06

1.9.0 STABLE

OpenHands 1.9.0 adds Azure DevOps resolver, multi-model discovery, MCP config for ACP agents, sub-agent visualizer, and org admin tooling.

└──▷ GET THIS VERSION

```
$ git clone --branch 1.9.0
https://github.com/OpenHands/OpenHands.git
# already have the repo? check out this version:
$ git checkout 1.9.0
```

└──▷ USE IT

Hide personal workspaces on an org-only OHE install so users only see org workspaces.

```ini
OH_HIDE_PERSONAL_WORKSPACES=true
OH_DEPLOYMENT_MODE=enterprise
```

Set a per-deployment resolver label and restrict resolver to enterprise cloud mode.

```ini
OH_RESOLVER_LABEL=my-team-resolver
OH_DEPLOYMENT_MODE=enterprise_cloud
```

Switch the LLM model mid-conversation for a cloud ACP agent via the proxy endpoint.

```
$ curl -X POST https://<your-openhands-
host>/api/acp/switch_acp_model \
  -H 'Authorization: Bearer <api_key>' \
  -H 'Content-Type: application/json' \
  -d '{"conversation_id": "<conversation_id>", "model": "gpt-4o"}'
```

- Adds `hide_personal_workspaces` flag for org-only OHE installs to enforce org-scoped workspaces.
- New `switch_acp_model` proxy endpoint enables model switching for cloud ACP conversations.
- Adds model dropdown and credential fields to the ACP agent settings page.
- Adds validation for secret names to ensure valid environment-variable format.
- Exposes copyable invite links so org invitations work without email delivery.

+33 more

WAS THIS USEFUL? 👍 👎

OpenCode v1.17.14

The open source coding agent.

Adds a code-mode MCP adapter for confined orchestration scripting, an OpenAPI tool adapter, and a gated `execute` tool for code-mode sessions.

└──▷ GET THIS VERSION

```
$ git clone --branch v1.17.14
https://github.com/anomalyco/opencode.git
# already have the repo? check out this version:
$ git checkout v1.17.14
```

- Adds a code-mode MCP adapter enabling confined orchestration scripts to run against connected MCP tools.
- Adds an OpenAPI tool adapter for code-mode, expanding available tool integrations.
- Gates the `execute` tool behind a code-mode flag so it only surfaces when code mode is active.
- Desktop: adds recently closed projects to the Home screen for quick re-entry.
- Desktop: adds reopening of closed tabs and background tab opening.

+5 more

WAS THIS USEFUL? 👍 👎

Windsurf `snapshot-20260707`

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

Windsurf snapshot-20260707 adds reviewable diffs in autonomous mode, `/mcp` status panel, sandbox exclusion config, and ACU usage tracking.

└──▷ TRY IT

Check live MCP server connectivity and status mid-session to confirm tools are available before delegating an agentic task.

```
$ /mcp
```

Review current ACU consumption to stay within quota before kicking off a long autonomous run.

```
$ /usage
```

Allow a specific high-trust command (e.g., a deployment script) to run outside the sandbox at the team level so it isn't blocked by the sandbox proxy.

> 📍 In Settings › Team Settings, add the command under sandbox.excluded with the desired allow/ask/deny value.

- Adds reviewable diffs for edits produced in Devin Local autonomous mode, enabling structured review before changes are applied.
- Skill permissions: frontmatter now applies to auto-approvals, enabling fine-grained control over which skills are auto-approved.

WAS THIS USEFUL? 👍 👎

PLATFORMS & UTILITIES

◆ General Utilities & Libraries

arsenal-ng v1.5

The classic launcher, evolved. Fast, Go-based command library equipped with 200+ cybersecurity cheat-sheets.

arsenal-ng v1.5 expands its built-in cheatsheet library, growing to 242 tools and 2,872 commands.

└──▷ GET THIS VERSION

```
$ git clone --branch v1.5 https://github.com/halilkirazkaya/arsenal-ng.git
# already have the repo? check out this version:
$ git checkout v1.5
```

› Adds new pentest tools to the built-in cheatsheet library, bringing the total to 242 tools and 2,872 commands.

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · July 8, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe