THE CYBER TOOLCHAIN

NO. 011

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED JULY 10, 2026 · EVERY DAY

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 12 tools

OFFENSIVE SECURITY

vim ? help

◆ Reconnaissance & OSINT

ProjectDiscovery httpx-toolkit ⓘ v1.10.0 NOTES ↗

httpx is a fast and multi-purpose HTTP toolkit that allows running multiple probes using the retryablehttp library.

httpx v1.10.0 adds duplicate custom request headers, IP-aware deduplication, and automatic `HTTP_PROXY` env var support.

└──▷ GET THIS VERSION

```
$ git clone --branch v1.10.0
https://github.com/projectdiscovery/httpx.git
# already have the repo? check out this version:
$ git checkout v1.10.0
```

└──▷ TRY IT

Inject multiple instances of the same header (e.g., to test WAF bypass or header-smuggling behavior) in a single httpx probe.

```
$ httpx -u https://target.example.com -H 'X-Forwarded-For: 127.0.0.1'
-H 'X-Forwarded-For: 10.0.0.1' -sc -title
```

Route all httpx traffic through a proxy without adding the `-proxy` flag — useful in CI pipelines where the proxy is already set in the environment.

```
$ HTTP_PROXY=http://proxy.corp.example.com:8080 httpx -l targets.txt
-sc -title -td
```

- Supports sending duplicate custom request headers in a single request (e.g., multiple `X-Forwarded-For` values).
- Adds IP-aware deduplication to filter results that resolve to the same IP across different hostnames.
- Automatically honors `HTTP_PROXY` / `HTTPS_PROXY` environment variables when `-proxy` flag is not explicitly set.

WAS THIS USEFUL? 👍 👎

APPLICATION SECURITY

◆ Secrets Detection & Management

Truffle Security trufflehog ⓘ v3.95.9 NOTES ↗ CODE ↗

trufflehog discovers, classifies, and validates leaked credentials

TruffleHog v3.95.9 adds 7 new secret detectors and archived-repo exclusion for GitHub org scans.

└──▷ GET THIS VERSION

```
$ git clone --branch v3.95.9
https://github.com/trufflesecurity/trufflehog.git
# already have the repo? check out this version:
$ git checkout v3.95.9
```

└──▷ TRY IT

Scan a GitHub org while skipping archived repos to reduce noise and scan time in large orgs.

```
$ trufflehog github --org=<your-org> --results=verified --exclude-
archived
```

- New OpenRouter detector identifies `sk-or-v1-` API keys and validates them against the OpenRouter API.
- New New Relic Insights Insert Key detector matches `NRII-` prefixed keys with live verification via the Events API.
- New Duffel Token detector for the Duffel travel API.
- New Shippo detector for Shippo shipping API keys.
- New IPinfo detector, now included in the default detector set.

+3 more

WAS THIS USEFUL? 👍 👎

CLOUD & CONTAINER SECURITY

◆ CNAPP

Rapid7 InsightCloudSec ⓘ changelog · Jul 9, 2026 BLOG ↗

Rapid7 InsightCloudSec is a cloud-native security platform that continuously monitors, detects, and automatically remediates misconfigurations and compliance risks across multi-cloud environments.

InsightCloudSec 26.7.7 adds new insights for Auto Scaling Groups, EBS Volumes, and Security Groups, plus CIS Red Hat OpenShift Benchmark v1.9.0.

- Adds new Insights covering Auto Scaling Groups, EBS Volumes, and Security Groups for expanded cloud misconfiguration detection.
- Supports CIS Red Hat OpenShift Container Platform Benchmark v1.9.0 for container platform compliance assessments.

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ Detection Engineering

SigmaHQ Sigma Rules ⓘ r2026-07-01 NOTES ↗

Main Sigma Rule Repository

20 new Sigma detection rules added, including TanStack supply-chain attack coverage, CVE-2026-41089, and NTLM hash leak via Curl.

└──▷ GET THIS VERSION

```
$ git clone --branch r2026-07-01 https://github.com/SigmaHQ/sigma.git
# already have the repo? check out this version:
$ git checkout r2026-07-01
```

- New rule: Detects APT malware signatures via antivirus telemetry.
- New rule: Detects remote access tool signatures via antivirus telemetry.
- New rule: Detects AppLocker 'application would have been blocked' audit events.
- New rule: Detects Authencesn crypto module load via Modprobe as a copy-fail indicator.
- New rule: Detects file uploads to file-sharing websites via Curl.

+19 more

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Identity & Access Management

SPIFFE spire ⓘ v1.15.2 NOTES ↗

The SPIFFE Runtime Environment

SPIRE v1.15.2 adds SPIFFE Broker, PQC curve support, per-caller rate limiting, and TLS-secured Prometheus metrics.

└──▷ GET THIS VERSION

```
$ git clone --branch v1.15.2 https://github.com/spiffe/spire.git
# already have the repo? check out this version:
$ git checkout v1.15.2
```

- Adds configurable JTI claim inclusion in JWT-SVIDs at the entry level.
- Introduces experimental per-caller rate limiting for the agent Workload API and Envoy SDS.
- Adds TLS support for the Prometheus metrics endpoint using a SPIRE SVID, with an optional SPIFFE ID allowlist.
- Adds optional verification of client certificate IPs in the `x509pop` node attestor.
- Introduces the SPIFFE Broker endpoint and API.

+10 more

WAS THIS USEFUL? 👍 👎

BUILD

◆ AI Coding Agents

Claude Code ⓘ v2.1.206 NOTES ↗ CODE ↗

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 v2.1.206 adds smarter `/cd` suggestions, `/doctor` CLAUDE.md trimming, broader push-remote support, and faster background agent upgrades.

└──▷ GET THIS VERSION

```
$ git clone --branch v2.1.206 https://github.com/anthropics/claude-code.git
# already have the repo? check out this version:
$ git checkout v2.1.206
```

└──▷ TRY IT

Identify and trim bloated CLAUDE.md files before committing them — useful when onboarding a repo where the memory file has grown to repeat what the codebase already shows.

```
$ /doctor
```

Push and open a PR from a repo whose push remote is set to something other than `origin` (e.g. a fork workflow with `remote.pushDefault=upstream`) without manually allowing the remote first.

```
$ /commit-push-pr
```

- Adds directory path tab-completion to `/cd`, matching the existing `/add-dir` behavior.
- New `/doctor` check analyzes checked-in `CLAUDE.md` files and proposes trimming content Claude can already derive from the codebase.
- Extends `/commit-push-pr` to auto-allow `git push` to the repo's configured `remote.pushDefault` (or the sole remote when only one exists), not just `origin`.
- Enables `/login` to authenticate against Anthropic-operated public gateway endpoints.
- `EnterWorktree` now prompts for confirmation before entering a git worktree that lives outside the project's `.claude/worktrees/` directory.

+3 more

WAS THIS USEFUL? 👍 👎

OpenAI Codex CLI ⓘ rust-v0.144.0 NOTES ↗ CODE ↗

Lightweight coding agent that runs in your terminal

Codex CLI v0.144.0 adds a writes approval mode, default MCP auth elicitation, Ultra concurrency warnings, and richer usage-limit credit details.

└──▷ GET THIS VERSION

```
$ git clone --branch rust-v0.144.0
https://github.com/openai/codex.git
# already have the repo? check out this version:
$ git checkout rust-v0.144.0
```

└──▷ TRY IT

Run Codex in writes-approval mode to let it read files freely while pausing for confirmation only before any write action — useful for exploratory refactoring sessions where you want speed on reads but control on writes.

```
$ codex --approval-mode writes
```

- Adds `writes` app-approval mode that permits declared read-only actions automatically while prompting only for write operations.
- Enables MCP tool interactive authentication by default — no experimental opt-in required.
- Adds runtime Codex authentication support for app-server hosts, with redirect to a hosted page on successful login.
- Usage-limit reset credits now display their type and expiration date and let users choose which credit to redeem.
- Warns when selecting Ultra reasoning model with high multi-agent concurrency that usage could increase rapidly.

WAS THIS USEFUL? 👍 👎

OpenHands

1.11.0 · 3 RELEASES · 2026-07-09 · NOTES ↗ · LATEST

STABLE

OpenHands: AI-Driven Development

OpenHands 1.11.0 adds Agent Profiles, a Budgets dashboard, expanded usage monitoring, and email provider visibility.

└──▷ GET THIS VERSION

```
$ git clone --branch 1.11.0
https://github.com/OpenHands/OpenHands.git
# already have the repo? check out this version:
$ git checkout 1.11.0
```

└──▷ HOW TO FIND IT

Verify your email provider is active before relying on agent notifications — check the surfaced SMTP/Resend status in admin settings.

> 📍 In the console, go to Settings › Email and confirm the SMTP or Resend provider status is shown as enabled.

Monitor team spend against budget limits to catch runaway agent usage before it exceeds allocation.

> 📍 In the console, go to Dashboards › Budgets to view configured budget thresholds and current consumption, or go to Dashboards › Usage for expanded utilization metrics.

Apply a reusable agent configuration across enterprise projects to enforce consistent model and tool settings.

> 📍 In the console (enterprise/SaaS), go to Settings › Agent Profiles, create or select a profile, and assign it to one or more projects.

- Adds Agent Profiles on the cloud/SaaS backend, enabling enterprise teams to define and manage reusable agent configurations.
- Introduces a Budgets dashboard and expands the Usage Dashboard with new spend and consumption metrics.
- New budgets and usage monitoring UI surfaces cost and utilization data directly in the product.
- Surfaces email provider status (SMTP/Resend enabled) in the UI so admins can verify

notification configuration at a glance.

- Passes repository metadata to observability traces, enriching telemetry with source context for agent runs.

▾ **2 more releases in this issue** · 2026-07-09

cloud-1.45.0 NOTES ↗ STABLE

OpenHands 1.45 adds Agent Profiles, a Budgets dashboard, expanded Usage dashboard, and email delivery status surfacing.

└──▷ **GET THIS VERSION**

```
$ git clone --branch cloud-1.45.0
https://github.com/OpenHands/OpenHands.git
# already have the repo? check out this version:
$ git checkout cloud-1.45.0
```

- New Agent Profiles support on the cloud/SaaS backend lets enterprises define and manage reusable agent configurations.
- New Budgets dashboard enables teams to set and monitor spending limits across agent usage.
- Expanded Usage Dashboard provides broader visibility into agent activity and resource consumption.
- Surfaces email-enabled status for SMTP/Resend configurations so admins can confirm delivery is active.

cloud-1.44.0 NOTES ↗ STABLE

OpenHands 1.44.0 adds repository metadata to observability traces for richer pipeline monitoring.

└──▷ **GET THIS VERSION**

```
$ git clone --branch cloud-1.44.0
https://github.com/OpenHands/OpenHands.git
# already have the repo? check out this version:
$ git checkout cloud-1.44.0
```

- Includes repository metadata (e.g., repo name, branch, commit) in observability traces, enabling richer filtering and attribution in tracing backends.

WAS THIS USEFUL? 👍 👎

OpenCode ⓘ v1.17.18 2 RELEASES · 2026-07-09 NOTES ↗ CODE ↗

LATEST STABLE

The open source coding agent.

Adds a model-specific system prompt for Meta Muse Spark to improve coding agent responses.

└──▷ GET THIS VERSION

```
$ git clone --branch v1.17.18
https://github.com/anomalyco/opencode.git
# already have the repo? check out this version:
$ git checkout v1.17.18
```

› Adds a tailored system prompt for the Meta Muse Spark model, enabling more accurate and model-optimized responses when using that provider.

▾ 1 more release in this issue · 2026-07-09

v1.17.17 NOTES ↗ CODE ↗ STABLE

OpenCode v1.17.17 adds a v2 free-model selector, dismissible tabs intro popup, and refreshed sub-agent task and revert-dock UI.

└──▷ GET THIS VERSION

```
$ git clone --branch v1.17.17
https://github.com/anomalyco/opencode.git
# already have the repo? check out this version:
$ git checkout v1.17.17
```

› Adds a v2 free-model selector with faster access to more providers in the desktop app.

› Introduces a dismissible tabs intro popup and a refreshed help entry point in the desktop UI.

› Updates sub-agent task rows to match the v2 session design, with distinct icon states for running, completed, and resting tasks.

› Restyled revert dock in v2 sessions for clearer restore actions, using v2 design tokens and a new outline-reset icon.

WAS THIS USEFUL? 👍 👎

Crush ⓘ v0.84.0 NOTES ↗ CODE ↗

Glamourous agentic coding for all

Crush v0.84.0 adds session-affinity headers for provider-side prompt caching.

└──▷ **GET THIS VERSION**

```
$ git clone --branch v0.84.0
https://github.com/charmbracelet/crush.git
# already have the repo? check out this version:
$ git checkout v0.84.0
```

› Sends `x-session-affinity` and `x-session-id` headers with every request, enabling supporting providers to pin sessions to a replica and maximize prompt cache hits.

WAS THIS USEFUL? 👍 👎

Windsurf ⓘ snapshot-20260710 NOTES ↗

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

Devin Desktop snapshot-20260710 adds sandbox exclusion controls, reviewable diffs, ACU usage visibility, and a plugin system for extending Devin Local.

└──▷ USE IT

Exclude a specific high-risk command from the sandbox so it runs in your real environment — useful when a tool must access hardware or network resources that the sandbox proxy blocks.

yaml

```yaml
# In team or user settings config:
sandbox:
  excluded:
    - command: "nmap"
      policy: ask
```

Check your current ACU consumption mid-session without leaving the chat interface.

```
$ /usage
```

Suppress Devin attribution in commit messages for repositories where automated-author footers violate commit policy.

yaml

```yaml
# In the Devin Local config file:
attribution: false
```

- Adds New session in space option to the session kebab menu for quicker task-scoped session creation.
- Enables auto-reconnect for Devin Cloud sessions when network connectivity is restored.
- Supports copying images from chat via the context menu.
- New users now default to agent mode out of the box.
- Edits produced in autonomous mode now generate reviewable diffs for human review.

+21 more

WAS THIS USEFUL? 👍 👎

Kiro ⓘ Hooks on Agent Writes, Lazy MCP Auth, and Multi-Window Sync

2 RELEASES · SEEN 2026-07-10 NOTES ↗ LATEST STABLE

Kiro is an AI-powered IDE by AWS that uses "specs" to help developers plan, design, and build software features with agentic assistance.

Kiro adds hooks on agent file writes, lazy MCP OAuth, and multi-window settings sync in v1.0.116.

- New hooks trigger on agent-driven file writes, enabling automation to react to AI-generated file changes.
- Lazy MCP authentication automatically handles OAuth sign-in for MCP servers that require it, removing manual auth steps.
- Multi-window settings sync keeps configuration consistent across multiple open Kiro windows.

▾ **1 more release in this issue** · seen 2026-07-10

Expanded MCP OAuth Support NOTES ↗ STABLE

Kiro MCP OAuth now supports pre-registered apps with client secrets, custom redirect URIs, and DCR bypass.

└──▷ USE IT

Connect Kiro to a remote MCP server like Figma that requires a pre-registered OAuth app with a client secret and a specific callback URL.

json

```
{
  "mcpServers": {
    "figma": {
      "url": "https://mcp.figma.com/sse",
      "oauth": {
        "clientId": "<your-client-id>",
        "clientSecret": "<your-client-secret>",
        "redirectUri": "http://localhost:7778/oauth/callback"
      }
    }
  }
}
```

- Supports `clientSecret` in MCP OAuth config for servers that require a client secret (e.g., Figma).

- Enables skipping Dynamic Client Registration when a custom `clientId` is provided, authenticating as your own pre-registered app.
- Accepts full URLs with custom paths in the `redirectUri` field (e.g., `http://localhost:7778/oauth/callback`) to match exact registered callback URLs.
- Adds full ASCII mode coverage for terminals without Unicode support.

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · July 10, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe