THE CYBER TOOLCHAIN

NO. 003

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED JULY 3, 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 8 tools

CLOUD & CONTAINER SECURITY

◆ Runtime Security

Falco 0.44.1

Cloud Native Runtime Security

Falco 0.44.1 adds support for disabling BPF iterators in userspace.

└──▷ GET THIS VERSION

```
$ git clone --branch 0.44.1
https://github.com/falcosecurity/falco.git
# already have the repo? check out this version:
$ git checkout 0.44.1
```

› Adds configuration support for disabling BPF iterators, giving operators control over BPF iterator usage in environments where they cause issues.

WAS THIS USEFUL? 👍 👎

◆ Container & Image Security

Anchore Grype

v0.115.0 · 3 RELEASES · 2026-06-03 → 2026-06-26 · LATEST · STABLE

A vulnerability scanner for container images and filesystems

Grype v0.115.0 adds golang.org/x/net vuln detection from govulndb and deduplicates Go/GHSA matches.

└──▷ GET THIS VERSION

```
$ git clone --branch v0.115.0 https://github.com/anchore/grype.git
# already have the repo? check out this version:
$ git checkout v0.115.0
```

└──▷ TRY IT

Scan a Go project image to surface golang.org/x/net CVEs now sourced directly from govulndb, with deduplication against GHSA entries.

```
$ grype <your-go-image>:latest
```

- Adds detection of golang.org/x/net vulnerabilities sourced from govulndb, expanding Go ecosystem coverage.
- Merges duplicate Go vuln matches with their corresponding GHSA matches to reduce noise in scan results.

▾ 2 more releases in this issue · 2026-06-03 → 2026-06-26

v0.114.0 · STABLE

Grype v0.114.0 adds Zarf package scanning and a Go Vuln DB OSV transformer for richer Go vulnerability data.

└──▷ GET THIS VERSION

```
$ git clone --branch v0.114.0 https://github.com/anchore/grype.git
# already have the repo? check out this version:
$ git checkout v0.114.0
```

└──▷ TRY IT

Scan a Zarf package archive for vulnerabilities across all bundled SBOMs in a single pass, with findings traceable to each source image.

```
$ grype zarf:path/to/package.tar.zst -o json
```

- Adds `zarf:` scan target to scan all SBOMs within a Zarf package archive (.tar.zst), with per-finding provenance traced back to the originating image via package annotations.
- Adds a Go Vuln DB OSV transformer to ingest and process govulndb records in OSV format, enabling broader Go vulnerability coverage.
- Respects withdrawn status of Go Vuln DB OSV records, suppressing false-positive findings from retracted advisories.

v0.113.0 STABLE

Grype v0.113.0 adds Ubuntu 26.04 "resolute" support and source RPM filtering for Hummingbird/CSAF VEX matching.

└──▷ **GET THIS VERSION**

```
$ git clone --branch v0.113.0 https://github.com/anchore/grype.git
# already have the repo? check out this version:
$ git checkout v0.113.0
```

- Adds Ubuntu 26.04 "resolute" as a recognized distro codename for vulnerability matching.
- Adds source RPM filtering for Hummingbird (CSAF VEX) matching, reducing false positives by distinguishing binary RPMs from source RPMs using an architecture qualifier.

WAS THIS USEFUL? 👍 👎

BUILD

◆ AI Coding Agents

Claude Code v2.1.199

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.

Stacked slash-skills (up to 5), auto-retry on 429s, and a raised retry ceiling via `CLAUDE_CODE_MAX_RETRIES`

└──▷ GET THIS VERSION

```
$ git clone --branch v2.1.199 https://github.com/anthropics/claude-code.git
# already have the repo? check out this version:
$ git checkout v2.1.199
```

└──▷ TRY IT

Apply multiple skills together in one prompt to layer context (e.g. a security-review skill and a repo-conventions skill) before asking Claude to act.

```
$ /skill-security-review /skill-repo-conventions find all places we call eval() and suggest safer alternatives
```

On long-running agentic jobs in flaky network environments, raise the retry ceiling so transient 429s don't abort the session.

```
$ CLAUDE_CODE_MAX_RETRIES=200 claude 'run the full test suite and summarise failures'
```

- Supports stacking up to 5 slash-skill invocations in a single prompt (e.g. `/skill-a /skill-b /skill-c do XYZ`), loading all leading skills instead of just the first.
- Auto-retries transient server rate-limit errors (HTTP 429s unrelated to usage limits) with backoff for subscribers, instead of failing the turn.
- New `CLAUDE_CODE_RETRY_WATCHDOG` behavior raises the default retry count for non-capacity transient errors to 300 and removes the previous hard cap of 15 on `CLAUDE_CODE_MAX_RETRIES`.
- Idle surplus subagents in the agent panel now collapse into an expandable summary row instead of vanishing.

WAS THIS USEFUL? 👍 👎

OpenAI Codex CLI `rust-v0.143.0-alpha.35` PRE-RELEASE

Lightweight coding agent that runs in your terminal

Adds configurable multi-agent mode hint text so deployment-specific delegation policies stay stable across reasoning-effort changes.

└──▷ GET THIS VERSION

```
$ git clone --branch rust-v0.143.0-alpha.35
https://github.com/openai/codex.git
# already have the repo? check out this version:
$ git checkout rust-v0.143.0-alpha.35
```

└──▷ USE IT

Lock a deployment to a specific multi-agent delegation policy so it doesn't flip between explicit-only and proactive when reasoning effort is adjusted.

yaml

```yaml
# In your Codex config file
features:
  multi_agent_v2:
    multi_agent_mode_hint_text: "Always delegate sub-tasks
proactively to sub-agents."
```

› New `features.multi_agent_v2.multi_agent_mode_hint_text` config setting lets operators supply a fixed delegation policy string that overrides the built-in explicit-only/proactive multi-agent behaviors regardless of reasoning effort.

WAS THIS USEFUL? 👍 👎

Goose v1.41.0

an open source, extensible AI agent that goes beyond code suggestions - install, execute, edit, and test with any LLM

Goose v1.41.0 adds TLS for ACP, 15+ new providers, hooks, summon sub-agents, and a wave of new CLI commands.

└──▷ GET THIS VERSION

```
$ git clone --branch v1.41.0 https://github.com/aaif-goose/goose.git
# already have the repo? check out this version:
$ git checkout v1.41.0
```

└──▷ TRY IT

Serve Goose's ACP endpoint over TLS so remote clients can connect securely.

```
$ goose serve --tls --tls-cert-path /etc/goose/server.crt --tls-key-path /etc/goose/server.key --port 3284
```

Edit a previous session's conversation context before forking it, useful for re-running with corrected instructions.

```
$ goose session --edit --resume <session-id>
```

Cap tool response payload size to prevent context bloat when tools return large outputs (e.g., grep over a huge codebase).

```
$ GOOSE_MAX_TOOL_RESPONSE_SIZE=16384 goose run --recipe my-recipe.yaml
```

- Adds `--edit` session flag to edit a conversation before forking it into a new session.
- New `tui` subcommand on goose-cli to launch the terminal UI directly.
- Supports TLS for `goose serve` via `--tls`, `--tls-cert-path`, and `--tls-key-path` flags.
- Adds iFlytek Spark, Astron MaaS, Fireworks AI, Together AI, OrcaRouter, EmpirioLabs AI, Perplexity, Alibaba (Qwen/DashScope), Scaleway, NEAR AI Cloud, Vercel AI

Gateway, Databricks AI Gateway, Routstr, FuturMix, oMLX, Atomic Chat, and xAI SuperGrok OAuth as new providers.

› Adds OpenRouter request parameters support for fine-grained API payload control.

+22 more

WAS THIS USEFUL? 👍 👎

Windsurf snapshot-20260703

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/Devin Desktop snapshot adds Devin plugin system, subagent MCP tool calling, terminal CLI agent, and new Agent Command Center views.

└──▷ USE IT

Suppress 'Generated by Devin' attribution in commit messages when using Devin Local for internal repositories.

```yaml
# In your Devin Local config file, add:
attribution: false
```

› Enables subagents to call MCP tools directly without routing through the parent agent.

› Adds list display option for the agent inbox alongside improved session sidebar sorting and filtering.

› Introduces Adaptive model router that dynamically selects the best underlying model per task at a fixed per-token quota draw rate.

› Model picker now displays token pricing information inline for cost-aware model selection.

› Subagents can now be configured with a default model per agent.

+3 more

WAS THIS USEFUL? 👍 👎

Kiro

Session Restore, Performance Optimizations, and Custom Agent Enhancements

3 RELEASES · seen 2026-07-03 LATEST STABLE

Kiro is an AI-powered IDE built on VS Code that uses "specs" to translate requirements into structured plans, tasks, and code automatically.

Kiro 1.0.89 adds automatic session restore on launch, lower idle resource use, and prepaid credit packs in the account dashboard.

- Reduces idle resource consumption, enabling use on lower-powered machines.
- Surfaces prepaid credit packs directly in the account dashboard.

▾ **2 more releases in this issue** · seen 2026-07-03

Custom Overage Caps via Service Quotas

STABLE

Enterprise admins can now set per-profile overage spending caps for Kiro via AWS Service Quotas.



└──▷ **HOW TO FIND IT**

Cap overage spend per profile to prevent runaway costs for enterprise users.

> 📍 In the Kiro console, go to Settings › Overages and click Manage to open the AWS Service Quotas console, then set the 'Maximum allowed overage per Kiro profile' quota to your desired limit.

- Adds AWS Service Quotas integration enabling enterprise admins to set a 'Maximum allowed overage per Kiro profile' cap, limiting unexpected costs across all users in a profile.

Stay Connected to MCP Servers

STABLE

Kiro adds MCP OAuth commands (`/mcp` auth, cancel-auth, logout) and keyboard shortcuts for managing remote server credentials.

└──▷ **TRY IT**

When a remote MCP server token expires mid-session, re-authenticate without restarting Kiro.

```
$ /mcp auth
```

When an OAuth browser confirmation flow hangs indefinitely, abort it cleanly so you can retry.

```
$ /mcp cancel-auth
```

When you need to rotate or revoke credentials for a remote MCP server, clear them entirely.

```
$ /mcp logout
```

- Adds `/mcp auth` command to force re-authentication when an OAuth token has expired or become invalid on a remote MCP server.
- Adds `/mcp cancel-auth` command to abort a pending OAuth flow stuck waiting for browser confirmation.
- Adds `/mcp logout` command to remove stored OAuth credentials entirely from a remote MCP server.
- Adds keyboard shortcuts in the MCP panel status view: `^A` to force auth, `^X` to abort, and `^R` to remove credentials.
- Updates `/usage` display to reflect the new prepaid credits model.

WAS THIS USEFUL? 👍 👎

PLATFORMS & UTILITIES

◆ General Utilities & Libraries

goshs v2.1.4

Feature-rich single-binary file server for red teamers and developers. HTTP/S · WebDAV · FTP/SFTP · SMB · LDAP/S · NTLM hash capture · DNS/SMTP callbacks · TLS · Auth · Share links.

goshs v2.1.4 adds TUI clipboard copy for reverse-shell payloads via y/c, with OSC 52 SSH support.

└──▷ GET THIS VERSION

```
$ git clone --branch v2.1.4 https://github.com/goshs-labs/goshs.git
# already have the repo? check out this version:
$ git checkout v2.1.4
```

└──▷ TRY IT

Generate a reverse-shell payload over an SSH session and copy it to your local clipboard via OSC 52 — no local clipboard tool required on the remote host.

```
$ goshs --tui
```

- Adds one-key clipboard copy (`y` / `c`) in the `--tui` reverse-shell generator, pushing payloads to xclip/xsel, wl-copy, pbcopy, clip, or over SSH via OSC 52 (filling both system clipboard and X11 primary selection).
- Restructures the `--tui` generator tab into a stacked layout so multi-line payload output can be mouse-selected without also grabbing menu entries.

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · July 3, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe