THE CYBER TOOLCHAIN

NO. 038

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED AUGUST 7, 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 12 tools

OFFENSIVE SECURITY

◆ AI-Powered Offensive Security

Strix

1 RELEASE · 2026-08-07 NOTES ↗

Open-source AI penetration testing tool to find and fix your app's vulnerabilities.

> Strix v1.5.0 lets agents scan OpenAPI/Swagger specs and Postman collections directly as targets, rewrites the interactive terminal UI in Go/Bubble Tea, and enriches SCA findings with dependency-chain and reachability evidence, alongside new LLM configuration environment variables and performance/security hardening.

└──▷ WHAT SHIPPED · 11 FEATURES most completely described first ? what's the number?

01 **LLM_EXTRA_HEADERS for custom request headers** NEW 90

Adds `LLM_EXTRA_HEADERS` environment variable to inject custom request headers into any OpenAI-compatible endpoint, enabling use with proxies, gateways, or auth-requiring local models.

Route Strix through an internal LLM gateway that requires a custom auth header, without modifying your API key setup.

```
$ export LLM_EXTRA_HEADERS='{"X-Gateway-Token": "my-gateway-secret"}'
export STRIX_LLM="openai/gpt-4o"
export LLM_API_KEY="your-api-key"
strix --target https://your-app.com
```

— Named env var with runnable example command v1.5.0

02 **API spec and Postman collection targets** NEW 85

Supports API specs (OpenAPI/Swagger) and Postman collections as scan targets, letting agents test every declared endpoint without crawling.

Scan every endpoint declared in an OpenAPI spec against a live staging server, skipping crawl-based discovery.

```
$ strix --target ./openapi.yaml
```

— Command example and named formats fully ground it v1.5.0

03 **STRIX_REASONING_EFFORT config option** NEW 75

Adds `STRIX_REASONING_EFFORT=max` config option for providers that expose a reasoning-effort control, letting agents push maximum reasoning effort on complex targets.

Push the LLM to use maximum reasoning effort on a complex target when using a provider that supports the setting.

```
$ export STRIX_REASONING_EFFORT=max
strix --target https://your-app.com
```

— Exact env var and value with runnable example v1.5.0

---

04 **SCA dependency chain and reachability evidence** IMPROVED 60

SCA findings now record the full transitive dependency chain, showing how a vulnerable package is pulled in, and include a structured reachability evidence ladder for dependency vulnerabilities, grading confidence from theoretical to exploitable.

— Explains mechanism but no way to act on it directly v1.5.0

---

05 **Required manifest_path field on CVE findings** BREAKING 60

Dependency CVE findings now require a repo-relative `manifest_path` field, giving precise location context in reports.

— Names exact required field, no migration steps given v1.5.0

---

06 **Installable SKILL.md and AGENTS.md support** NEW 60

Adds installable `SKILL.md` skills and `AGENTS.md` support for extending agent capabilities.

— Names the files but no example of authoring one v1.5.0

THINNER COVERAGE BELOW

---

07 **LLM_DISABLE_STREAMING opt-in flag** NEW 55

Adds `LLM_DISABLE_STREAMING` environment variable as an opt-in flag to disable streaming for OpenAI-compatible endpoints that don't support it.

— Named env var but no usage example given v1.5.0

---

08 **Go/Bubble Tea terminal UI** IMPROVED 45

Replaces the Python/Textual TUI with a Go/Bubble Tea interface for the interactive terminal UI.

— Names old and new stack but no usage detail v1.5.0

09 **Faster CLI startup via lazy imports** IMPROVED 40

Delivers ~10x faster CLI startup via lazy imports.

— Gives concrete speedup figure but no further detail v1.5.0

10 **Local target mounting into sandbox** IMPROVED 35

Mounts local targets into the sandbox instead of copying them, reducing startup overhead for local directory scans.

— Describes change but no configurable surface named v1.5.0

11 **Owner-only credential file permissions** IMPROVED 35

Credential files are now created with owner-only permissions, hardening local secret storage.

— States the hardening but no file path or command v1.5.0

WAS THIS USEFUL? 👍 👎

APPLICATION SECURITY

◆ SAST / SCA / Code Security

Veracode ⓘ 1 RELEASE · 2026-08-06 BLOG ↗

Veracode is a cloud-based application security platform that performs static, dynamic, and software composition analysis to identify vulnerabilities.

> Veracode significantly expanded DAST this window: DAST Enterprise mode gained AI-assisted login and richer authentication/scripting support, a DAST Target Configuration Service REST API went public, EASM now feeds discovered targets into DAST, and scheduling became more flexible — alongside smaller scan-scope, detection, and auth improvements. The DAST scheduling REST API endpoints also changed, requiring integration updates.

└──▷ **WHAT SHIPPED · 20 FEATURES** most completely described first ? what's the number?

01 **DAST Enterprise auth and scripting support** NEW 65

DAST Enterprise mode adds support for login scripts, scanner variables, client certificates for web applications, and Scriptable Request Modifications (SRM) for APIs.

— Names several concrete mechanisms (SRM, scanner variables) without setup steps.

DAST updates (2026-08-06)

02 **DAST Target Configuration Service REST API public** NEW 60

The DAST Target Configuration Service REST API is now publicly available to automate management of DAST targets and trigger analyses.

— Names the API surface but omits endpoint paths. DAST updates (2026-08-06)

03 **Enhanced DAST scheduling with pause/resume** IMPROVED 60

Enhances the DAST Schedule feature with advanced scheduling capabilities and greater configuration flexibility, including the ability to schedule an analysis to pause and resume on specific days of the week, during specific periods, or both; all existing schedules are automatically migrated to the new system.

— Describes mechanism and migration behavior but no exact config key.

DAST updates (2026-08-06)

04 **ISM proxy exclusion list (endpoint 24.10.0)** NEW 60

ISM endpoint 24.10.0 introduces a proxy exclusion list for hosts that should bypass configured proxy settings.

— Names exact ISM endpoint version and feature purpose. DAST updates (2026-08-06)

05 **DAST Enterprise API spec upload and firewall scanning via ISM** NEW 60

DAST Enterprise mode adds support for uploading or dynamically referencing API specifications and enables Internal Scanning Management (ISM) for scanning behind a corporate firewall.

— Names ISM and API spec handling without setup steps. DAST updates (2026-08-06)

THINNER COVERAGE BELOW

06 **TOTP seed support for MFA-protected scans** NEW 55

Web application and API scans now support time-based one-time password (TOTP) seeds for MFA-protected URLs, configurable via the REST API.

— Names TOTP mechanism and REST API configuration path. DAST updates (2026-08-06)

07 **Org-level URL scan settings via Dynamic Analysis API** IMPROVED 55

Dynamic Analysis REST API now supports setting URL scan settings at the organization level for all analyses and scans.

— Names the API and scope but no endpoint path. DAST updates (2026-08-06)

08 **EASM auto-creates DAST targets** NEW 50

EASM now automatically creates discovered targets in DAST, which can be mapped or converted to regular DAST targets for scanning.

— Explains flow but not the exact UI path or config. DAST updates (2026-08-06)

09 **DAST scheduling REST API endpoints changed** BREAKING 50

The DAST scheduling REST API endpoints have changed; integrations that use the REST API to manage schedules must be updated to use the new endpoints, per the DAST API specification.

— Flags migration need but doesn't list the new endpoint paths. DAST updates (2026-08-06)

10 **Business unit targeting for DAST targets** NEW 50

Enables selection of a business unit when creating a web application or API specification target, or on the DAST configuration page.

— Names the UI location but no config key or API. DAST updates (2026-08-06)

11 **Postman Collection scanning for APIs** NEW 50

API scanning now supports uploading and scanning Postman Collections.

— Names the supported format and where it's used. DAST updates (2026-08-06)

12 **AI-assisted login for DAST Enterprise mode** NEW 45

DAST Enterprise mode now provides AI-assisted login, an AI-based authentication method that handles complex login flows without requiring recorded login scripts.

— Names the capability and mechanism but no config path given. DAST updates (2026-08-06)

13 **Manual application linking to Veracode Platform** NEW 45

DAST now supports manual application linking to the Veracode Platform for policy evaluation and combined multi-scan-type reporting.

— States purpose but not the mechanism for linking. DAST updates (2026-08-06)

14 **Custom host-to-IP mapping for DAST scans** NEW 45

Adds custom host-to-IP address mapping configuration for DAST scans when DNS lookup is unavailable or not desired.

— Names the feature and use case, no exact config location. DAST updates (2026-08-06)

15 **Directory Restrictions for DAST scan scope** NEW 45

Adds Directory Restrictions to target configuration to control DAST scan scope.

— Names the setting and its location in target configuration. DAST updates (2026-08-06)

16 **CAA record checks on SSL certificates (CWE-862)** IMPROVED 45

Adds improved detection for CAA record checks on SSL certificates for CWE-862 in both Dynamic Analysis and DAST.

— Names the CWE and scan types but no further mechanism. DAST updates (2026-08-06)

17 **Downloadable DAST Enterprise scan reports** NEW 40

DAST Enterprise mode now supports downloadable scan reports providing visibility into scan coverage and scanner behavior.

— Describes purpose but no format or download location. DAST updates (2026-08-06)

18 **Custom cookies for scan authentication** NEW 40

Web application and API scans now support one or more custom cookies for authentication.

— States the feature without configuration detail. DAST updates (2026-08-06)

19 **Open-port scanning for web applications** NEW 35

Dynamic Analysis and DAST Enterprise Mode now support scanning web applications for open ports.

— States the capability with no configuration detail. DAST updates (2026-08-06)

20 **New HTTP header, TLS, and fingerprinting detections** NEW

35

Adds new detections for HTTP headers, TLS, and fingerprinting to the scan engine.

— Lists detection categories with no specifics on rules. DAST updates (2026-08-06)

└──▷ **BREAKING ON UPGRADE**

! The DAST scheduling REST API endpoints have changed; integrations that use the REST API to manage schedules must be updated to use the new endpoints (refer to the DAST API specification for details).

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ SIEM

Sumo Logic ⓘ 1 RELEASE · 2026-08-06 BLOG ↗

Sumo Logic is a cloud-based monitoring and analytics platform for logs, metrics, and security data.

> Sumo Logic introduced a new operator for querying threat intelligence indicators directly against log data, and changed indicator matching to default to active indicators only.

└──▷ **WHAT SHIPPED · 2 FEATURES** most completely described first ? what's the number?

01 **threatlookup operator for threat intel search** NEW 50

A new `threatlookup` operator enables searching threat intelligence indicators against log data directly within Sumo Logic queries.

— Names the operator but gives no syntax example Threat Intelligence (Security) (2026-08-…

02 **Active-indicators-only default for threat matching** IMPROVED 30

Threat intelligence indicator search and Cloud SIEM entity enrichment now default to matching only active indicators, rather than all indicators.

— States behavior change but no config to override it

Threat Intelligence (Security) (2026-08-…

WAS THIS USEFUL? 👍 👎

EXPOSURE & VULNERABILITY MANAGEMENT

◆ Vulnerability Management

OSV-Scanner

1 RELEASE · 2026-08-07 NOTES ↗

Vulnerability scanner written in Go which uses the data provided by https://osv.dev

> OSV-Scanner v2.5.0 completes its migration to the osv-scalibr scanning pipeline and unlocks experimental plugins, while adding VSIX and Ubuntu chiseled-package scanning plus broader ecosystem and Go version support.

└──▷ WHAT SHIPPED · 6 FEATURES most completely described first ? what's the number?

01 osv-scalibr pipeline migration and experimental plugins IMPROVED

85

Completes the migration of scanning, filtering, and matching to the full `osv-scalibr` end-to-end pipeline, which enables most `osv-scalibr` plugins via the new `--experimental-plugins` flag.

Use an osv-scalibr plugin that wasn't previously accessible in osv-scanner — e.g. to scan a VS Code extension package in a directory.

```
$ osv-scanner scan source --experimental-plugins -r
/path/to/your/dir
```

— Names flag and exact command; mechanism partly explained. v2.5.0

02 ScanGoModVersion config key for go.mod version scanning NEW

75

The `ScanGoModVersion` config key enables scanning of the Go version declared in `go.mod` files; it is disabled by default because the `go` directive specifies a minimum required language version rather than the actual toolchain in use.

Enable Go version scanning when you want OSV-Scanner to flag vulnerabilities tied to the Go version declared in go.mod.

```yaml
ScanGoModVersion: true
```

— Names config key with example value and rationale for default. product docs

THINNER COVERAGE BELOW

03 PURL type resolution in osvscannerjson extractor IMPROVED

55

Updates the `osvscannerjson` extractor with PURL type resolution, mapping ecosystem names to valid PURL types (golang, gem, cargo, npm, etc.).

— Names extractor and PURL types but no usage example. `v2.5.0`

04 **Expanded ecosystem and PURL mapping** IMPROVED 50

Extends ecosystem mapping in `osv-scalibr` to cover SUSE, Azure Linux / Mariner, Alpaquita, Mageia, openSUSE Leap, and Debian/Ubuntu PURL.

— Lists specific ecosystems added but no actionable step. `v2.5.0`

05 **Ubuntu chiseled package scanning** NEW 45

OSV-Scanner adds support for scanning Ubuntu chiseled packages by reading `/var/lib/chisel/manifest.wall`.

— Names exact file path but no usage example or command. `product docs`

06 **VSIX package extractor** NEW 45

Adds a `javascript/vsix` extractor to support scanning VS Code extension (`.vsix`) packages.

— Names extractor and file type but lacks concrete usage steps. `v2.5.0`

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Identity & Access Management

Auth0 ⓘ 1 RELEASE · 2026-08-06 BLOG ↗

Auth0 is a cloud-based identity and access management platform providing authentication, authorization, and user management solutions for applications.

> Auth0 shipped general availability of Google Workspace Directory Sync for Groups, adding a dashboard UI for browsing groups and a self-service flow for selective sync.

└──▷ **WHAT SHIPPED · 1 FEATURE** most completely described first ? what's the number?

01 **Google Workspace Directory Sync for Groups GA** NEW 65

Google Workspace Group and Group Membership sync is now generally available, with a paginated, searchable, filterable table in the Auth0 Management Dashboard for browsing and selecting Google Workspace groups to sync. Enterprise IT admins can use the Self-Service assistant flow to choose all or a subset of groups for selective synchronization.

.
.
.
.

— Names dashboard and self-service flow but no API/config detail.

Google Workspace Directory Sync for Grou…

WAS THIS USEFUL? 👍 👎

BUILD

◆ AI Coding Agents

Kiro ⓘ 1 RELEASE · seen 2026-08-07 NOTES ↗

> Kiro's IDE release adds open Agent Plugin format support for sharing packaged Powers, plus session pinning, Kiro CLI hand-off, and update notifications in Agent Focus Mode.

└──▷ **WHAT SHIPPED · 8 FEATURES** most completely described first ? what's the number?

01 **Agent Plugin format support for Powers** NEW 65

Kiro supports installing Powers packaged in the open Agent Plugin format from a local folder or a GitHub URL, bundling skills, steering, scripts, and assets for sharing across compatible agent tools.

– Names install sources but not exact command or manifest fields.

Agent Plugin Support and Session Pinning

THINNER COVERAGE BELOW

02 **In-app update notifications** NEW 50

Adds an update row in the rail footer and a Check for Updates button in the settings pane that appear when a new Kiro version is available.

– Two named UI surfaces but only a notification, not a workflow.

Agent Plugin Support and Session Pinning

03 **Pin Session in Agent Focus Mode** NEW 45

Adds a Pin Session action in Agent Focus Mode to keep a session pinned at the top of its section.

– Clear UI action named but no further mechanism detail.

Agent Plugin Support and Session Pinning

04 **Open with Kiro CLI from a session** NEW 45

Adds an Open with Kiro CLI option to resume an existing session directly in the Kiro CLI.

– Names the action but not the resulting CLI command syntax.

Agent Plugin Support and Session Pinning

05 **Safer handling of untrusted workspace content** IMPROVED 35

Improves spec hovers and MCP installs to handle untrusted workspace content safely.

– Names affected surfaces but not the safety mechanism itself.

Agent Plugin Support and Session Pinning

06 **Editor base updated to Code OSS v1.109.5** IMPROVED 35

Updates the underlying editor to Code OSS v1.109.5.

— Exact version given but no actionable change described.

Agent Plugin Support and Session Pinning

07 **Spec documents and task rows open in editor** IMPROVED 30

Spec documents and task rows in the context panel now open directly in the editor.

— Brief statement with no further behavioural detail.

Agent Plugin Support and Session Pinning

08 **Bulk session migration and error recovery** IMPROVED 20

Adds bulk session migration and improved error recovery in Agent Focus Mode.

— No detail on migration scope or recovery mechanism.

Agent Plugin Support and Session Pinning

WAS THIS USEFUL? 👍 👎

OpenAI Codex CLI

2 RELEASES · 2026-08-07 NOTES ↗ CODE ↗

Lightweight coding agent that runs in your terminal

> OpenAI Codex CLI's latest releases add a `migrate-rollouts` subcommand for moving legacy sessions into paginated thread history, an `--approve-for-me` flag for unattended `codex exec` runs, portable Agent Plugins with remote catalog access, MCP 2026-07-28 protocol support, and Bedrock cached web search, while removing the deprecated `--full-auto` flag and redundant Linux bundle archives.

└──▷ WHAT SHIPPED · 16 FEATURES most completely described first ? what's the number?

01 migrate-rollouts subcommand for thread history migration NEW

95

`codex migrate-rollouts` inspects or migrates legacy local sessions into the new paginated thread history, with `--apply`, `--thread`, `--max-mib-per-second`, `--json`, and `--verbose` flags to control dry-run inspection, targeting a specific thread, throttling throughput, and output format.

Dry-run inspection of all local sessions eligible for migration before committing any changes.

```
$ codex migrate-rollouts --verbose --json
```

Migrate a specific thread to paginated history with a throughput cap to avoid saturating disk I/O.

```
$ codex migrate-rollouts --apply --thread <THREAD_ID> --max-mib-per-second 50
```

— Full flag list and two runnable example commands provided. rust-v0.148.0-alpha.1

02 --approve-for-me flag for codex exec NEW

80

`codex exec --approve-for-me` enables automatically reviewed approvals so tasks run without manual confirmation prompts.

Run a coding task in CI without manual approval prompts, letting the agent proceed automatically.

```
$ codex exec --approve-for-me 'add unit tests for the auth module'
```

— Exact flag and runnable example given, mechanism brief. `rust-v0.147.0`

03 **`--full-auto` flag removed from `codex exec`** BREAKING — 70

The deprecated `--full-auto` flag for `codex exec` has been removed; use `--sandbox workspace-write` instead.

— Exact flags named with migration path, no further mechanism. `rust-v0.147.0`

THINNER COVERAGE BELOW

04 **MCP 2026-07-28 protocol support** NEW — 55

Codex supports the opt-in MCP 2026-07-28 protocol, including paginated discovery, multi-round requests, and non-blocking server startup.

— Names protocol version and features, no flag or config shown. `rust-v0.147.0`

05 **Portable Agent Plugins with remote catalog access** IMPROVED — 55

Codex installs portable Agent Plugins and searches across local, personal, workspace, and remote plugin catalogs; it also supports fetching remote installed plugins across all scopes.

— Names catalog scopes but no command or config surface shown. `rust-v0.147.0` `rust-v0.148.0-alpha.1`

06 **Guardian circuit-breaker for cyber model turns** NEW — 55

Adds a Guardian circuit-breaker policy that interrupts cyber model turns after the first Guardian denial, while retaining existing denial thresholds for all other models.

— Explains mechanism and scope, no config surface named. `rust-v0.148.0-alpha.1`

07 **Redundant Linux bundle archives dropped** BREAKING — 50

Redundant Linux bundle archives are no longer published; use the standard `codex-package-<target>` release archives instead.

— Names replacement archive pattern but little else. `rust-v0.147.0`

08 **Bedrock cached web search and conversation compaction** NEW — 40

Enables cached web search and remote conversation compaction for Amazon Bedrock.

– Names Bedrock integration but no mechanism detail. `rust-v0.147.0`

09 **Import and sync Cursor and Claude conversations** NEW

40

Imports Cursor-managed skills and synchronizes changes to imported Claude and Cursor conversations without creating duplicates.

– Names source integrations but no command shown. `rust-v0.147.0`

10 **Minimal /dev mount in Bubblewrap sandboxes** IMPROVED

40

Mounts a minimal `/dev` in full-filesystem Bubblewrap sandboxes.

– Names sandbox mechanism, lacks further detail. `rust-v0.148.0-alpha.1`

11 **Persistent ordered conversation sections** NEW

35

Organizes conversations into persistent, manually ordered sections and supports incremental browsing of long transcripts.

– Describes behavior but no UI path or config named. `rust-v0.147.0`

12 **MCP server auto-recovery after OAuth reauth** IMPROVED

25

Recovers MCP servers automatically after OAuth reauthentication.

– Brief statement, no mechanism or config detail. `rust-v0.148.0-alpha.1`

13 **Lazy startup of cached MCP servers for subagents** IMPROVED

25

Starts cached MCP servers lazily for subagents, reducing startup overhead.

– States benefit, no mechanism specifics. `rust-v0.148.0-alpha.1`

14 **Inline visualization content references** NEW

15

Supports content references for inline visualizations.

– Bare description, no format or usage detail. `rust-v0.148.0-alpha.1`

15 **Per-agent context window tracking** NEW

15

Tracks context windows per agent.

– Bare feature name, no mechanism given. `rust-v0.148.0-alpha.1`

16 **Model routing hints sent to backend** NEW

15

Sends model routing hints to the Codex backend.

– Bare statement, no mechanism or format specified. `rust-v0.148.0-alpha.1`

╰──▷ BREAKING ON UPGRADE

! The deprecated `--full-auto` flag for `codex exec` has been removed; use `--sandbox workspace-write` instead.

! Redundant Linux bundle archives are no longer published; use the standard `codex-package-<target>` release archives instead.

WAS THIS USEFUL? 👍 👎

Pi

2 RELEASES · 2026-08-06 → 2026-08-07 NOTES ↗

AI agent toolkit: unified LLM API, agent loop, TUI, coding agent CLI

> Pi's biggest change this window is v0.84.0, which introduced a fullscreen TUI mode, per-directory `AGENTS.override.md` context, custom model `samplingParams`, and a v4 lane-based session storage rewrite that breaks several extension and provider APIs; v0.84.1 followed with a `pi auth check` credential preflight command, a new Qwen Token Plan Individual provider, and fullscreen text-selection improvements.

└──▷ WHAT SHIPPED · 10 FEATURES most completely described first ? what's the number?

01 **v4 lane-based session storage API** BREAKING 90

Replaces the inherited pi-agent-core harness session model with the v4 lane-based `Session`, `SessionStorage`, and `SessionRepo` APIs. Legacy JSONL and in-memory repository APIs are removed; code must migrate to `JsonlSessionRepo` or `InMemorySessionRepo`, and custom harness file-system implementations must now provide a FileSystem.renameFile() operation for atomic JSONL publication.

— Named replacement classes and required migration path v0.84.0

02 **Provider/extension registry API changes** BREAKING 90

Renames `ModelsStreamTransforms` to `ModelsRequestTransforms`; changes ModelRegistry.getApiKeyAndHeaders() to return `ProviderHeaders` with `string | null` values; changes ModelRegistry.refresh() to accept `ModelsRefreshOptions` and return `ModelsRefreshResult`; changes ModelRuntime.setRuntimeApiKey() to accept auth cancellation options instead of catalog refresh options, requiring a separate refresh({ providers: [providerId], signal }) call; replaces dynamic provider refresh context store access with the read-only `context.stored` snapshot and generation-checked context.publish() transaction; and requires config-form extension OAuth refreshToken(credentials, signal) callbacks to accept and honor a concrete abort signal.

— Multiple renamed/changed APIs given with exact signatures v0.84.0

03 **Custom `samplingParams` model configuration** NEW 75

Supports custom `samplingParams` (e.g. `temperature`, `top_p`) and a `thinking_token_budget` field in model configuration, demonstrated for a vLLM-hosted model.

Configure a vLLM-hosted model with custom sampling parameters and a thinking token budget.

```json
{
  "id": "vllm/qwen3-235b",
  "samplingParams": {
    "temperature": 0.6,
    "top_p": 0.95
  },
  "thinking_token_budget": 8192
}
```

— Concrete config fields with worked JSON example v0.84.0

04 **`pi auth check` credential preflight command** NEW 73

New `pi auth check` command runs provider/model auth preflight before a run and can optionally emit the resolved credential.

Verify that a provider or model's credentials are correctly configured before running a session.

```
$ pi auth check
```

Verify that your configured provider credentials are valid before starting a long agent run.

```
$ pi auth check
```

— Exact runnable command with clear preflight purpose given v0.84.1

05 **Qwen Token Plan Individual provider** NEW 60

Adds `QWEN_TOKEN_PLAN_API_KEY` environment variable and Qwen Token Plan Individual as a built-in provider with its documented subscription model catalog.

— Env var and provider named, no usage example shown v0.84.1

THINNER COVERAGE BELOW

06 **`terminate` support for blocked extension tool_call events** NEW 55

Adds `terminate` support to blocked extension `tool_call` events, allowing all-terminating batches to skip the automatic follow-up model call.

— Behavior explained but no code example provided v0.84.1

07 **Ctrl+P/Ctrl+N prompt history navigation** NEW 50

Adds opt-in `Ctrl+P` / `Ctrl+N` prompt history navigation in the TUI editor.

— Keybindings named but opt-in mechanism not detailed `v0.84.0`

08 **Fullscreen TUI text selection improvements** NEW 45

Adds double-click word selection, granularity-aware drag selection, and triple-click paragraph selection in fullscreen mode.

— UI behavior named, no navigation or config detail `v0.84.1`

09 **Unbound half-page transcript scrolling in fullscreen mode** NEW 35

Adds unbound half-page transcript scrolling actions for fullscreen mode, configurable via keybindings.

— Feature named but exact keybindings not specified `v0.84.1`

10 **Baseten provider support** NEW 23

Adds Baseten as a supported model provider.

— Only named in summary, no further detail given `v0.84.0`

└──▷ BREAKING ON UPGRADE

! The `ModelsStreamTransforms` interface is renamed to `ModelsRequestTransforms`; extensions referencing `ModelsStreamTransforms` will break.

! JSON and RPC `message_update` events now emit only `assistantMessageEvent` deltas; the cumulative `message` and `assistantMessageEvent.partial` fields are removed. Clients must assemble deltas between `message_start` and `message_end`.

! ModelRegistry.getApiKeyAndHeaders() now returns `ProviderHeaders` with `string | null` values; extensions that inspect returned headers must handle `null`.

! ModelRegistry.refresh() now accepts `ModelsRefreshOptions` and returns `ModelsRefreshResult` instead of discarding cancellation and provider errors.

! ModelRuntime.setRuntimeApiKey() now accepts auth cancellation options instead of catalog refresh options; callers must call refresh({ providers: [providerId], signal }) separately when remote freshness is required.

! Config-form extension OAuth refreshToken(credentials, signal) callbacks are now required to accept and honor a concrete abort signal.

! Dynamic provider refresh context store access is replaced with the read-only `context.stored` snapshot and generation-checked context.publish() transaction; handwritten Provider.refreshModels() implementations using context.store.read() / context.store.write() must migrate.

! The inherited pi-agent-core harness session model is replaced with the v4 lane-based `Session`, `SessionStorage`, and `SessionRepo` APIs; code using the old session model will break.

! The legacy JSONL and in-memory repository APIs are removed; code must migrate to `JsonlSessionRepo` or `InMemorySessionRepo` from pi-agent-core v4.

! Custom harness file-system implementations must now provide a FileSystem.renameFile() operation for atomic JSONL publication.

! `RemoteSession.sessions` no longer exposes runtime phase, model, thinking, attachment, or lock state; that data is now only available from acquired `SessionSnapshot` values.

WAS THIS USEFUL? 👍 👎

Cline ⓘ 1 RELEASE · 2026-08-07 NOTES ↗ CODE ↗

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

> Cline desktop v0.0.10 adds OAuth authentication for remote MCP servers, new CLI commands to remove MCP servers, and several UX improvements around connection status and error visibility.

└──▷ **WHAT SHIPPED · 7 FEATURES** most completely described first ? what's the number?

01 **`cline mcp uninstall`/`mcp rm` commands** NEW 80

New `cline mcp uninstall <name>` command (alias `cline mcp rm`) removes a registered MCP server from `cline_mcp_settings.json`. Supports scripting via flags like `--json` for output.

Remove a registered MCP server by name when decommissioning an integration.

```
$ cline mcp uninstall docs
```

Remove a remote MCP server using the short alias, with JSON output for scripting.

```
$ cline mcp rm remote --json
```

— Exact command, alias, and config file named with runnable examples desktop-v0.0.10

02 **`CLINE_MCP_SETTINGS_PATH` environment variable** NEW 75

New `CLINE_MCP_SETTINGS_PATH` environment variable points the CLI at a custom MCP settings file, enabling per-project or per-repo MCP server configs.

Point the CLI at a project-specific MCP settings file to manage per-repo server configs.

```
$ CLINE_MCP_SETTINGS_PATH=./project/cline_mcp_settings.json
cline mcp uninstall legacy-server
```

— Exact env var name with runnable usage example desktop-v0.0.10

03 **OAuth for remote MCP servers** NEW 65

Remote MCP servers can now authenticate via OAuth from Settings → MCP, including servers that require a pre-registered OAuth client (client ID/secret) instead of dynamic registration. Stored tokens are invalidated when a server's client configuration changes.

— Names UI path and mechanism but no exact flag/endpoint `desktop-v0.0.10`

04 **New keyboard shortcuts for sessions and settings** NEW

65

New shortcuts: `Cmd/Ctrl+N` starts a new session, `Cmd/Ctrl+,` opens settings, and `Esc` stops the current turn.

— Exact keybindings given but no deeper mechanism `desktop-v0.0.10`

THINNER COVERAGE BELOW

05 **'Connect a model' welcome screen notice** NEW

45

Welcome screen shows a notice when no provider has credentials configured, updating live as credentials are added, and recognizing Bedrock/Vertex and keyless local endpoints as already connected.

— Describes behaviour but no config surface to act on `desktop-v0.0.10`

06 **Enriched error surfacing for failed turns** IMPROVED

40

Failed turns now surface an error in the transcript enriched with the underlying cause and a pointer to Settings → Models, instead of failing silently.

— Explains behaviour change but no named surface `desktop-v0.0.10`

07 **Per-server MCP error visibility** IMPROVED

40

MCP errors are now shown on the individual server rather than as a page-level error, and servers with invalid configuration surface their error instead of disappearing silently.

— Clear behaviour change but no exact UI path or config detail `desktop-v0.0.10`

WAS THIS USEFUL? 👍 👎

OpenCode

1 RELEASE · 2026-08-07 | NOTES ↗ | CODE ↗

The open source coding agent.

> OpenCode added a configurable TUI cursor style, JSON export of full session transcripts from the UI, and expanded desktop locale support.

└──▷ **WHAT SHIPPED · 3 FEATURES** most completely described first ? what's the number?

01 Configurable TUI cursor style and blinking NEW

85

A new `cursor` config block controls the terminal cursor in TUI input fields via `cursor.style` (accepting `"block"` (default), `"underline"`, `"line"`, or `"default"`) and `cursor.blinking`; setting `style` to `"default"` restores the terminal's own cursor and makes `blinking` have no effect.

Set a blinking underline cursor in TUI input fields instead of the default block cursor.

yaml

```yaml
cursor:
  style: "underline"
  blinking: true
```

Set a non-blinking block cursor in OpenCode for a stable, high-contrast editing experience.

json

```json
{
  "cursor": {
    "style": "block",
    "blinking": false
  }
}
```

— Exact config keys and values given with runnable YAML/JSON examples. product docs

02 Session export as JSON from the UI NEW

70

Full session transcripts can now be exported as JSON via an `Export...` option in the session 3-dot dropdown, an `Export session` button in the Context tab, or the `session.export` command palette action invoked with `/export`.

— Names exact UI controls and command but no runnable example. v1.18.15

THINNER COVERAGE BELOW

03 Broader desktop locale support IMPROVED

15

The desktop app expands locale coverage with much broader language support.

— No languages, counts, or mechanism named. v1.18.15

WAS THIS USEFUL? 👍 👎

Claude Code

1 RELEASE · 2026-08-07 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 v2.1.224 adds self-hosted execution runners, cross-session messaging with approval controls, archive-based plugin installs, and new sandbox credential-masking options, alongside several Remote Control and fullscreen improvements.

└──▷ WHAT SHIPPED · 10 FEATURES most completely described first ? what's the number?

01 **Sandbox credential-masking options** NEW 95

New sandbox credential-masking options — `extract` and `onExtractNoMatch` for structured env values, `decode: "jwt"` with `maskClaims` for JWT-aware masking, and `awsPairs` / `sigv4` for AWS SigV4 re-signing — are honored only from user, managed, or `--settings` settings and require `network.tlsTerminate`.

Enable JWT-aware credential masking in the sandbox to redact specific claims from bearer tokens before they leave the environment.

yaml

```yaml
decode: "jwt"
maskClaims:
  - sub
  - email
  - aud
```

— Names exact config keys and shows a working YAML example. v2.1.224

02 **Bedrock cross-region inference profile override** NEW

85

New `ANTHROPIC_BEDROCK_REGION_PREFIX` environment variable lets Bedrock users prefer a specific cross-region inference profile over the `AWS_REGION` `-derived` default.

Route Bedrock API calls through a specific cross-region inference profile instead of the one derived from `AWS_REGION`.

```
$ export ANTHROPIC_BEDROCK_REGION_PREFIX=us-west-2
claude
```

— Exact env var name plus a runnable shell example. v2.1.224

03 **Cross-session SendMessage and ListAgents API** NEW

75

New cross-session `SendMessage` API lets Claude Code sessions message each other across any of your machines; `ListAgents` discovers available sessions (macOS and Linux).

— Names two API calls but gives no call syntax. v2.1.224

04 **Self-hosted runner subcommand** NEW

70

New `claude self-hosted-runner` subcommand turns your own machines or containers into execution environments for Claude Code web, mobile, and desktop sessions, available on Team and Enterprise plans.

— Names the subcommand but no usage example given. v2.1.224

05 **Cross-session message approval settings** NEW

65

New `crossSessionInbound` and `dialogExpiry` settings control cross-session messaging: messages sent to a bypassed-permission session are held for approval, while messages to other sessions auto-deliver.

— Names settings but not the file they live in. v2.1.224

06 **Archive plugin source for installs** NEW

65

New `archive` plugin source lets you install plugins from a zip over HTTPS without git or npm, with optional SHA-256 pinning.

— Names the source type and pinning mechanism, no example shown. v2.1.224

07 **Subagent spawn cap removed** IMPROVED

60

Removes the 200-subagent-per-session spawn cap, allowing long-running sessions to continue spawning agents without hitting a hard limit; concurrency and depth limits still apply.

— Gives exact old limit but no way to configure new behavior. v2.1.224

THINNER COVERAGE BELOW

08 **Remote Control compaction and clear sync** IMPROVED 55

Remote Control improvements let attached web and mobile clients see compaction progress and the post-compaction boundary; `/clear` resets now propagate to attached clients.

— Names `/clear` command but describes rest in prose. v2.1.224

09 **Remote Control persistent failure indicator** IMPROVED 45

Remote Control now shows a persistent failure indicator with details and a reconnect shortcut on connection failure, instead of only an 8-second toast.

— Describes UI change with no named surface or path. v2.1.224

10 **Fullscreen mode full compaction history** IMPROVED 45

Fullscreen mode now keeps the full pre-compaction history in scrollback across repeated compactions instead of only the most recent interval.

— Explains behaviour change but no config or command to act on. v2.1.224

WAS THIS USEFUL? 👍 👎

DEPLOY

◆ AI Model & Data Infrastructure

emisar ⓘ 1 RELEASE · 2026-08-07 NOTES ↗

An MCP that lets AI tools securely connect to your infrastructure, write IaaS code, debug issues, and assist during incidents - without risking production stability. Built for security teams to approve and infrastructure teams to experience like magic.

> emisar runner 0.17.2 adds BunnyCDN operations, explicit runbook targets, and zone placement control for production MIG rollouts.

└──▷ **WHAT SHIPPED · 3 FEATURES** most completely described first ? what's the number?

01 **Production MIG rollout zone placement** NEW 35

Production Managed Instance Group (MIG) rollouts can now be placed in available zones, giving control over rollout placement.

– Names MIG and zone placement but no flag or config shown. `runner-v0.17.2`

02 **BunnyCDN operations support** NEW 25

The emisar runner adds operations for BunnyCDN, expanding the set of infrastructure providers it can act on.

– Names BunnyCDN but no specific operations or commands given. `runner-v0.17.2`

03 **Explicit runbook targets** NEW 20

Runbooks can now specify explicit targets, per the runner-v0.17.2 release notes.

– No config key or syntax provided for the target field. `runner-v0.17.2`

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · August 7, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe