THE CYBER TOOLCHAIN

NO. 052

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED AUGUST 21, 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 18 tools

APPLICATION SECURITY

◆ SAST / SCA / Code Security

StackHawk ⓘ 1 RELEASE · seen 2026-08-21 NOTES ↗

StackHawk is an application security testing platform that performs dynamic security scanning to find vulnerabilities in web applications during development and CI/CD pipelines.

> StackHawk's HawkScan 6.4.0 gives explicit control over scan depth across multiple authentication profiles, adds a new HTTP header authentication-bypass scan rule, and fixes `hawk validate` so it actually fails CI on a broken configuration.

└──▷ WHAT SHIPPED · 5 FEATURES most completely described first ? what's the number?

01 Multi-profile scan mode control NEW 95

Adds `--profile-scan-mode` flag (env: `PROFILE_SCAN_MODE`) to control plugin coverage across authentication profiles: `business-logic` (default, BOLA/BFLA only), `primary-full` (full policy on one profile, BOLA/BFLA on the rest), or `all-full` (full policy on every profile). Adds `--full-scan-profile` flag (env: `FULL_SCAN_PROFILE`) to designate which profile receives the full scan policy under `primary-full` mode, defaulting to the first profile declared in configuration. Findings from multi-profile scans now carry a `[profile=<name>]` prefix on their evidence identifying which identity a vulnerability was discovered under.

Run a full policy scan against your primary auth profile while still running BOLA/BFLA against all other profiles, to get deep coverage without multiplying scan time.

```
$ hawk scan --profile-scan-mode primary-full --full-scan-profile admin-user stackhawk.yml
```

Run a full policy scan against your primary profile and BOLA/BFLA-only against all others during multi-profile testing.

```
$ hawk scan --profile-scan-mode primary-full --full-scan-profile admin stackhawk.yml
```

— Full flag/env names, all three modes, and a runnable example `snapshot-20260821`

02 hawk validate exits non-zero on config errors BREAKING 80

`hawk validate` / `hawk validate config` previously exited `0` even on hard validation errors and missing configuration files. It now exits non-zero in those cases, making it usable as a real CI gate; warnings (unknown-property, lint) continue to exit 0.

Pipelines relying on the old always-zero behavior will now correctly fail on a broken configuration.

Gate a deployment on a valid StackHawk config — the pipeline now stops on a broken configuration instead of silently continuing.

```
$ hawk validate config stackhawk.yml && ./deploy.sh
```

— Exact before/after exit-code behavior with a CI gating example `snapshot-20260821`

---

03 **HTTP Header Authentication Bypass scan rule** NEW 75

Adds active scan rule plugin `40059` (HTTP Header Authentication Bypass) that tests whether authentication can be bypassed via injected headers such as `X-Forwarded-For`, `X-Original-URL`, and `X-Rewrite-URL`. Disabled by default; enabled through policy management.

— Names plugin id and headers but no runnable example `snapshot-20260821`

---

04 **External authentication indicator config guidance** NEW 65

Adds `hawk config show app.authentication.external` guidance recommending `loggedInIndicator: '.*'` and `loggedOutIndicator: '$^'` to prevent spurious re-authentication attempts when using external credentials.

Configure external authentication credentials to suppress spurious re-auth attempts and misleading log lines during BOLA/BFLA testing.

```yaml
app:
  authentication:
    external:
      loggedInIndicator: ".*"
      loggedOutIndicator: "$^"
      testPath: /api/v1/me
```

— Named config keys and values with a config example `product docs`

THINNER COVERAGE BELOW

05 Oracle time-based SQL injection detection improved IMPROVED

50

Oracle time-based SQL injection detection (plugin `40021`) now uses dose-response confirmation rather than a single delayed response, improving accuracy.

— Names plugin and mechanism change but no example `product docs`

└──▷ BREAKING ON UPGRADE

! `hawk validate` previously exited `0` even on hard validation errors and missing configuration files; it now exits non-zero in those cases, which will cause pipelines relying on the old always-zero behavior to correctly fail on a broken configuration.

! `hawk validate config` previously exited 0 even on hard validation errors; it now exits non-zero for hard errors and missing configuration files. Pipelines relying on the always-zero exit code will now correctly fail on a broken configuration.

WAS THIS USEFUL? 👍 👎

Snyk Code

1 RELEASE · 2026-08-21 BLOG ↗

Snyk Code is a static analysis tool that scans source code to identify and fix security vulnerabilities and code quality issues.

> Snyk Code's biggest change this window is that committed files matched by `.gitignore` are now scanned by default (a mandatory, non-disableable shift for CLI users on 1.1307.0+), alongside new template-file XSS analysis and expanded Java library and language coverage.

└──▷ WHAT SHIPPED · 5 FEATURES most completely described first ? what's the number?

01 Committed .gitignore files now analyzed by default BREAKING

80

Committed files matched by `.gitignore` rules are now analyzed by Snyk Code and Snyk Secrets across all interfaces, and this behavior cannot be disabled. CLI scans require Snyk CLI 1.1307.0 or later to pick up the new behavior; earlier CLI versions retain the old behavior, so CLI results can differ from SCM and web results until upgraded. `.snyk` exclude patterns remain the supported way to deliberately exclude a path from analysis.

— Names exact CLI version and config file, clear upgrade action 2026-08-21-72f14d53

02 Template-file XSS analysis across ten engines NEW

70

Snyk Code now analyzes template files and traces data flow from application code into the template, reporting XSS vulnerabilities that only become exploitable at render time. Supported engines: Jinja2, Razor, FreeMarker, EJS, Handlebars, Pug, Thymeleaf, Twig, Mustache, and Velocity.

— Names mechanism and all ten engines but no user action 2026-08-21-72f14d53

03 Expanded Java library detection coverage IMPROVED

60

Adds or improves Java library coverage for Apache CXF (including HTTP transport), OkHttp, Spring Security OAuth2 Client, Google OAuth Client, Google API Client, MSAL4J, Apache Commons Collections, Flyway, JAXB, and SAP Commerce (Hybris) FlexibleSearch queries with safe parameter binding.

— Names ten libraries but no configuration or usage step 2026-08-21-72f14d53

THINNER COVERAGE BELOW

04 Broader source/sink detection across languages IMPROVED

50

Recognizes Python LangChain LiteLLM as a source of untrusted data, and extends detection coverage for Java, Kotlin, C#, Go, JavaScript, and PHP with additional sources, sinks, and unsafe API patterns, particularly for cryptography.

— Names LiteLLM and six languages but no concrete rule list `2026-08-21-72f14d53`

05 **Java 25 source analysis support** NEW 30

Adds support for analyzing Java 25 source code.

— Bare statement of version support, no further detail `2026-08-21-72f14d53`

└─▷ **BREAKING ON UPGRADE**

! Committed files matched by a `.gitignore` rule are now included in analysis across all interfaces and this cannot be disabled. CLI scans require an upgrade to Snyk CLI 1.1307.0 or later; earlier versions retain the previous behavior, causing CLI results to differ from SCM and web results.

WAS THIS USEFUL? 👍 👎

StepSecurity

1 RELEASE · 2026-08-21 BLOG ↗

StepSecurity is a security platform that hardens GitHub Actions workflows and CI/CD pipelines by reducing attack surface and preventing supply chain compromises.

> Dev Machine Guard v1.16.0 adds two brand-new local inventories — credential locations and browser extensions — and broadens AI agent, MCP, and dev-tool detection with several targeted scope expansions.

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

01 Credential location inventory across 13 sources NEW

75

New credential location inventory scans thirteen sources — AWS credentials, AWS config, GCP application default credentials, SSH private keys, git credential store, `.netrc`, GitHub CLI hosts, `.npmrc`, `.pypirc`, Docker config, kubeconfig, Terraform credentials, and Vault token — reporting exact file path, credential count, usable-or-wrapped status, file mode (macOS/Linux), and whether the file is tracked inside a git repository; no credential value, substring, digest, or fingerprint ever leaves the device.

— Full mechanism and field list given but no command or UI path.

Dev Machine Guard v1.16.0 (2026-08-21)

02 Browser extension inventory across three browsers NEW

75

New browser extension inventory covers Google Chrome, Microsoft Edge, and Mozilla Firefox (including Firefox under snap/flatpak and Edge under flatpak) on macOS, Windows, and Linux, recording per-extension identity (id, name, version, manifest version), enabled state and who disabled it, install method (store, sideloaded, registry installed, unpacked, or policy installed), store attribution and listing/flag status, Firefox signature state, and the host and API permissions the browser is currently honouring.

— Exhaustive field and platform coverage but no direct usage step.

Dev Machine Guard v1.16.0 (2026-08-21)

03 **OpenCode MCP server collection** NEW 75

OpenCode MCP servers are now collected from `~/.config/opencode/opencode.json` and `opencode.jsonc` (both formats, including comments and trailing commas), using the top-level `mcp` key OpenCode declares rather than `mcpServers`; project-level configs are found by the existing bounded search.

— Names exact config file paths and key readers can check.

Dev Machine Guard v1.16.0 (2026-08-21)

04 **Pi, Factory Droid, and Amp detection added** IMPROVED 65

Pi, Factory Droid, and Amp are now detected in the AI agent and tool inventory, proven from on-disk artifacts (npm or Bun manifests, installer anchor directories, Homebrew cask roots, WinGet publisher directories, or pacman file manifests) rather than by binary name, with version read from disk or reported as `unknown`.

— Names detection mechanism and tools but no operator action.

Dev Machine Guard v1.16.0 (2026-08-21)

05 **Copilot CLI detection across seven install locations** IMPROVED 60

Copilot CLI installed via `gh copilot` is now detected across seven additional install locations (the gh copilot download directories on both platforms, the non-root install script path, WinGet and npm global shims, and the gh-copilot extension) when a PATH lookup misses.

— Lists specific install paths but no direct reader action.

Dev Machine Guard v1.16.0 (2026-08-21)

THINNER COVERAGE BELOW

06 **Expanded detection for version managers and agent skills** IMPROVED 55

Detection of global installs now searches per-version trees of `nvm`, `fnm`, `mise`, `volta`, and `asdf`. Two new agent skills roots are scanned: `~/.config/amp/skills` and `~/.agent/skills`.

— Named paths and tools but each addition is a thin one-liner.

Dev Machine Guard v1.16.0 (2026-08-21)

07 **MCP server secret redaction** IMPROVED 50

Secrets held in MCP server `command`, `argument`, and `URL` fields are now redacted before the MCP inventory is reported.

— Names the redacted fields but no further mechanism detail.

Dev Machine Guard v1.16.0 (2026-08-21)

WAS THIS USEFUL? 👍 👎

GitHub

2 RELEASES · 2026-08-20 BLOG ↗

GitHub is a web-based platform for version control and collaborative software development using Git repositories.

> GitHub's latest updates focus on Issues UI refinements (pinned saved views, reaction avatars, dashboard density) and a new Windows 11 arm64 runner image with Visual Studio 2026 that will soon become the default, potentially breaking existing VS2022-dependent workflows.

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

01 Windows 11 arm64 runner image with Visual Studio 2026

BREAKING

95

GitHub-hosted Actions runners gain `windows-11-vs2026-arm` as a `runs-on` target, providing a Windows 11 arm64 image with Visual Studio 2026 on standard and larger runners. Starting September 21, 2026, the existing `windows-11-arm` image will be gradually updated to default to Visual Studio 2026 (rollout completes September 30, 2026), which may break workflows depending on Visual Studio 2022; teams are advised to opt in to `windows-11-vs2026-arm` now via their workflow's `runs-on` field to validate build pipelines before the forced migration.

Opt in to the new VS2026 arm64 image now to validate your build pipeline before the September 2026 forced migration.

yaml

```yaml
jobs:
  build:
    runs-on: windows-11-vs2026-arm
    steps:
      - uses: actions/checkout@v4
      - name: Build
        run: msbuild MyProject.sln
```

— Exact runner label, dates, and a runnable workflow snippet.

Windows 11 arm64 VS2026 image generally …

THINNER COVERAGE BELOW

02 Pinned saved views in repository issues sidebar

NEW

52

Pinning saved views to the repository issues sidebar is now generally available, giving one-click access to a saved view even when the sidebar is collapsed.



— Describes mechanism but no exact UI path or config.

Pinning saved views to the repository is…

03 Issue reaction avatars and dashboard density setting NEW

30

GitHub adds profile avatars for reactions on issues, and introduces an Issues Dashboard density setting to control how many issues are visible at once.





— Two thin UI additions with no configuration details given.

Pinning saved views to the repository is…

└──▷ BREAKING ON UPGRADE

! Starting September 21, 2026, the `windows-11-arm` image will be gradually updated to use Visual Studio 2026 by default (rollout completes September 30, 2026), which may break workflows that depend on Visual Studio 2022.

WAS THIS USEFUL? 👍 👎

Legit Security

1 RELEASE · 2026-08-20 BLOG ↗

Legit Security is a platform that secures software development pipelines by detecting and preventing supply chain attacks across code, build, and deployment stages.

> Legit Security launched VibeGuard 2.0, extending developer endpoint security to discover AI agents and enforce runtime governance over their actions.

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

01 **Runtime governance of AI agent actions** NEW 58

Surfaces sensitive or destructive agent actions — such as deleting code, altering database data, or touching production resources — to the developer at runtime for human-in-the-loop review before execution, and lets security teams enforce organizational policy over which AI agents, skills, and models are permitted in the development environment.

— Describes mechanism and examples but no concrete config or API.

Your AI Agent Has New Skills. Can You Tr…

02 **Discovery of AI agents on developer endpoints** NEW 50

VibeGuard 2.0 extends developer endpoint security to discover and inventory AI agents, models, MCP servers, and skills running in the agentic environment on developer endpoints.

— Names surfaces discovered but no config or command detail given.

Your AI Agent Has New Skills. Can You Tr…

WAS THIS USEFUL? 👍 👎

GitLab

3 RELEASES · 2026-08-20 BLOG ↗

GitLab is a web-based DevOps platform providing Git repository hosting, CI/CD pipelines, and collaboration tools for software development teams.

> GitLab 19.3 adds a Flow Creator agent that turns plain-language requests into runnable Custom Flow YAML, extends GitLab Dedicated to host the Duo Agent Platform's AI Gateway inside customers' own AWS environments, and lets teams bulk-triage and auto-remediate SAST vulnerability backlogs with agentic tooling.

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

01 **Flow Creator agent generates Custom Flow YAML** NEW 88

A new Flow Creator agent in GitLab Duo Agent Platform (accessible via Agentic Chat) converts plain-language descriptions into complete, runnable Flow Registry YAML definitions with no manual schema knowledge required. It reads current Flow Registry documentation before every response and runs a pre-output checklist to catch known failure patterns such as missing `project_id`, broken human-in-the-loop gates, wrong `sends_response_to` targets, and missing stopping instructions. Generated YAML can be pasted directly into the configuration editor when creating a flow from a project or the AI Catalog, with visibility set to private, restricted, or public; enabling a flow still requires Maintainer role or higher, Group Owners/admins can disable Custom Flows entirely, and every flow runs under a scoped service account with composite identity bounded to the top-level group.

Use Flow Creator in Agentic Chat to instantly generate a triage automation without writing any YAML schema.

> 📍 Steps: 1. Open GitLab Duo Agentic Chat in your GitLab 19.3 instance. 2. Invoke Flow Creator and enter: 'When a work item is created with the label security-triage, check it against our known false-positive patterns, find the affected dependency and its owner, and post a severity assessment as a comment.' 3. Respond to any clarifying questions (e.g., target project, whether a human-approval step is needed). 4. Copy the generated flow definition YAML. 5. Go to your project › AI Catalog › Create Flow, paste the YAML into the configuration editor, set visibility (private / restricted / public), and add the desired triggers.

— Names exact failure checks and roles, includes runnable steps

Build custom flows in minutes with the F…

02 **Bulk SAST false positive detection and agentic resolution** NEW 88

The vulnerability report gains a bulk-select UI to run SAST False Positive Detection and Agentic SAST Vulnerability Resolution across multiple findings at once instead of one-at-

a-time triage. False Positive Detection analyzes surrounding code and returns a confidence score and explanation; findings imported from third-party scanners via SARIF format into the unified vulnerability report can also be run through these bulk agentic flows. Pipelines can also run both automatically on Critical and High severity new findings so triage and fix MR creation happen before a developer opens the finding, and bulk jobs show a progress indicator with a cancellation control plus concurrency limits to avoid competing with pipeline build capacity.

Triage and remediate your entire SAST backlog at once instead of opening each finding individually.

> 📍 In the GitLab vulnerability report, select all SAST findings using the bulk-select checkbox, then choose 'Run SAST False Positive Detection' followed by 'Run Agentic SAST Vulnerability Resolution' from the bulk-action menu. A progress indicator tracks the job; click Cancel to stop it at any point.

— Names SARIF, severity thresholds, UI flow with runnable example

When your backlog outgrows your team, Gi…

THINNER COVERAGE BELOW

03 **AI Gateway hosted inside GitLab Dedicated** NEW 57

GitLab Dedicated now hosts the AI Gateway for the Duo Agent Platform inside each customer's single-tenant AWS environment, keeping AI inference within the customer's chosen AWS region and data residency boundary. It supports Amazon Bedrock as a model backend and a bring-your-own-model option so customers can connect preferred model providers under their own data classification rules, unlocking all Duo Agent Platform capabilities — including automated custom code reviews, fixing failed pipelines, and security analysis — against customer-selected models.

— Names AWS Bedrock and BYOM but gives no setup steps

Run agentic software delivery inside the…

WAS THIS USEFUL? 👍 👎

Veracode

2 RELEASES · 2026-07-31 → 2026-08-19 BLOG ↗

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

> Veracode's CLI added packaging exit codes, a toolchain-discovery command, batch vulnerability fixing, target-UUID dynamic scans, OAuth2 onboarding, and SBOM generation in CycloneDX/SPDX formats, while its integrations gained platform-managed GitHub app installs, new veracode.yml config keys, and expanded Java API Wrapper coverage — alongside breaking changes to CLI defaults and a Jira Server 9.x end-of-support notice.

└──▷ WHAT SHIPPED · 22 FEATURES most completely described first ? what's the number?

01 New flags and environment variables for `veracode package` NEW

95

Adds `--exclude` (v2.51.0) to prevent specified Java packages or JAR files from being scanned; `--skip-packagers` (v2.48.0) to exclude specific artifacts from packaging without affecting other languages; `--java-source` flag and `VERACODE_PACKAGE_JAVA_SOURCE=true` env var (v2.46.0) for Java source code packaging; `VERACODE_PACKAGE_GOLANG_GENERATE` env var (v2.43.0) for client-side CGO code generation when packaging Go apps; `SRCLR_MAKE_WINDOWS` env var (v2.44.0) to preprocess C/C++ source with Make on Windows using a native gcc or clang compiler; a new `--verbose` flag (v2.38.0), deprecating `--debug`; an option to process all Makefiles in a directory tree (v2.41.0); and an option to include the directory path in the artifact name for easier flaw location (v2.41.0).

— Every flag and env var named verbatim with exact behavior. CLI updates (2026-07-31)

02 `veracode package discover` command and packaging exit codes

NEW

85

Introduces the `veracode package discover` command to detect toolchains required to create scannable artifacts (v2.44.0), later adding Gradle toolchain detection for Java projects (v2.46.0) and its own exit codes (v2.48.0). `veracode package` gains a `--strict` flag that returns exit code 4 on build failures during packaging (v2.39.0), plus exit codes 5, 6, and 7 for packaging/build issues to improve CI/CD automation (v2.49.0).

— Names exit codes and flags but not their individual meanings. CLI updates (2026-07-31)

03 New veracode.yml configuration keys across Workflow Integrations

NEW

85

Azure DevOps Workflow Integration v2.3.10 adds `analysis_branch` key support in `veracode.yml` so scheduled scans run against a specified branch instead of the default. Azure DevOps v2.3.6, GitHub v1.0.6, and GitLab v2.1.4 add a `debug` configuration option in `veracode.yml` to enable debugging and troubleshooting. Azure DevOps v2.4.3 adds a custom agent pool name parameter in `veracode.yml` to specify the agent pool used for pipeline execution.

Target scheduled Azure DevOps scans at a specific branch rather than the repo default, useful when your mainline integration branch differs from the default.

yaml

```yaml
# veracode.yml
analysis_branch: main-security
```

Enable debug output in veracode.yml to troubleshoot pipeline scan failures across GitHub, GitLab, or Azure DevOps Workflow Integrations.

yaml

```yaml
# veracode.yml
debug: true
```

— Exact keys and file given with example snippets. Integration updates (2026-08-19)

04 **Result quality and reliability improvements in `veracode scan`**

IMPROVED

80

`veracode scan` categorizes secret-type findings as Critical (v2.45.0), prioritizes vulnerability results from the NVD database when available (v2.45.0), introduces schema enhancements for container and IaC scan results (v2.51.0), enables specifying a custom location from which vulnerability databases can be downloaded (v2.41.0), adds support for parsing Dockerfile heredoc syntaxes (v2.41.0), and retries failed static scans up to five times on server errors or too-many-requests responses (v2.38.0).

— Enumerates each behavior change but omits the custom DB location config key.

CLI updates (2026-07-31)

05 **New default for `SRCCLR_DOWNLOAD_URL`**

BREAKING

80

The `SRCCLR_DOWNLOAD_URL` environment variable now defaults to `https://sca-downloads.veracode.com`, deprecating the previous default of `https://download.sourceclear.com`; update all instances in your environment (v2.39.0).

— Exact old and new URLs given with an update instruction. CLI updates (2026-07-31)

06 **Java API Wrapper API coverage and reliability improvements**

IMPROVED

80

Java API Wrapper v26.3.19.0 adds page size support to the Platform Applications API (`/appsec/v1/applications`) and introduces support for the paginated Sandbox REST API for retrieving sandbox lists. v26.2.18.0 adds support for the Veracode Platform Findings REST API to access open and mitigated application findings, and implements a configurable retry mechanism for `appsec/v1/applications` .

— Names endpoints and versions but no wrapper method signatures.

Integration updates (2026-08-19)

---

07 **GitHub Workflow Integration platform-managed lifecycle and packaging**

NEW

80

GitHub Workflow Integration v2.0.0 enables installing, configuring, and updating credentials for the GitHub integration directly from the Veracode Platform, eliminating manual GitHub Marketplace steps, and adds autopackaging support for Apex, VB6, and Perl. v2.1.1 adds a new uninstallation workflow on the Veracode Platform to remove the Veracode app from GitHub organizations, updates the default runner image to `scm-packaging-5.0.0` (including Alpine v3.24.0, Ubuntu v26.04, .NET v10, PipEnv v2026.6.2, libicu v78, Node.js v22.22.1, and Python v3.14.4), and downgrades GitHub Veracode Workflow App permissions to remove administration permissions, preventing the app from altering or removing installed repositories.

— Names install/uninstall workflow and runner image but not exact platform navigation.

Integration updates (2026-08-19)

---

08 **New language and build tool support in `veracode package`** NEW

75

`veracode package` adds support for the Poetry package management tool in Python for autopackaging (v2.47.0), `requirements-dev.txt` in Python packaging workflows to include development dependencies (v2.48.0), a generic packager for Apex (v2.43.0), packaging for MSBuild .NET framework projects (v2.42.0), Go v1.24 (v2.40.0), and .NET 9 (v2.38.2).

— Lists each new supported tool/version without usage specifics. CLI updates (2026-07-31)

---

09 **SBOM generation in `veracode sca`** NEW

75

`veracode sca` now supports SBOM generation via SCA agent-based scans, with results publishable in CycloneDX 1.6 and SPDX 2.3 formats (v2.41.0).

— Names exact SBOM formats but not the publishing flag. CLI updates (2026-07-31)

---

10 **Deprecation of legacy Flaw Importer task name** DEPRECATED

75

The `Veracode Flaw Importer` task (with spaces in the task name) in the Veracode Azure DevOps extension v3.35.0 is deprecated and replaced by `VeracodeFlawImporter`; the old task is scheduled for removal in a future release.

– Names old and new task names but no removal date. `Integration updates (2026-08-19)`

---

11 **End of support for Jira Server/Data Center 9.x** DEPRECATED

75

Veracode will end support for the Veracode Integration for Jira on Jira Server and Jira Data Center 9.x on November 30, 2026; upgrade to Jira 10 or later to maintain a supported configuration.

– Exact date and target version given, no migration steps detailed.

`Integration updates (2026-08-19)`

---

12 **Custom policy evaluation in `veracode scan`** NEW

65

`veracode scan` now allows applying a custom policy defined in the Veracode Platform and viewing policy evaluation for individual findings alongside the overall policy result (v2.44.0).

– Explains the change but no flag name for selecting the policy. `CLI updates (2026-07-31)`

---

13 **Scan scheduling from the Veracode Platform for GitHub and Azure DevOps**

NEW

65

GitHub Workflow Integration v2.0.0 enables scheduling Static Analysis, SCA, and Infrastructure as Code (IaC) scans for GitHub organizations directly from the Veracode Platform. Azure DevOps Workflow Integration v2.3.9 enables scheduling scans for every organization where the integration is installed, driven by `veracode.yml` configuration.

– Names scan types and config trigger but no exact schedule syntax.

`Integration updates (2026-08-19)`

---

14 **Preprocessed source scanning default for C/C++ packaging**

IMPROVED

60

Preprocessed source code scanning is now the default method for C/C++ projects on Windows, and support is now available on Linux, replacing the previous autopackaging solution (v2.39.0).

– States the before/after but no flag to opt out. `CLI updates (2026-07-31)`

---

15 **Target UUID support for `veracode dynamic scan`** IMPROVED

60

`veracode dynamic scan` now supports target UUIDs, in addition to webhook UUIDs, for triggering scans (v2.51.0).

– Names the command and UUID types but no flag syntax. CLI updates (2026-07-31)

16 **OAuth2 onboarding via `auth login`** NEW 60

Introduces the `auth login` command to onboard new users via OAuth2 (v2.41.0).

– Names the exact command but not the OAuth2 flow details. CLI updates (2026-07-31)

17 **Data incompleteness warning for pre-v2.48.0 CLI** BREAKING 60

Using CLI versions older than v2.48.0 with the Veracode Platform will result in incomplete data displayed in the platform (v2.48.0); upgrading the CLI is needed to avoid missing data.

– States exact version threshold but no detail on what data is missing.

CLI updates (2026-07-31)

THINNER COVERAGE BELOW

18 **Batch fix processing in `veracode fix`** IMPROVED 55

`veracode fix` now supports enhanced batch fix processing, enabling remediation of a large number of vulnerabilities in a single batch operation (v2.51.2).

– Names the command but not the batch size limit or syntax. CLI updates (2026-07-31)

19 **Azure DevOps SCA policy enforcement for build failures** IMPROVED 55

Azure DevOps Workflow Integration v2.3.3 enforces SCA scan failure when vulnerabilities are found under a custom policy with the 'Build Action: error' configuration for agent-based scans.

– Specific config value named but no full setup steps. Integration updates (2026-08-19)

20 **Scan Scope setting and usage analytics in IDE plugins** NEW 55

Veracode Scan for Visual Studio v0.8.0 adds a 'Scan Scope' setting to choose between scanning the full project directory or only the active solution, and adds usage analytics for plugin adoption, feature usage, and scan activity; Veracode Scan for JetBrains v1.8.0 and Veracode Scan for VS Code v1.16.0 add the same usage analytics for plugin adoption, feature usage, and scan activity.

.
.
.
.

– Names the setting but not what analytics data is exposed to whom.

Integration updates (2026-08-19)

21 `--verbose` no longer default for `veracode static scan`

45

BREAKING

The `veracode static scan` command no longer includes the `--verbose` flag by default (v2.38.2).

— States the change but not how to restore verbose output. CLI updates (2026-07-31)

22 Consistent access token reading from disk across CLI IMPROVED

35

All Veracode CLI commands can consistently read access tokens from disk (v2.45.0).

— Describes the change but not the file path or token format. CLI updates (2026-07-31)

└──▷ BREAKING ON UPGRADE

! The Veracode Flaw Importer task (with spaces in the task name) in the Veracode Azure DevOps extension v3.35.0 is deprecated and replaced by `VeracodeFlawImporter`; the old task is scheduled for removal in a future release.

! Veracode will end support for the Veracode Integration for Jira on Jira Server and Jira Data Center 9.x on November 30, 2026; upgrade to Jira 10 or later to maintain a supported configuration.

! The `veracode static scan` command no longer includes the `--verbose` flag by default (v2.38.2).

! The `--debug` flag on `veracode package` is deprecated in favor of `--verbose` (v2.38.0).

! The previous `SRCCLR_DOWNLOAD_URL` default of `https://download.sourceclear.com` is now deprecated; the new default is `https://sca-downloads.veracode.com` — update all instances in your environment (v2.39.0).

! Using old CLI versions (pre-v2.48.0) with the Veracode Platform will result in incomplete data displayed in the platform (v2.48.0).

WAS THIS USEFUL? 👍 👎

◆ Secrets Detection & Management

infisical

1 RELEASE · 2026-08-20 NOTES ↗

Infisical is the open-source platform for secrets, certificates, and privileged access management.

> Infisical v0.162.22 adds Kubernetes-native authentication for gateway enrollment, scopes code-signing approvals more granularly, and migrates four Access Control surfaces to a new v3 UI, alongside a Secret Manager insights view and Cloudflare sync performance improvements.

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

01 **infisical-nkp Helm chart 0.2.0 with Valkey and extraEnv** IMPROVED 65

The `infisical-nkp` Helm chart was bumped to 0.2.0, adding Valkey support and an `extraEnv` configuration option.

— Names exact chart, version, and config key v0.162.22

THINNER COVERAGE BELOW

02 **Cloudflare bulk update for worker secrets** IMPROVED 45

Worker secret syncs now use Cloudflare's bulk update endpoint, improving sync performance.

— Names the mechanism but not the endpoint path or numbers v0.162.22

03 **Kubernetes auth for gateway enrollment** NEW 40

Gateways can now be enrolled using Kubernetes-native authentication, adding a new auth method for the gateway enrollment process.

— Names the capability but no config or flag detail v0.162.22

04 **Access Control migrated to v3 UI** IMPROVED 40

Machine identities access control, project access control groups, secret rotations setup flow, and project users access control were all migrated to the new v3 UI in the Access Control section.

— Names all four migrated areas but no functional change detail v0.162.22

05 **Scoped code-signing approvals** IMPROVED 35

Code-signing approvals can now be scoped to a specific signing situation, giving more granular control over approval workflows.

— Describes behavior but not the mechanism for scoping v0.162.22

06 **Secret Manager insights view** NEW 30

A new Secret Manager product insights view provides visibility into secret manager usage and activity.

— Bare description of a new view, no navigation path given v0.162.22

07 **Deprecation notices for native integrations** DEPRECATED 25

Deprecation banners and email notifications now warn users about native integrations that are being deprecated.

— States the notice mechanism but not which integrations v0.162.22

08 **Revamped commit history UI** IMPROVED 20

The commit history UI was revamped to improve auditability of secret changes.

— No specifics on what changed in the UI v0.162.22

WAS THIS USEFUL? 👍 👎

REVERSE ENGINEERING, MALWARE & FORENSICS

◆ Malware Analysis

CAPEv2 ⓘ changes since 2026-08-19 CODE ↗

Malware Configuration And Payload Extraction

CAPEv2 cleaners gain `--banned-clean` flag and `--db-batch-size` control for database deletions.

└──▷ GET THIS VERSION

```
$ git clone --branch commits-2026-08-19
https://github.com/kevoreilly/CAPEv2.git
# already have the repo? check out this version:
$ git checkout commits-2026-08-19
```

└──▷ TRY IT

Purge all banned tasks from the database in large batches to speed up cleanup on a busy instance.

```
$ python utils/cleaners.py --banned-clean --db-batch-size 5000
```

- Adds `--banned-clean` argument to `utils/cleaners.py` to remove all tasks marked with `TASK_BANNED` status.
- Adds `--db-batch-size` argument to `utils/cleaners.py` to control the batch size for MongoDB and SQL database deletions (default: 1000, constant `DB_BATCH_SIZE`).

WAS THIS USEFUL? 👍 👎

CLOUD & CONTAINER SECURITY

◆ CNAPP

Plerion ⓘ 1 RELEASE · 2026-08-21 NOTES ↗

Plerion is a cloud security platform that enables continuous vulnerability discovery and remediation across cloud infrastructure and applications.

> Plerion shipped a new external access grant inventory and in-product review workflow for AWS, letting security teams track, decide on, and audit third-party access across 97 resource types.

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

01 External access grant inventory and review workflow for AWS NEW

83

Plerion now builds an external access grant inventory for every tenant, analyzing 97 AWS resource types across four sharing mechanisms: resource policies, role trust policies, Resource Access Manager (RAM) shares, and cross-account permissions set directly as an attribute. Grants can be exported to a spreadsheet for offline review, or reviewed end-to-end inside Plerion by assigning an accountable team and recording a `Keep`, `Remove`, `Review later`, or `Trust until review` decision with notes and a future review date; a full audit history tracks every decision change, and a `Past due` preset surfaces grants whose review date has passed. A finding is raised for every asset granting access to an external principal not confirmed as trusted, with trusted principals configurable under `Settings > Profiles > Trusted principals`.

Suppress the first-scan wave of untrusted-access findings by pre-loading known-good external principals before reviewing findings one by one.

> 📍 In Plerion, go to Settings › Profiles › Trusted principals and add the AWS account IDs, federated identities, or AWS services that your organization intentionally grants access to.

– Names resource types, mechanisms, statuses and config path, but no API/CLI.

`Review external access to AWS with resou…`

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ Endpoint Security (EDR/XDR)

Huntress

2 RELEASES · seen 2026-08-21 NOTES ↗

Huntress is a managed security platform that provides threat detection, incident response, and endpoint protection for small and mid-sized businesses.

> Huntress added two portal visibility features this window: full IPv4 address exposure per agent and WSL detection across Windows endpoints in Managed EDR.

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

01 **All IPv4 addresses exposed for agents** NEW 75

Huntress Portal now displays all IPv4 addresses associated with an Agent via UI hover and exports, and adds an `ipv4_addresses` REST API field on agent records that returns the full list of IPv4 addresses collected by the Base Agent survey, not just the first one.

— Names exact API field and behaviour change, no example given

All IPv4 Addresses associated with an Ag…

02 **WSL visibility in Managed EDR** NEW 75

Huntress Managed EDR now surfaces Windows Subsystem for Linux (WSL) status on the EDR agent page for each Windows endpoint, showing whether WSL is Installed or Uninstalled. Expanding the field reveals per-account detail including instance name, user account, SID, WSL version, and state (running or stopped), letting teams audit their fleet for unsanctioned WSL usage.

Audit your fleet for unsanctioned WSL usage by reviewing the EDR agent page for each Windows endpoint.

> 📍 In the Huntress portal, navigate to the EDR agent page for a Windows endpoint and review the WSL status field (Installed or Uninstalled), then expand per-account detail to see instance name, user account, SID, WSL version, and state (running or stopped).

— Clear UI navigation and fields, but no API/flag

Windows Subsystem for Linux Visibility i…

WAS THIS USEFUL? 👍 👎

Trend Vision One

2 RELEASES · 2026-08-20 BLOG ↗

Trend Vision One is Trend Micro's unified cybersecurity platform providing threat intelligence, vulnerability management, and incident response across endpoints and networks.

> Trend Vision One's Private Access Connector added PAM authentication support, per-Connector SSH host key uniqueness, automatic recovery of lost registration files, and made token revocation deterministic, alongside smaller log streaming improvements.

└──▷ WHAT SHIPPED · 5 FEATURES most completely described first ? what's the number?

01 **PAM support via updated OpenSSH build** NEW 45

Enables Pluggable Authentication Modules (PAM) support via an updated OpenSSH build, expanding authentication integration options for Private Access Connectors.

— Names PAM and OpenSSH but no config or flag to invoke it

Zero Trust Secure Access Private Access …

02 **Unique SSH host key per Connector** IMPROVED 45

Ensures each Connector generates a unique SSH host key, eliminating host-key collisions in cloned or templated deployments.

— Explains mechanism and problem solved, but is automatic with no user action

Zero Trust Secure Access Private Access …

03 **Auto-recovery of Connector registration file** NEW 45

Adds automatic recovery of the Connector registration file from backup when the file is missing or corrupted, reducing manual intervention after storage failures.

— Describes trigger and benefit but not the recovery process itself

Zero Trust Secure Access Private Access …

04 **Log streaming logging and rotation improvements** IMPROVED 40

Adds more detailed logging to the Connector's log streaming scripts to improve visibility into streaming activity, and adds log rotation for log streaming logs on Rocky Linux 9 Connectors.

— Groups two thin log-streaming increments naming the OS scope

Zero Trust Secure Access Private Access … Zero Trust Secure Access Private Access …

05 **Synchronous token revocation** IMPROVED 40

The token revocation command now runs synchronously, ensuring deterministic completion before returning, instead of completing asynchronously.

— Describes behavior change but doesn't name the exact command

Zero Trust Secure Access Private Access …

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Identity & Access Management

Passbolt ⓘ 1 RELEASE · 2026-08-21 NOTES ↗

Passbolt is an open-source password manager designed for teams to securely store, share, and manage passwords collaboratively.

> Passbolt 5.15 focused on browser extension refinements, improving autofill behavior and reworking the permissions confirmation dialog UI.

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

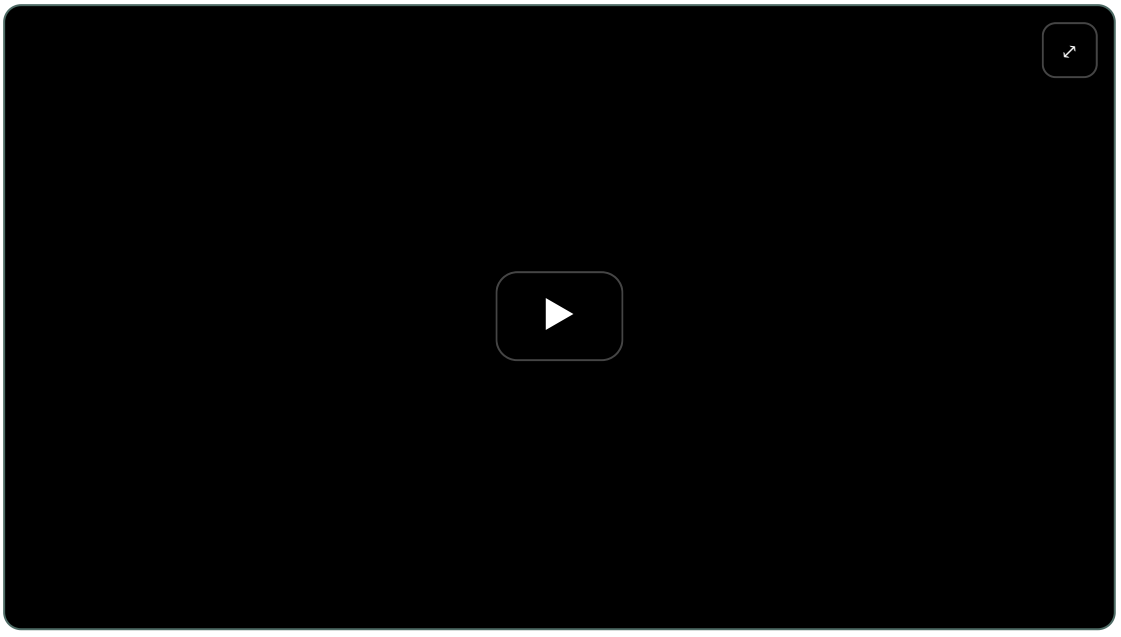
01 **Improved autofill in browser extension** IMPROVED 20

Passbolt's browser extension received improvements to its autofill behavior.

— No detail on what changed in autofill mechanism. Who Is He | Browser Extension & API

02 **Enhanced permissions confirmation dialog UI** IMPROVED 20

The UI for permissions confirmation dialogs has been enhanced.



— No specifics on what UI elements changed. Who Is He | Browser Extension & API

WAS THIS USEFUL? 👍 👎

1Password

1 RELEASE · 2026-08-20 BLOG ↗

1Password is a password manager that securely stores, generates, and autofills login credentials and sensitive information across devices.

> 1Password SaaS Manager added a new Claude Console usage import, expanded workflow automation with custom person-field triggers and a Lark 'Frozen' status field, and made smaller improvements to BambooHR field mapping, AI spend key management, OpenAI Platform error messages, and WPS Office provisioning.

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

01 **Claude Console usage import** NEW 52

Adds Claude Console as a new import source, pulling message and Claude Code usage consumption data into SaaS Manager.

– Names the source and data types but no setup steps

1Password SaaS Manager #1358 (2026-08-20)

02 **Lark 'Frozen' status person field** NEW 52

Adds the Lark 'Frozen' status as a dedicated person field, distinguishing temporary leave from suspension, and makes it usable in workflows.

– Names the field and provider but no exact usage steps

1Password SaaS Manager #1358 (2026-08-20)

03 **Pathify custom-field mapping in BambooHR** NEW 45

Adds custom-field mapping support for Pathify in BambooHR, including the 'Division' field.

– Names integration and field but no mapping mechanism detail

1Password SaaS Manager #1358 (2026-08-20)

04 **API key editing from AI Spend dashboard** IMPROVED 45

Supports direct editing of API key details from the AI Spend and Consumption dashboard.

– Names the dashboard as a clear UI starting point

1Password SaaS Manager #1358 (2026-08-20)

05 **Clearer OpenAI Platform reconnect errors** IMPROVED 45

Adds clearer reconnect errors in OpenAI Platform when an administrator key belongs to a personal organization rather than an enterprise organization.

– Describes the exact error condition but not the fix

1Password SaaS Manager #1358 (2026-08-20)

06 **WPS Office provisioning improvements** IMPROVED 45

WPS Office provisioning now sends an invitation after user creation and handles unsupported username characters.

— States two concrete behaviour changes without full mechanism

1Password SaaS Manager #1358 (2026-08-20)

07 **Custom person fields as workflow triggers** NEW 35

Enables custom person fields as workflow triggers, expanding automation options based on people data.

— General capability with no named fields or config path

1Password SaaS Manager #1358 (2026-08-20)

WAS THIS USEFUL? 👍 👎

SailPoint

1 RELEASE · 2026-08-19 BLOG ↗

SailPoint is an identity governance and access management platform that automates user access provisioning, certification, and compliance across enterprise systems.

> SailPoint's MySailPoint Home gets admin-controlled default layouts, pre-built dashboard templates including an Admin Overview equivalent, resizable widgets, and a user notification when defaults change.

└──▷ WHAT SHIPPED · 5 FEATURES most completely described first ? what's the number?

01 **Managed Defaults for Home layout** NEW 81

Admins can draft and publish a global default Home layout (action tiles and widgets) that applies tenant-wide, overriding users' previous individual customizations, via `Dashboard Manager > Templates > Home Page Templates`. Once published, the default appears under `Managed Dashboards > Default Home Pages` where it can be further edited or deleted; deleting it reverts users to the SailPoint baseline layout.

Set an org-wide Home baseline so all users start from an approved layout when they first log in.

📍 In the Dashboard Manager, go to Templates › Home Page Templates. Select 'Home Page', click 'Create Dashboard' to preview the default layout. Remove unwanted tiles or widgets from the preview, then click 'Edit' to add items. Click 'Save' and confirm to apply the Managed Default immediately across the tenant. The saved default then appears under Managed Dashboards › Default Home Pages for future edits.

— Exact UI navigation and behavior given, though no API/config key.

Enhancement: MySailPoint Managed Default…

02 **Admin Overview dashboard template** NEW 77

A new 'Admin Overview' dashboard template recreates the classic Admin Overview page's capabilities inside Custom Dashboards and is available by default to all administrators regardless of license. It's generated via `Dashboard Manager > Templates > Home Page Templates`, selecting 'Admin Overview' and clicking 'Create Dashboard' to produce an editable copy.

Give your admin team an Admin Overview dashboard so they are ready before the classic Admin Overview page is deprecated.

📍 In the Dashboard Manager, go to Templates › Home Page Templates. Select the 'Admin Overview' template and click 'Create Dashboard' to generate a copy.

> Customize as needed and save — the dashboard is available to all administrators regardless of license.

— Clear scope, license note, and exact creation steps.

Enhancement: MySailPoint Managed Default…

---

03 **Multi-size widgets** NEW 60

Widgets built by SailPoint product teams now ship in three sizes — Small (three per row), Medium (two per row, the current default), or Large (one per row). Size is fixed at widget creation and is not configurable by admins.

— Concrete sizing behavior but nothing for a reader to configure.

Enhancement: MySailPoint Managed Default…

THINNER COVERAGE BELOW

04 **Pre-built Dashboard Templates** NEW 46

Ready-made, copyable dashboards covering a persona, industry, or information type let admins start from a pre-built layout instead of a blank canvas, accessed via `Dashboard Manager > Templates`.

— Names the UI area but no concrete template list or mechanism.

Enhancement: MySailPoint Managed Default…

---

05 **Notification on Managed Default changes** NEW 33

Users receive an in-app notification on their first Home visit after an admin publishes a Managed Default change, alerting them that the layout was updated and that prior personalizations may need to be re-applied.

— Describes trigger and effect but no configurable surface.

Enhancement: MySailPoint Managed Default…

└──▷ **ALSO FROM THESE RELEASES**

WAS THIS USEFUL? 👍 👎

GOVERNANCE, RISK & COMPLIANCE

◆ Integrated & IT Risk Management

CISO Assistant

1 RELEASE · 2026-08-20 NOTES ↗

CISO Assistant is a one-stop-shop GRC platform for Risk Management, AppSec, Compliance & Audit, TPRM, BIA, Privacy, and Reporting. It supports 150+ global frameworks with automatic control mapping, including ISO 27001, NIST CSF, SOC 2, CIS, PCI DSS, NIS2, DORA, GDPR, HIPAA, CMMC, and more.

> CISO Assistant's v3.21.2 release adds a new privacy framework to its library, lets assessors manually override computed scores, and gives administrators finer control over outgoing notifications.

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

01 **Manual override of question-driven scores** NEW 40

Assessors can now manually override scores that are computed from question answers, allowing adjustment of computed scores without being locked to the automated answer-driven result.

— Describes behaviour but no UI path or config detail v3.21.2

02 **ISO 27701-2025 framework added to library** NEW 40

Adds the ISO 27701-2025 framework outline to the framework library, enabling privacy information management assessments against the updated standard.

— Names the specific standard but no usage steps v3.21.2

03 **Per-template email toggle in mailing system** IMPROVED 35

Administrators can now disable individual outgoing emails on a per-template basis within the mailing system, giving fine-grained control over which notifications are sent.

— States capability but no exact setting or config key named v3.21.2

WAS THIS USEFUL? 👍 👎

GOVERN

◆ AI/LLM Security

NVIDIA OpenShell ⓘ 1 RELEASE · 2026-08-20 NOTES ↗

OpenShell is the safe, private runtime for autonomous AI agents.

> OpenShell v0.0.110 adds headless OIDC login support, non-root sandbox identities, and persistent credential refresh for providers.

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

01 **OIDC device authorization for headless login** NEW 45

OpenShell now supports the OIDC device authorization grant flow for headless (browserless) login, enabling authentication in CI/CD pipelines and other non-interactive environments.

— Names the OIDC grant flow but no exact command or flag v0.0.110

02 **Persistent credential refresh in providers** IMPROVED 45

Credential drivers now store refresh credentials so providers can maintain long-lived credential sessions without requiring re-authentication.

— Explains mechanism but no named driver, key or command v0.0.110

03 **Non-root identities in sandboxes** NEW 30

Sandbox environments can now run under non-root identities, expanding the range of workloads and privilege models the sandbox can support.

— States the capability but no config or setup detail v0.0.110

WAS THIS USEFUL? 👍 👎

PLATFORMS & UTILITIES

◆ General Utilities & Libraries

GitHub CLI ⓘ 1 RELEASE · 2026-08-20 NOTES ↗

GitHub's official command line tool

> gh v2.98.0 adds worktree-based PR checkout, semantic and hybrid issue search, and a new environment variable for extension authors.

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

01 Worktree checkout for pull requests NEW 75

Adds the `--worktree PATH` flag to `gh pr checkout` to check out a pull request directly into a git worktree, letting you review a PR without disturbing your current branch.

Check out a PR into an isolated git worktree to review it without disturbing your current branch.

```
$ gh pr checkout 12 --worktree ../wt-feature
```

— Named flag with runnable example, mechanism clear. v2.98.0

02 Semantic and hybrid issue search NEW 75

Adds a `--search-type` flag to `gh search issues` supporting `semantic` and `hybrid` search modes, for finding issues by intent rather than exact keyword match.

Run a semantic or hybrid search across GitHub issues when keyword search misses intent-based matches.

```
$ gh search issues --search-type semantic 'authentication token expiry'
```

— Named flag and values with runnable example command. v2.98.0

THINNER COVERAGE BELOW

03 GH_EXTENSION environment variable for extensions NEW 55

`gh` now sets the `GH_EXTENSION=1` environment variable when it invokes an extension, allowing the extension code to detect that it was launched by `gh`.

— Named env var but no usage example given. v2.98.0

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · August 21, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe