THE CYBER TOOLCHAIN

NO. 029

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED JULY 29, 2026 · EVERY DAY

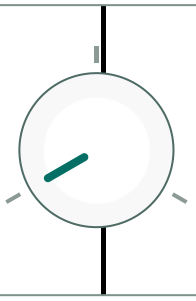
The daily firehose — everything the toolchain shipped today, already filtered.

▸ // HOW THIS ISSUE IS MADE SHOW

VIEW

ISSUE VIEW

scroll



SCROLL | EXPAND IN PLACE | PREVIEW PANE

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 37 tools

APPLICATION SECURITY

vim ? help

◆ SAST / SCA / Code Security

Promptfoo

Feedback ⓘ snapshot-20260729 NOTES ↗

Promptfoo is an open-source tool for testing, evaluating, and red-teaming LLM applications to detect vulnerabilities, improve reliability, and compare model outputs.

└──▷ TRY IT

View Promptfoo log output directly from the CLI for debugging provider or scan issues.

```
$ promptfoo logs
```

Generate a red team scan with a description and cap test cases per strategy, targeting a telecom AI system.

```
$ promptfoo redteam generate -d "Telecom voice agent test" --plugins telecom --config redteam.yaml
```

Adds fork PR support for code scanning pull requests.

Adds comment-triggered scans to initiate code scans via PR comments.

Adds Telecom red team plugins for industry-specific testing of telecommunications AI systems.

Red team scans now support multiple input variables for testing systems with complex input structures.

Propagates `-j` flag to Python worker pools for improved Python concurrency.

WAS THIS USEFUL? 👍 👎

REVERSE ENGINEERING, MALWARE & FORENSICS

◆ Digital Forensics & Incident Response

Mobile Verification Toolkit

Feedback ⓘ v2026.7.29

NOTES ↗ CODE ↗

MVT (Mobile Verification Toolkit) helps with conducting forensics of mobile devices in order to find signs of a potential compromise.

MVT gains shell completion, custom module loading, iOS sysdiagnose checking, Safari profile scanning, and parallelized URL checks.

└──▷ GET THIS VERSION ▾

```
$ git clone --branch v2026.7.29 https://github.com/mvt-project/mvt.git
# already have the repo? check out this version:
$ git checkout v2026.7.29
```

└──▷ TRY IT

Install shell completion for your shell so mvt-ios and mvt-android arguments tab-complete in your terminal.

```
$ mvt-ios completion bash --install
mvt-android completion zsh --install
```

Run an AndroidQF check with a custom detection module to extend MVT's analysis beyond built-in modules.

```
$ mvt-android check-androidqf --load-module
/path/to/my_custom_module.py <target>
```

Adds shell completion command for Bash, Zsh, and Fish via `mvt-ios completion` and `mvt-android completion`.

Supports loading custom Python analysis modules with `--load-module PATH` or the `MVT_CUSTOM_MODULES` environment variable.

Adds iOS sysdiagnose checking support.

Scans Safari profile databases for browsing history and browser state.

Parallelizes URL indicator checks for faster IOC scanning.

+4 more

WAS THIS USEFUL? 👍 👎

NETWORK SECURITY

◆ Firewalls & Network Defense

Rspamd

Feedback ⓘ 4.1.4 NOTES ↗

Rapid spam filtering system.

Rspamd 4.1.4 grants read-only WebUI users access to the Selectors tab and Errors history.

└──▷ GET THIS VERSION ▾

```
$ git clone --branch 4.1.4 https://github.com/rspamd/rspamd.git
# already have the repo? check out this version:
$ git checkout 4.1.4
```

└──▷ BREAKING ON UPGRADE

! Rspamd now refuses to link against a static-only jemalloc; builds configured with a static-only jemalloc will fail to start.

WAS THIS USEFUL? 👍 👎

Sublime Security

Feedback ⓘ

Platform v1.87.1 (Customer Account Access) (2026-07-28) · 2 RELEASES · 2026-07-28

BLOG ↗ · LATEST · STABLE

Sublime Security is an AI-powered email security platform that detects and remediates advanced threats like phishing and business email compromise.

Sublime adds Customer Account Access controls so admins can govern, audit, and time-limit support sessions in their tenant.

└──▷ HOW TO FIND IT

Review the audit log of all Sublime support sessions in your tenant to verify what was accessed and when.

> 📍 In the Sublime console, navigate to Settings › Customer Account Access to view and export the session audit log.

New single admin setting to enable or disable Sublime support access to a customer environment at any time.

Every support session is written to an audit log that admins can view and export for full accountability.

Live banner displayed to Sublime employees working inside a customer tenant, showing the account, role, and active session.

Support sessions auto-expire with a renewal prompt at 10 minutes, limiting unattended access.

▾ 1 more release in this issue · 2026-07-28

> Platform v1.87 (Advanced Graymail Protection - GA) (2026-07-28) · BLOG ↗
>
> STABLE
>
> Sublime Security's Advanced Graymail Protection is now GA, with automated remediation, fuzzy detection, and per-user preference learning.
>
> .
>
> └──▷ HOW TO FIND IT
>
> Enable user preference learning so Sublime automatically tailors graymail routing per sender based on individual user behavior.
>
> > 📍 In the console, go to Admin → Account and enable Graymail User Preferences.
>
> Adds Advanced Graymail Protection (GA) to identify and manage marketing emails,

newsletters, and subscription content across Microsoft 365 and Google Workspace.

New Remediate graymail flagged messages Automation routes detected graymail to Promotions automatically.

New Rule Fuzzy Attack Score: Advanced Graymail Detection extends graymail detection coverage, designed to pair with the included Automation.

New Graymail User Preferences feature (Admin → Account) learns from users moving messages into or out of Promotions or Junk/Spam and applies sender-level preferences to future messages.

WAS THIS USEFUL? 👍 👎

Fastly

Feedback ⓘ Fastly DNS (2026-07-28) BLOG ↗

Fastly is a cloud edge platform that accelerates, secures, and delivers websites, apps, and APIs by caching content closer to users globally.

Fastly launches authoritative DNS service backed by its global edge network.

WAS THIS USEFUL? 👍 👎

CLOUD & CONTAINER SECURITY

◆ Runtime Security

NoLabs nono

Feedback ⓘ v0.70.0 NOTES ↗ CODE ↗

Sandbox any AI agent in seconds - zero setup, zero latency.

nono v0.70.0 adds SPIFFE/SPIRE workload identity, per-route rate limiting, Vault OIDC mediation, JWT-shaped capture nonces, and profile-declared no_proxy bypass.

└──▷ GET THIS VERSION ▾

```
$ git clone --branch v0.70.0 https://github.com/nolabs-ai/nono.git
# already have the repo? check out this version:
$ git checkout v0.70.0
```

Adds SPIFFE/SPIRE workload identity authentication for upstream proxy routes, enabling zero-trust service-to-service auth without static credentials.

Adds per-route request rate limiting via RouteRateLimiter, letting profiles cap how many requests a sandboxed tool can make to a given upstream.

Adds support for mediating `vault login -method=oidc`, including a custom inject header and per-command `open_port` to handle the OIDC browser callback.

Adds a JWT-shaped nonce option (`CapturedNonceShape::Jwt`) for capture intercepts, producing a `<header>.<payload>.nono_<64hex>` token for consumers that validate token structure before use.

Adds profile-declared `no_proxy` bypass support, allowing profiles to specify hosts that skip the nono proxy.

+1 more

WAS THIS USEFUL? 👍 👎

Wiz Defend

Feedback ⓘ changelog · Jul 29, 2026 BLOG ↗

Wiz Defend is a cloud detection and response platform that identifies, investigates, and remediates real-time threats across cloud environments.

Wiz Defend GA's Red Agent AI pentester with Web API Crawler, logic-driven API DAST, and Secrets Blast Radius modules.

Red Agent is now generally available (GA): a continuous, autonomous AI pentester that reasons through business logic to uncover unknown vulnerabilities across custom-built software, vibe-coded applications, and APIs.

New Web API Crawler module: uses client-side code analysis to map API endpoints, extract and analyze API specifications, and surface hidden or forgotten shadow APIs.

New API DAST Attacker module: continuously finds and validates logic-driven exploitable risks — including OWASP API Top 10 flaws, authorization bypasses, and logic flaws — adapting its strategy in real time and delivering proofs of execution with reproduction steps.

New Secrets Blast Radius module: validates secrets exposed in public websites, APIs, and code repositories by executing safe checks against third-party SaaS provider APIs to confirm exploitability and determine the precise scope of permissions held.

Red Agent automatically ingests context from Wiz sources — API schemas, cloud resources, Runtime Sensor, code repositories, and network layers — without manual setup.

+2 more

WAS THIS USEFUL? 👍 👎

◆ Container & Image Security

Anchore syft

Feedback ⓘ v1.50.0 NOTES ↗

CLI tool and library for generating a Software Bill of Materials from container images and filesystems

Syft v1.50.0 adds a Bun binary classifier for detecting the Bun JavaScript runtime in SBOMs.

└──▷ GET THIS VERSION ▾

```
$ git clone --branch v1.50.0 https://github.com/anchore/syft.git
# already have the repo? check out this version:
$ git checkout v1.50.0
```

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ Endpoint Security (EDR/XDR)

Iru

Feedback ⓘ Managed OS for Apple: New embedded delay option NOTES ↗

Manage devices and everything they touch. See how security, IT, and compliance get easier when unified around devices with Iru.

Managed OS for Apple gains an embedded delay option (up to 90 days) for Rolling Enforcement target version declarations.

└──▷ HOW TO FIND IT

Slow-roll a new macOS version to your fleet by staggering when devices receive the target version declaration — useful before broad deployment.

> 📍 In the Iru console, open your Managed OS for Apple configuration, enable Rolling Enforcement, and set the embedded delay (up to 90 days) to control when a new target version declaration is sent to devices.

Adds an automatic delay option (up to 90 days) within Rolling Enforcement for Managed OS for Apple, preventing Iru from sending a new target version declaration to devices until the delay elapses.

Enables combining the new embedded delay with Apple software update deferrals configured in a Software Update Library Item for layered update control.

WAS THIS USEFUL? 👍 👎

Trend Vision One

Feedback ⓘ

Zero Trust Secure Access supports masking sensitive data in DLP and AI detection logs (2

BLOG ↗

Trend Vision One is a unified cybersecurity platform that integrates extended detection and response (XDR) across endpoints, networks, email, and cloud environments.

Trend Vision One Zero Trust Secure Access adds masked/unmasked display mode for sensitive data in DLP and AI detection logs.

└──▷ **HOW TO FIND IT**

Control whether sensitive matched content is visible to reviewers of DLP or AI detection events — useful for restricting raw data exposure to only authorized analysts.

> 📍 In the console, go to Zero Trust Secure Access → Internet Access and AI Secure Access Configuration → Global Settings → DLP/AI detection logs, then set the display mode to Masked or Unmasked.

Adds configurable masking for matched content in DLP and AI content detection logs, letting administrators control whether sensitive data (up to 100 bytes) is hidden or visible when reviewing Internet Access and AI Secure Access detection events.

WAS THIS USEFUL? 👍 👎

◆ Detection Engineering

Splunk Security Content

Feedback ⓘ v6.3.0 NOTES ↗

Splunk Security Content

Splunk Security Content v6.3.0 adds a Starland RAT campaign story, 4 new Linux/Windows analytics, and expands 67 existing detections.

└──▷ GET THIS VERSION ▾

```
$ git clone --branch v6.3.0
https://github.com/splunk/security_content.git
# already have the repo? check out this version:
$ git checkout v6.3.0
```

New Analytic Story: Starland RAT Campaign (UAT-11795) — tags analytics across PowerShell abuse, ClickFix social engineering, in-memory execution, credential theft, and Telegram-based C2 for end-to-end campaign visibility.

New detection: Linux AppArmor Bypass Via Aaexec — covers attempts to evade AppArmor confinement using aaexec.

New detection: Linux Auditd Possible Setuid Execve Privesc — identifies local privilege escalation attempts via setuid execve patterns on Linux.

New detection: Linux Pedit Offset Out Of Bounds — detects kernel-level exploitation technique targeting pedit.

New detection: Windows AppCertDLL Modification Via Registry — covers persistence via AppCertDLL registry manipulation.

+1 more

WAS THIS USEFUL? 👍 👎

◆ SIEM

Google SecOps

Feedback ⓘ July 29, 2026 (2026-07-29) BLOG ↗

Google SecOps is a cloud-based security operations platform that helps organizations detect, investigate, and respond to cybersecurity threats using AI-powered analytics and threat intelligence.

Google SecOps lets you inspect prebuilt parser preview content even when a custom parser is active for the same log type.

WAS THIS USEFUL? 👍 👎

Elastic Security Labs

Feedback ⓘ

Stop rewriting detection rules by hand: automatic Sentinel-to-Elastic migration is here

BLOG ↗

Elastic Security Labs publishes threat research, vulnerability analysis, and security insights to help organizations understand emerging cyber threats.

Elastic Security 9.5 adds automatic Microsoft Sentinel detection rule migration, translating Scheduled and NRT analytics rules to Elastic via LLM.

.
.
.

└──▷ **HOW TO FIND IT**

Start a Sentinel-to-Elastic rule migration to automatically translate your detection rules and plan data onboarding around what those rules actually require.

> 📍 In Elastic Security, go to Security Launchpad › Manage Automatic Migrations, select your AI provider, expand 'Migrate your existing SIEM rules to Elastic', and choose Microsoft Sentinel from the top-right drop-down. Follow the prompts to export rules from your Sentinel workspace and upload them.

Adds automatic migration of Microsoft Sentinel Scheduled and Near Real Time (NRT) analytics rules into Elastic Security using an LLM of your choice.

Supports Watchlists-to-ES|QL Lookups conversion and Sentinel severity mapping during rule migration.

Identifies required Elastic integrations from exported Sentinel rules, enabling a `rules-first` migration path to plan data onboarding before moving logs.

Surfaces per-rule translation status (Installed, Translated, Partially translated, Not translated, Failed) in the Manage Automatic Migrations UI.

Available in Tech Preview in Elastic Security 9.5 across multiple cloud providers and regions.

WAS THIS USEFUL? 👍 👎

◆ Threat Intelligence

OpenCTI

Feedback ⓘ 7.260728.0 NOTES ↗

Open Cyber Threat Intelligence Platform

OpenCTI 7.260728.0 ships a full draft approval workflow engine, XTM Hub integration, TAXII error visibility, OAuth SMTP dynamic tokens, and audit log session tracking.

└──▷ GET THIS VERSION ▾

```
$ git clone --branch 7.260728.0 https://github.com/OpenCTI-Platform/opencti.git
# already have the repo? check out this version:
$ git checkout 7.260728.0
```

└──▷ HOW TO FIND IT

Enable XTM Hub connection so integrations can be pushed directly from the Hub into your OpenCTI instance.

📍 In the console, go to Settings › Filigran Experience and click the XTM Hub card to connect your OpenCTI instance to the Hub.

Introduces a complete draft approval workflow engine: define, visualize, and apply workflows via a ReactFlow graph UI, with filter-based conditions, async task actions, schema validation on save, auto-save/publish, and synchronous/asynchronous transition reactions.

Adds draft workspace metadata (participants, assignees, description, creator) and the ability to filter, edit, and visualize draft details directly in the drafts list.

Connects OpenCTI to XTM Hub, enabling integrations to be discovered and connected directly from the Hub into OpenCTI.

Reworks the integrations UI with a pipeline ribbon, aligned lines view, config import, facets, sorting, and next-run visibility.

Reworks the Filigran Experience settings screen with hero-style Enterprise Edition and XTM Hub cards.

+9 more

WAS THIS USEFUL? 👍 👎

◆ Security Data Pipeline

Cribl

Feedback ⓘ

Why full-text search matters for modern log analytics (2026-07-28) BLOG ↗

Cribl is an observability pipeline platform that helps organizations collect, process, route, and transform machine data from any source to any destination.

Cribl Search 4.19 makes full-text inverted-index search on `_raw` the default for Lakehouse engines, with backfill for existing engines.

└──▷ TRY IT

During incident response, search a dataset for a raw token (e.g., an error code or hostname fragment) across the full event message without specifying a field.

```
$ dataset="flowlogs" 123456 | ...
```

Use the `where … has` form to explicitly invoke the full-text index when the token search follows a pipeline operator.

```
$ dataset="flowlogs" | where _raw has 123456 | ...
```

Enables full-text search (FTS) via an inverted index on `_raw` as the default experience in Cribl Search's Lakehouse Engine, allowing token-based searches without targeting a specific field.

Delivers 150×–350× query acceleration on token-based 'needle in the haystack' searches (tested on 1 billion row datasets) by skipping irrelevant storage blocks.

Supports FTS activation via the simple string predicate in the leftmost implied cribl operator, or via the `where` operator with the `has` string operator.

WAS THIS USEFUL? 👍 👎

EXPOSURE & VULNERABILITY MANAGEMENT

◆ Vulnerability Management

Future Architect Vuls

Feedback ⓘ v0.40.0-rc.1 NOTES ↗

CODE ↗ PRE-RELEASE

Agent-less vulnerability scanner for Linux, FreeBSD, Container, WordPress, Programming language libraries, Network devices

Vuls v0.40.0-rc.1 migrates NVD, Cisco, JVN, VulnCheck, Fortinet, Palo Alto, and CTI detection to the vuls2 engine, adds ENISA EUVD and Seal Security coverage.

└──▷ GET THIS VERSION ▾

```
$ git clone --branch v0.40.0-rc.1 https://github.com/future-architect/vuls.git
# already have the repo? check out this version:
$ git checkout v0.40.0-rc.1
```

Routes NVD CPE detection and enrichment through the vuls2 engine with cpematch-expanded criteria, replacing go-cve-dictionary's version-range-only matching.

Routes Cisco, Fortinet, Palo Alto, VulnCheck, and JVN data sources through vuls2 for detection and enrichment.

Adds ENISA EUVD (European Union Vulnerability Database) as a vuls2 enrich data source.

Replaces go-cti with vuls2 attack/CAPEC/CWE datasources; adds ScanResult-level `CWEDict`, `CAPECDict`, and `ATTACKDict` catalog maps and a per-VulnInfo `CTIs` reference list.

Enriches MITRE CVE v5 data via the vuls2 pipeline.

+4 more

└──▷ BREAKING ON UPGRADE

! The `[cti]` config section is removed; CTI data is now sourced from vuls2 rather than go-cti.

! The per-VulnInfo field previously named `Ctis` is renamed to `CTIs`; consumers of scan result JSON will need to update field references.

! EUVD content is no longer sourced from go-cve-dictionary; it is now provided solely through the vuls2 enrich path.

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Secure Access (VPN / SASE / ZTNA)

Progress ShareFile

Feedback ⓘ snapshot-20260729 NOTES ↗

Progress ShareFile is a cloud-based file sharing and storage platform enabling businesses to securely send, receive, and manage documents and client communications.

ShareFile adds Tasks workspace, AI document validation, Security Insights dashboard, session management, and a wave of new integrations across Mac, Windows, and Outlook.

Adds export of Request Lists to Excel (.xlsx) or CSV (.csv) for offline use or custom analysis, accessible from the three-dot menu on the Request List page.

Adds Projects, Client Hub, and Solutions access in ShareFile for Mac for all Premium plan users.

Adds Folders in ShareFile for Clients app, enabling browse, view, download, upload, and delete of shared folders from a service provider.

Adds Projects, Client Hub & Solutions access in ShareFile for Windows for all Premium plan users (version 26.03.12.0 and later).

Adds ShareFile one-time code authentication for client users, configurable by administrators.

+5 more

└──▷ **BREAKING ON UPGRADE**

- ! Upgrading to ShareFile for Mac 26.04.20 requires all users to re-authenticate.
- ! Upgrading to ShareFile for Windows 26.3.12.0 requires users to re-authenticate.
- ! ShareFile for Windows 25.6.5.0 is signed with Progress Software Corporation's digital certificate; environments that restrict software by publisher may block this update until Progress Software Corporation is added to the trusted publishers list.

WAS THIS USEFUL? 👍 👎

Cisco Duo Desktop

Feedback ⓘ snapshot-20260729 NOTES ↗

Cisco Duo Desktop is an endpoint security application that verifies device health and security posture before granting users access to protected corporate resources.

Duo Desktop adds Microsoft Defender for Endpoint detection on Linux, Ubuntu 26.04 LTS support, and user-level preference persistence on macOS.

Adds detection for Microsoft Defender for Endpoint on Linux (v4.6.0).

Adds support for Ubuntu 26.04 LTS on Linux (v4.6.0).

Adds fallback to `/etc`/machine-id for Trusted Endpoints identifier when the primary identifier is unavailable on Linux (v4.7.0).

Removes the requirement for the dmidecode utility on Linux (v4.7.0).

User-level preferences now persist across uninstall on macOS (Public Beta v7.19.3.0).

└─▷ **BREAKING ON UPGRADE**

! Support for Ubuntu 23.04 and 20.04 LTS has been dropped in Linux v4.6.0.

WAS THIS USEFUL? 👍 👎

DNSFilter Feedback ⓘ

07/29 July 29 – Windows Roaming Client v3.6.10 Beta (2026-07-29) BLOG ↗

PRE-RELEASE

DNSFilter is a cloud-based DNS security platform that blocks malicious websites, filters unwanted content, and protects networks from cyber threats in real time.

DNSFilter Windows Roaming Client v3.6.10 Beta adds DNS PreCheck v2 with hijack-resistant policy enforcement and automatic tray process recovery.

└──▷ HOW TO FIND IT

Confirm DNS PreCheck v2 is active for your organization after it has been enabled — the system tray will display `DNS PreCheck v2` instead of the previous label.

> 📍 In the DNSFilter dashboard, go to Deployments → Roaming Clients → Beta Channel, download and install the v3.6.10 beta installer, then check the system tray on enrolled Windows endpoints for the `DNS PreCheck v2` indicator once your organization's rollout is enabled.

Adds DNS PreCheck v2, which maintains policy enforcement on networks that hijack or redirect DNS traffic, closing a gap where certain network conditions could allow content through that should have been blocked.

Adds automatic tray process recovery so the system tray process self-restarts if it stops unexpectedly, keeping tray status and controls available without manual intervention.

WAS THIS USEFUL? 👍 👎

Termius

Feedback ⓘ 9.42.2 (2026-07-29) BLOG ↗

Termius is a secure SSH client and terminal emulator for managing remote servers across multiple devices with encrypted credential storage.

Termius 9.42.2 adds bulk host management via context menu and less disruptive app updates.

Open selected hosts in a new workspace or add them to an existing one directly from the Hosts screen context menu.

└─▷ **BREAKING ON UPGRADE**

! MultiKey authentication will no longer be available after October 15, 2026 — migrate to SSH ID or another authentication method before that date.

WAS THIS USEFUL? 👍 👎

◆ **Identity & Access Management**

Nudge Security

Feedback ⓘ Enforce SSO login for Nudge Security

NOTES ↗

Nudge Security discovers and secures all SaaS apps used across an organization, helping IT teams manage shadow IT and enforce security policies through automated nudges.

Nudge Security now lets admins enforce SSO-only login, disabling Google/Microsoft sign-in and routing all auth through your IdP.

└─▷ **HOW TO FIND IT**

Enforce SSO-only login for your organization to ensure all users authenticate via your IdP and inherit its MFA and deprovisioning policies.

📍 In the console, go to Settings › Organization and enable login restrictions.

Adds SSO login enforcement that disables alternative sign-in methods (Sign in with Google, Sign in with Microsoft) org-wide, routing all logins through your configured IdP (e.g., Okta) to inherit its MFA, conditional access, and deprovisioning controls.

WAS THIS USEFUL? 👍 👎

1Password Feedback ⓘ

1Password for Android beta 8.12.32-26 (2026-07-29)

10 RELEASES · 2026-07-28 → 2026-07-29 BLOG ↗ LATEST STABLE

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

1Password for Android now saves logins on multi-screen username/password flows.

Offers to save logins when a site splits username and password entry across separate screens.

▾ 9 more releases in this issue · 2026-07-28 → 2026-07-29

> 1Password for Linux beta 8.12.32-26 (2026-07-29) BLOG ↗ STABLE
>
> 1Password for Linux now respects your system date format for item date fields.

> 1Password for Mac beta 8.12.32-26 (2026-07-29) BLOG ↗ STABLE
>
> 1Password for Mac beta adds Claude AI agent sign-in support via MCP, letting Claude fill logins with user approval.
>
> Adds 1Password for Claude integration: Claude can sign in to websites on your behalf, with per-request approval before credentials are filled — credentials are never shared with Claude.
>
> Shows a clear error message when attempting to move or duplicate an item with a custom icon while file storage is disabled by an admin policy.
>
> Item date fields now respect the date format chosen in system settings, or the language set in 1Password when it differs from the system language.

> 1Password for Windows beta 8.12.32-26 (2026-07-29) BLOG ↗ STABLE
>
> Auto-Type now prompts before filling untrusted apps, and window picker gains app icons for easier targeting.
>
> Auto-Type now requests confirmation before filling credentials into unsigned or untrusted apps, replacing silent failure.
>
> The `Type in window` window selection menu now displays an app icon alongside each open window for easier identification.
>
> Item date fields now respect the date format configured in system settings, or the language set in 1Password when it differs from the system language.

> 1Password for iOS beta 8.12.32-26 (2026-07-29) BLOG ↗ STABLE

1Password iOS beta adds cellular-data warnings for large file uploads and smarter multi-account Home screen switching.

Warns users before uploading large files over cellular or metered connections when drag-and-dropping into a Document item.

Home screen automatically switches to All Accounts when a second account is unlocked, and returns to single-account view when only one account is active.

Updated buttons throughout the app to use the iOS 26 Liquid Glass style.

Diagnostic Report sending is now split into separate `Email Diagnostic Report to Support` and `Export Diagnostic Report file` actions.

`1Password in the browser 8.12.32-26 (2026-07-29)` **BLOG ↗** **STABLE**

1Password adds Claude AI agent sign-in support, Secret Key paste blocking, and reorganized phishing/security settings.

└──▷ **HOW TO FIND IT**

Control whether 1Password prompts to save credentials captured by shell plugins like the 1Password CLI.

> 📍 In the 1Password browser extension, go to Settings › Autofill & save and toggle the option to offer saving API credentials for shell plugins.

Adds 1Password for Claude integration, letting Claude sign in to websites on your behalf — filling logins and one-time codes after your explicit approval, without sharing credentials with Claude.

New setting in Settings > Autofill & save lets you choose whether 1Password offers to save API credentials for shell plugins.

Shell plugin credential saves now use the same autosave notification as standard logins for a consistent experience.

Phishing warning settings relocated to Settings > Security & privacy > Phishing prevention, with a new separate toggle for the popup phishing warning.

Selecting `Hide on this page` now suppresses all 1Password notifications on that page (except Device Trust notifications).

> └──▷ **BREAKING ON UPGRADE**
>
> ! Phishing warning settings have moved from their previous location to Settings > Security & privacy > Phishing prevention; any workflow or documentation referencing the old location will need updating.

`1Password for Linux 8.12.30 (2026-07-28)` **BLOG ↗** **STABLE**

1Password for Linux adds a local MCP server so AI assistants can access Developer tools directly from the app.

New local MCP server in the Developer tab lets AI assistants access 1Password Developer tools.

Watchtower descriptions now surface plaintext secrets scanning coverage, including .env files and SSH keys, on the Developer homepage and in Watchtower.

`1Password for Mac 8.12.30 (2026-07-28)` **BLOG ↗** STABLE

1Password for Mac adds a local MCP server for AI assistant access to Developer tools and expands Watchtower secret-scanning descriptions.

Adds a local MCP server launchable from the Developer tab, enabling AI assistants to access 1Password Developer tools.

Watchtower descriptions now surface plaintext secret scanning coverage, including .env files and SSH keys, on the Developer homepage and in Watchtower.

`1Password for Windows 8.12.30 (2026-07-28)` **BLOG ↗** STABLE

1Password for Windows adds a local MCP server so AI assistants can access Developer tools directly from the app.

Adds a local MCP server launchable from the Developer tab, enabling AI assistants to access 1Password Developer tools.

Watchtower descriptions now explicitly mention scanning for plaintext secrets, including .env files and SSH keys.

`1Password in the browser 8.12.30 (2026-07-28)` **BLOG ↗** STABLE

1Password in the browser adds toggleable extension diagnostic logging in Settings.

└──▷ HOW TO FIND IT

Enable diagnostic logging to capture extension activity for troubleshooting or sharing with 1Password Support.

📍 In the extension, go to Settings › Help › Share diagnostic logs with 1Password and toggle diagnostic logging on.

WAS THIS USEFUL? 👍 👎

Auth0 Feedback ⓘ

Dashboard Search for Organization members now in Beta! (2026-07-29)

3 RELEASES · 2026-07-29 BLOG ↗ LATEST STABLE

Auth0 is a cloud-based identity platform that provides authentication and authorization services, enabling developers to securely add login and access control to applications.

Auth0 Dashboard gains real-time search for Organization members by name, email, ID, and blocked status (Public Beta).

└──▷ **HOW TO FIND IT**

Quickly locate a specific organization member without scrolling through paginated lists.

> 📍 In the Dashboard, go to Organizations › [your organization] › Members, then use the search bar to enter a name, email address, or user ID. Use the `Blocked` filter to narrow results to blocked members only.

Search Organization members in real time by name, email, or ID directly from the Auth0 Dashboard — no more paginating through full member lists.

Filter Organization members by blocked status from the Dashboard member search interface.

▾ **2 more releases in this issue** · 2026-07-29

> Organization-Level Roles - Early Access (2026-07-29) BLOG ↗ STABLE
>
> Auth0 adds organization-scoped roles in Early Access, enabling per-org RBAC without tenant-wide role sharing or custom workarounds.
>
> Adds organization-scoped roles so each Auth0 Organization can have its own independent role definitions and permission assignments.
>
> Supports creating, updating, and deleting org-scoped roles via the Management API or Dashboard.
>
> Enables assigning org-scoped roles to users and enterprise groups within a specific organization.
>
> Supports pre-assigning an org-scoped role when sending a user invitation to an organization.

> Organization-to-Application Entitlement - Early Access (2026-07-29) BLOG ↗
>
> STABLE

> Auth0 adds native Organization-to-Application Entitlement, letting you restrict which apps org members can access without custom code.
>
> .
>
> Adds Organization-to-Application Entitlement (Early Access): natively enforce which applications members of an organization can access, with automatic denial on unauthorized login attempts — no Actions, metadata checks, or custom logic required.
>
> Supports per-org, opt-in enforcement so entitlements can be configured and tested before going live, with no risk of disrupting existing login flows.

WAS THIS USEFUL? 👍 👎

SailPoint

Feedback ⓘ

Enhancement: Smarter Output Handling for HTTP Request (POST) (2026-07-28)

BLOG ↗

SailPoint is an identity security platform that helps organizations manage and govern user access to applications, data, and systems across the enterprise.

SailPoint Workflows now auto-trims HTTP POST response payloads inside loops, matching existing GET behavior.

Extends automatic payload trimming to HTTP Request (POST) steps — loop inputs now retain only the fields referenced in downstream steps, reducing data stored and transferred per run.

Full POST response remains accessible during test/build mode so practitioners can inspect all fields while authoring workflows.

WAS THIS USEFUL? 👍 👎

Clerk Feedback ⓘ

Hosted authentication for Expo, iOS, and Android (2026-07-28) BLOG ↗

Clerk is a user authentication and identity management platform that provides developers with pre-built UI components, APIs, and SDKs for sign-up, sign-in, and user management.

Clerk now supports hosted authentication via Account Portal for Expo, iOS, and Android apps.

WAS THIS USEFUL? 👍 👎

◆ Data Security & DLP

Varonis

Feedback ⓘ Classify tools by capability

10 RELEASES · SEEN 2026-07-29 NOTES ↗ LATEST STABLE

Varonis is a data security platform that detects and stops insider threats, data breaches, and ransomware attacks across cloud and on-premises environments.

Varonis Atlas can now classify tools by functional capability for improved policy evaluation and MCP risk visibility.

▾ 9 more releases in this issue · seen 2026-07-29

> Connect GitHub using least-privilege access NOTES ↗ STABLE
>
> Varonis Atlas supports connecting GitHub via a read-only GitHub App for least-privilege repository discovery.

> Discover AI resources in TypeScript repositories NOTES ↗ STABLE
>
> Varonis Atlas now scans TypeScript repositories to discover and inventory AI resources and artifacts.

> Discover Salesforce Agentforce resources through Hosted Services NOTES ↗ STABLE
>
> Varonis Atlas now discovers Salesforce Agentforce AI agents and configurations via Hosted Services.

> Expanded support for monitoring and governing coding agents NOTES ↗ STABLE
>
> Varonis Atlas adds runtime monitoring and governance for Devin CLI, Devin Desktop, Google Antigravity, Kiro, and OpenAI Codex coding agents.
>
> Adds Atlas runtime monitoring and governance support for Devin CLI, Devin Desktop, Google Antigravity, Kiro, and OpenAI Codex coding agents.
>
> Enables logging, review, and evaluation of coding agent activity via Atlas runtime policies.

> Identify Agents, Tools, and MCPs faster NOTES ↗ STABLE
>
> Varonis Inventory adds dedicated views for AI agents, tools, and MCP resources.

> Ingest and monitor AWS Bedrock activity NOTES ↗ STABLE
>
> Varonis Atlas now ingests AWS Bedrock activity for AI usage visibility, investigation, and runtime policy enforcement.

Manage Claude-hosted agents in Atlas NOTES ↗ STABLE

Varonis Atlas now surfaces Claude Managed Agent as a supported hosted service resource for inventory and governance.

Sync Copilot and ChatGPT Enterprise activity with Varonis DSPM NOTES ↗

STABLE

Varonis DSPM now ingests Microsoft Copilot and ChatGPT Enterprise prompt activity for correlation with sensitive data context.

Syncs Microsoft Copilot prompt activity with Varonis DSPM to correlate AI interactions with sensitive data context and policy enforcement.

Syncs ChatGPT Enterprise prompt activity with Varonis DSPM to improve investigation workflows and sensitive data visibility.

Trace user intent and agent activity over time NOTES ↗ STABLE

Varonis AI Investigation Sessions gain an Intent Timeline for chronological tracing of user intent and agent activity.

Adds Intent Timeline to AI Investigation Sessions, giving investigators a chronological view of user intent, agent behavior, and tool activity throughout a session.

Enables tracing of activity leading up to and following a runtime policy trigger to understand causation in AI agent workflows.

WAS THIS USEFUL? 👍 👎

DigiCert CertCentral

Feedback ⓘ July 28, 2026 NOTES ↗

DigiCert CertCentral is a centralized platform for managing SSL/TLS certificates, automating issuance, renewal, and deployment across organizational infrastructure.

CertCentral adds DCV polling status to APIs, ACME URL delegation to Service Users, and API key ownership transfers.

└──▷ **TRY IT**

Check whether automatic DCV polling is still active for a domain, so you know if a manual validation check is needed.

```
$ curl -X GET
'https://www.digicert.com/services/v2/domain/<domain_id>' \
  -H 'X-DC-DEVKEY: <api_key>' \
  -H 'Content-Type: application/json'
# Look for dcv_polling_status and dcv_polling_last_checked in the
response
```

Transfer an ACME Directory URL to a Service User before offboarding an employee, so automations keep running without re-issuing credentials.

> 📍 In CertCentral, go to Automation › ACME Directory URLs. Find the URL, open its Actions menu, and select Update ACME Directory URL. In the Update ACME Directory URL restrictions window, use the User menu to select the target Service User, then select Update ACME Directory URL.

Transfer an API key to a Service User before deleting a user whose key is embedded in active integrations.

> 📍 In CertCentral, go to Automation › API Keys. Find the API key and select its link. In the Update API Key window, use the User menu to select the CertCentral user or Service User to transfer ownership to, then save.

Adds `dcv_polling_status` and `dcv_polling_last_checked` fields to the Domain info and Order validation status API endpoints, exposing whether automatic DCV polling is active and when it last ran.

Enables creating ACME Directory URLs on behalf of another CertCentral user, Service User, or new Service User — no longer limited to self-service only.

Enables transferring ACME Directory URL ownership to another CertCentral user or Service User, decoupling credentials from individual accounts.

Enables transferring API key ownership to another CertCentral user or Service User, allowing integrations to survive user departures without credential rotation.

WAS THIS USEFUL? 👍 👎

GOVERNANCE, RISK & COMPLIANCE

◆ Third-Party & Vendor Risk (TPRM)

Conveyor

Feedback ⓘ 📄 Download Signed NDAs Through the API

3 RELEASES · SEEN 2026-07-29 NOTES ↗ LATEST STABLE

Conveyor is a security tool that automates vendor security reviews by enabling companies to share and manage security documentation and questionnaire responses efficiently.

Conveyor adds a new API endpoint to download signed NDAs as PDFs with a temporary link.

└──▷ TRY IT

Pull a signed NDA PDF download link into your system after an authorization is completed — requires enabling the Signed Documents permission under Settings > Integrations > API Keys > Edit permissions first.

```
$ curl -X GET
'https://app.conveyor.com/api/v2/exchange/gate_document_signatures/<ga
te_document_signature_id>' \
  -H 'Authorization: Bearer <api_token>'
```

Enable the required API permission before making calls to the new endpoint.

📍 In the console, go to Settings › Integrations › API Keys › Edit permissions and enable Signed Documents.

▾ 2 more releases in this issue · seen 2026-07-29

🔍 Search Your Knowledge Library and See Your Trust Center Subscribers via API

NOTES ↗ STABLE

Conveyor adds Knowledge Library search and Trust Center subscriber visibility via two new API endpoints.

└──▷ TRY IT

Retrieve the full list of Trust Center subscribers to audit who will be notified when your subprocessor list changes.

```
$ curl -H "Authorization: Bearer <your_api_key>"
"https://app.conveyor.com/api/v2/vendor_subscriptions"
```

New `GET /api/v2/knowledge_base/search` endpoint enables keyword search across curated Q&As and past questionnaire answers, letting agents pull from

existing approved language.

New `GET /api/v2/vendor_subscriptions` endpoint exposes the full list of subscribers receiving Trust Center subprocessor change notifications.

Both endpoints are also available as MCP tools, allowing agents connected via the Conveyor AI Connector to call them directly.

🔐 Refreshed Login and Sign Up, Now with One-Click Access from Email NOTES ↗

STABLE

Conveyor adds one-click magic-link login, eliminating manual token copy-paste during onboarding.

Adds a one-click button in login token emails that opens Conveyor with the authentication code pre-filled, removing manual copy-paste.

Rebuilt login and sign-up pages now surface previously hard-to-find features such as configurable roles and the AI Connector.

WAS THIS USEFUL? 👍 👎

◆ Integrated & IT Risk Management

CISO Assistant

Feedback ⓘ v3.20.4 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 v3.20.4 adds full TPRM domain export/import, evidence on exceptions, batch asset BIA, AI file uploads, and posture management enhancements.

└──▷ GET THIS VERSION ▾

```
$ git clone --branch v3.20.4 https://github.com/intuitem/ciso-assistant-community.git
# already have the repo? check out this version:
$ git checkout v3.20.4
```

Includes the full Third-Party Risk Management (TPRM) ecosystem in domain export/import operations.

Enriches the ENISA Cyber Resilience Assessment framework with recommended controls.

Enables batch-adding assets to Business Impact Analyses (BIA).

Supports attaching evidence files directly to security exceptions.

Adds more capabilities to posture management.

+2 more

WAS THIS USEFUL? 👍 👎

BUILD

◆ AI Coding Agents

Kiro Feedback ⓘ

Editor Actions, Guided Hook Creation, and Code OSS Upgrade

2 RELEASES · SEEN 2026-07-29 NOTES ↗ LATEST STABLE

Kiro is an AI-powered IDE by AWS that uses "specs" to translate requirements into structured plans, then automatically generates and implements code.

Kiro adds editor context menu actions, guided hook creation, and Code OSS v1.108.2 upgrade with IDE language replies.

└──▷ HOW TO FIND IT

Quickly invoke Kiro assistance on a specific error or warning without leaving your editor.

> 📍 In the editor, hover over a red/yellow underline → click the lightbulb or press the quick fix shortcut → select `Ask Kiro to Fix`.

Adds a Kiro submenu to the editor context menu for quick access to Kiro actions directly from right-click.

Adds an `Ask Kiro to Fix` quick fix option surfaced inline on errors and warnings in the editor.

Upgrades the underlying IDE to Code OSS v1.108.2.

Kiro now replies in the user's configured IDE display language.

Chat history now persists across workspace folder changes.

▾ 1 more release in this issue · seen 2026-07-29

Spec Drafting and Plan Auto-Execution NOTES ↗ STABLE

Kiro adds guided spec creation and automatic plan execution after approval in Plan mode.

Adds a guided description step to `/spec new` so the agent uses your provided description as ground truth when drafting requirements, rather than inferring from the spec name alone.

Plan mode now automatically begins executing an approved plan immediately after approval, eliminating the manual mode-switch step.

WAS THIS USEFUL? 👍 👎

OpenAI Codex CLI

Feedback ⓘ rust-v0.147.0-alpha.1

2 RELEASES · 2026-07-29 NOTES ↗ CODE ↗ PRE-RELEASE

Lightweight coding agent that runs in your terminal

Codex CLI exec servers gain stdin-close exit control, plugin eligibility metadata, and MCP legacy-server fallback improvements.

└──▷ GET THIS VERSION ▾

```
$ git clone --branch rust-v0.147.0-alpha.1
https://github.com/openai/codex.git
# already have the repo? check out this version:
$ git checkout rust-v0.147.0-alpha.1
```

└──▷ TRY IT

Keep a remote exec server's lifetime tied to the spawning process — useful in CI or orchestration where you want the server to exit cleanly when the parent dies rather than becoming an orphan.

```
$ codex exec-server --remote --exit-on-stdin-close
```

Adds `--exit-on-stdin-close` flag (and `CODEX_EXEC_SERVER_EXIT_ON_STDIN_CLOSE` env var) to remote exec servers, enabling graceful shutdown with telemetry flush when the parent process closes stdin.

Exposes plugin eligibility metadata (`disabledReason` , `eligiblePlanTypes`) in app-server plugin summaries, surfacing plan-gating and admin-disabled status.

Adds `parent_turn_id` tracking across nested Codex agent spawns, delegated sessions, and follow-up tasks for improved request provenance.

▾ 1 more release in this issue · 2026-07-29

rust-v0.146.0 NOTES ↗ CODE ↗ LATEST STABLE

Codex CLI v0.146.0 adds named/pinned sessions, thread forking, Agent Plugins, WebSocket Code Mode, and standalone web search for custom providers.

└──▷ GET THIS VERSION ▾

```
$ git clone --branch rust-v0.146.0
https://github.com/openai/codex.git
# already have the repo? check out this version:
$ git checkout rust-v0.146.0
```

Name new sessions with `/new` or `/clear`, pin important threads, and switch between side conversations without closing them.

Fork threads with paginated history, including temporary forks that do not appear in thread listings.

Support Agent Plugins manifests, workspace plugin publishing, and additional plugin marketplaces for Amazon Bedrock and Claude Code.

Connect the app-server to remote Code Mode hosts over WebSocket.

Enable standalone web search for compatible custom model providers.

+1 more

WAS THIS USEFUL? 👍 👎

Cline

Feedback ⓘ v4.0.12 2 RELEASES · 2026-07-28 NOTES ↗ CODE ↗

LATEST STABLE

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

Cline v4.0.12 adds free model support with limit-reached error cards showing reset time.

└──▷ GET THIS VERSION ▾

```
$ git clone --branch v4.0.12 https://github.com/cline/cline.git
# already have the repo? check out this version:
$ git checkout v4.0.12
```

▾ 1 more release in this issue · 2026-07-28

sdk/sdk/v0.0.66 NOTES ↗ CODE ↗ STABLE

Cline SDK v0.0.66 adds free-tier models, persistent settings, connector session auto-reconnect, and broader provider coverage.

└──▷ GET THIS VERSION ▾

```
$ git clone --branch sdk/sdk/v0.0.66
https://github.com/cline/cline.git
# already have the repo? check out this version:
$ git checkout sdk/sdk/v0.0.66
```

Adds support for `cline-free` models, labeled `(free)` and priced at zero, with a dedicated rate-limit error that includes the free-tier reset time.

Makes agentic compaction the default context-compaction strategy.

Persists plan/act mode, tool auto-approve, and compaction mode to global settings with cross-process-safe writes, so CLI TUI toggles survive restarts.

Connector sessions now persist and automatically reconnect after a daemon or hub restart.

Generates the built-in provider list from models.dev, broadening out-of-the-box provider coverage.

+3 more

└──▷ BREAKING ON UPGRADE

! The `onRetryAttempt` callback is removed from `ApiHandlerOptions` and provider config.

WAS THIS USEFUL? 👍 👎

gemini-cli

Feedback ⓘ v0.53.0 NOTES ↗

An open-source AI agent that brings the power of Gemini directly into your terminal.

gemini-cli v0.53.0 adds an eval coverage report command and an LLM triage orchestrator.

└──▷ GET THIS VERSION ▾

```
$ git clone --branch v0.53.0 https://github.com/google-gemini/gemini-cli.git
# already have the repo? check out this version:
$ git checkout v0.53.0
```

Adds `eval coverage report` command to surface evaluation coverage metrics.

Implements an LLM triage orchestrator for automated issue triage workflows.

WAS THIS USEFUL? 👍 👎

OpenCode

Feedback ⓘ v1.18.9 NOTES ↗ CODE ↗

The open source coding agent.

OpenCode v1.18.9 adds an opt-in v2 desktop sidecar and collapsible model provider sections in settings.

└──▷ GET THIS VERSION ▾

```
$ git clone --branch v1.18.9 https://github.com/anomalyco/opencode.git
# already have the repo? check out this version:
$ git checkout v1.18.9
```

Adds opt-in v2 desktop sidecar: set `OPENCODE_SIDECAR_V2=1` to initialize the desktop app from the v2 background daemon instead of the v1 utility sidecar.

Adds collapsible model provider sections in the V2 settings page, with collapse state persisted per server and search expanding matching sections dynamically.

WAS THIS USEFUL? 👍 👎

AGENT

◆ AI Agent Frameworks

LangGraph

Feedback ⓘ 1.2.10 NOTES ↗

Build resilient agents.

LangGraph 1.2.10 adds per-node trace policies and typed v3 stream_events with native projections.

└──▷ GET THIS VERSION ▾

```
$ git clone --branch 1.2.10 https://github.com/langchain-ai/langgraph.git
# already have the repo? check out this version:
$ git checkout 1.2.10
```

└──▷ USE IT

Restrict tracing on a sensitive node by setting a custom trace policy at node registration time.

```python
graph.add_node("sensitive_step", sensitive_fn, trace_policy=my_trace_policy)
```

Exposes `trace_policy` parameter on `add_node`, enabling per-node control over tracing behaviour.

Adds typed return for v3 `stream_events` and supports native projections for more precise event filtering.

Removes `tags` from `TracePolicy`, simplifying the tracing configuration surface.

WAS THIS USEFUL? 👍 👎

GOVERN

◆ AI/LLM Security

ToolHive

Feedback ⓘ v0.41.0 NOTES ↗

ToolHive is an enterprise-grade platform for running and managing Model Context Protocol (MCP) servers.

ToolHive v0.41.0 adds MCP 2026-07-28 support, reproducible skill lock files, RFC 8693 token exchange, and an Envoy network-isolation backend.

└──▷ GET THIS VERSION ▾

```
$ git clone --branch v0.41.0 https://github.com/stacklok/toolhive.git
# already have the repo? check out this version:
$ git checkout v0.41.0
```

└──▷ TRY IT

Restore and verify a project's pinned MCP skills on a CI machine from the lock file.

```
$ thv skill sync
```

Re-resolve all pinned skills to newer content and update the lock file without silent drift.

```
$ thv skill upgrade
```

Supports the MCP 2026-07-28 stateless (Modern) spec across all proxies and Virtual MCP, bridging era-mismatched client×backend combinations automatically.

Virtual MCP is now fully MCP-conformant: completions, resource templates, subscriptions, and mid-call server→client forwarding (progress, sampling, elicitation) all work.

Adds `thv skill sync` to restore a project's pinned skill set on any machine and verify on-disk content in CI.

Adds `thv skill upgrade` to re-resolve pinned skills to newer content without silent lock drift.

Project-scoped skill installs are now pinned in a `toolhive.lock.yaml` lock file for reproducibility.

+10 more

└──▷ BREAKING ON UPGRADE

- ! Namespace-scoped operator installs (`operator.rbac.scope=namespace`) now fail `helm upgrade` at render time unless `operator.features.storageVersionMigrator: false` is explicitly set, because the StorageVersionMigrator controller is enabled by default.
- ! JSON-RPC batch requests (top-level arrays) are now rejected with HTTP 400 / error code `-32600` instead of being executed; send individual requests.
- ! The rate-limit JSON-RPC error code changed from `-32029` to `429` ; clients branching on `error.code == -32029` must match `429` instead.

WAS THIS USEFUL? 👍 👎

PLATFORMS & UTILITIES

◆ General Utilities & Libraries

Syslifters SysReptor

Feedback ⓘ 2026.61 NOTES ↗

A customizable and powerful penetration testing reporting platform for offensive security professionals. Simplify, customize, and automate your pentest reports with ease.

SysReptor 2026.61 adds Prowler/ScoutSuite import, stdin AES key support, and granular API token permissions.

└──▷ GET THIS VERSION ▾

```
$ git clone --branch 2026.61
https://github.com/Syslifters/sysreptor.git
# already have the repo? check out this version:
$ git checkout 2026.61
```

Adds Prowler and ScoutSuite importers to the `scanimport` plugin for ingesting cloud security scan results.

Allows creating API tokens with or without superuser permissions for finer-grained access control.

Adds automatic user lockout after multiple failed MFA login attempts.

Enables `backup` / `restorebackup` commands to read AES encryption keys from stdin for safer secret handling.

Validates initial status transitions at report/finding creation time.

+4 more

└──▷ BREAKING ON UPGRADE

! PDF compression is removed and the `COMPRESS_PDFS` setting no longer exists; any configuration referencing `COMPRESS_PDFS` will need to be cleaned up.

! Plugin loading is reworked so that the source code directory is now read-only in the Docker image; plugins or workflows that write to that directory will break.

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

▷ Subscribe Feedback on this issue