THE CYBER TOOLCHAIN

NO. 128

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED NOVEMBER 2, 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

INFORMATION DENSITY

everything



BRIEFED | EVERYTHING

Every tool in the issue, in full.

all 44 changes

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 124 tools

▾ // THE BRIEF

HIDE SAME ISSUE, SAME PROMPT, TWO WRITERS: GPT-5.5 | Opus 5

What stands out across today's releases, grouped by what it lets you do. Every tool named links to its entry below.

Three unrelated things stand out today: Jamf Pro can keep third-party Mac apps current without repackaging, BloodHound makes privilege-

vim ? help

zone exposure easier to query and export, and opentaint extends taint-flow analysis into Go codebases.

PROTECT

Keep non-App Store Mac apps updated without repackaging them

Jamf Pro's App Lifecycle Management Engine adds declarative, vendor-direct deployment and auto-updating for non-App Store Mac apps. That removes the packaging treadmill that often delays application updates and leaves endpoints running older builds.

Jamf Pro

IDENTIFY

Map privilege exposure with more usable graph outputs

BloodHound adds synthetic privilege-zone graph nodes, richer Explore controls, sortable and exportable tables, CSV export for findings, and sharper search and audit APIs. Teams can turn graph analysis into reviewable evidence and handoffs without manually reconstructing paths outside the tool.

bloodhound

PROTECT

Run taint-flow analysis against Go services

opentaint adds a formal models system and built-in Go models alongside its Java coverage. That lets teams apply source-to-sink analysis to Go codebases instead of treating those services as a blind spot or building approximations by hand.

opentaint

DETECT

Harden rule pipelines before bad telemetry silently drops coverage

rsigma now validates rule loads strictly, exposes a parse-error gauge, and renders EVTX records closer to native Windows output. Detection teams get earlier failure signals when content will not load cleanly, instead of discovering during an investigation that a rule never matched.

rsigma

Does **GPT-5.5** read better? 👍 👎

OFFENSIVE SECURITY

◆ Reconnaissance & OSINT

OpenOSINT

Feedback ⓘ CVE-2026-86045 CVE ↗

Open-source engine for passive OSINT checks: 21 tools as CLI, MCP server and web UI. Hosted Monitor & Diligence at app.openosint.tech.

`CVE-2026-86045`: Unauthenticated setup endpoint lets network attackers hijack OpenOSINT AI backend traffic (CVSS 10.0, affects `<= 2.23.0`)

WAS THIS USEFUL? 👍 👎

bbot Feedback ⓘ CVE-2026-12568 CVE ↗ STABLE

The recursive internet scanner for hackers.

`CVE-2026-12568` : Arbitrary File Write in postman_download Module (CVSS 6.5, affects `>= 2.1.0, <= 2.8.5`)

▾ **4 more releases in this issue** · 2025-10-09 → 2026-06-17

> CVE-2026-12565 CVE ↗ STABLE
>
> `CVE-2026-12565` : Path traversal (Zip-Slip) in unarchive module - incomplete fix for CVE-2025-10284 (CVSS 5.3, affects `>= 2.3.1, <= 2.8.4`)

> CVE-2025-10284 CVE ↗ STABLE
>
> `CVE-2025-10284` : Various issues in unarchive.py can cause arbitrary file write and RCE (CVSS 9.6, affects `< 2.7.0`)

> CVE-2025-10282 CVE ↗ STABLE
>
> `CVE-2025-10282` : gitlab.py exposes globally configured `gitlab` API key to on-premise GitLab instances, potentially threatening confidentiality of a gitlab.com API key (CVSS 4.7, affects `< 2.7.2`)

> CVE-2025-10281 CVE ↗ STABLE
>
> `CVE-2025-10281` : git_clone.py can be made to expose a user's github.com API key to an attacker-controlled webserver (CVSS 4.7, affects `< 2.7.0`)

WAS THIS USEFUL? 👍 👎

sherlock

Feedback ⓘ CVE-2026-44590 CVE ↗

Hunt down social media accounts by username across social networks

`CVE-2026-44590`: Command Injection via pull_request_target in validate_modified_targets.yml (CVSS 9.3, affects `<= v0.16.0`)

WAS THIS USEFUL? 👍 👎

tookie-osint

Feedback ⓘ CVE-2026-42866 CVE ↗

Tookie is a advanced OSINT information gathering tool that finds social media accounts based on inputs.

`CVE-2026-42866`: Arbitrary file write via path traversal in `-u` username / `-U` userfile output filename (affects `<= 4.1`)

WAS THIS USEFUL? 👍 👎

web-check

Feedback ⓘ CVE-2025-32778 CVE ↗

All-in-one OSINT tool for analysing any website

`CVE-2025-32778`: Command Injection via Unvalidated URL in Screenshot API (affects `<2.0.0`)

WAS THIS USEFUL? 👍 👎

osmedeus

Feedback ⓘ CVE-2024-51735 CVE ↗

A Modern Orchestration Engine for Security

`CVE-2024-51735`: Stored XSS to RCE on Osmedeus Web Server (affects `<= 4.6.4`)

WAS THIS USEFUL? 👍 👎

reconftw

Feedback ⓘ CVE-2023-46117 CVE ↗

reconFTW is a tool designed to perform automated recon on a target domain by running the best set of tools to perform scanning and finding out vulnerabilities

`CVE-2023-46117`: Inadequate validation of retrieved subdomains may lead to a Remote Code Execution (RCE) (CVSS 9.6, affects `< v2.7.1`)

WAS THIS USEFUL? 👍 👎

◆ Exploitation & C2

Rapid7 Metasploit Framework

Feedback ⓘ

CVE-2026-41316 CVE ↗

Metasploit Framework

`CVE-2026-41316`: db_import unsafe deserialisation (CWE-502) exposes Metasploit to code execution via crafted XML/ZIP import (related to CVE-2026-41316) (CVSS 7.0, affects `>= 4.0, < 6.5.5`)

WAS THIS USEFUL? 👍 👎

Bishop Fox sliver

Feedback ⓘ CVE-2026-77622 CVE ↗

STABLE

Sliver is an adversary emulation and red team framework

`CVE-2026-77622` : Unauthenticated Memory Exhaustion Denial of Service in Sliver HTTP(S) Listener PNG Decoder (affects `1.7.3`)

▾ **9 more releases in this issue** · 2023-06-20 → 2026-07-15

> CVE-2026-34227 CVE ↗ STABLE
>
> ▶ Watch video
>
> `CVE-2026-34227` : One-Click Remote Access: Insecure CORS & Unauthenticated MCP Interface (CVSS 8.8, affects `<= v1.7.3`)

> CVE-2026-32941 CVE ↗ STABLE
>
> `CVE-2026-32941` : Authenticated OOM via Memory Exhaustion in mTLS/WireGuard Transports (CVSS 6.5, affects `<= v1.7.3`)

> CVE-2026-29781 CVE ↗ STABLE
>
> `CVE-2026-29781` : CWE-476: Authenticated Nil-Pointer Dereference in Handlers (CVSS 6.5, affects `<= v1.7.3`)

> CVE-2026-25791 CVE ↗ STABLE
>
> `CVE-2026-25791` : DNS C2 OTP Bypass Allows Unauthenticated Session Flooding and Denial of Service (CVSS 7.5, affects `1.6.11`)

> CVE-2026-25760 CVE ↗ STABLE
>
> `CVE-2026-25760` : Website Path Traversal / Arbitrary File Read (Authenticated) in Sliver (CVSS 6.5, affects `1.6.10`)

> CVE-2025-27093 CVE ↗ STABLE
>
> `CVE-2025-27093` : Unrestricted traffic between Wireguard clients. (CVSS 6.3, affects `<= 1.5.43`)

CVE-2025-27090 CVE ↗ STABLE

`CVE-2025-27090` : SSRF in sliver teamserver v1.5.42/85b0e870d05ec47184958dbcb871ddee2eb9e3df (CVSS 5.3, affects `v1.5.26 to v1.5.42`)

CVE-2024-41111 CVE ↗ STABLE

`CVE-2024-41111` : Authenticated Operator-to-Server RCE (CVSS 7.2, affects `1.6.0-dev`)

CVE-2023-35170 CVE ↗ STABLE

`CVE-2023-35170` : MitM attack against implants due to a cryptographic vulnerability (CVSS 8.1, affects `1.5.0 - 1.5.39`)

WAS THIS USEFUL? 👍 👎

---

aptrs

Feedback ⓘ CVE-2026-34406 CVE ↗ STABLE

Automated pentest reporting with custom templates, project tracking, customer dashboard and client management tools. Streamline your security workflows effortlessly!

.
.
.
.

`CVE-2026-34406` : Privilege Escalation via Mass Assignment of is_superuser in User Edit Endpoint (CVSS 8.8, affects `<= 2.0`)

▾ **1 more release in this issue** · 2024-12-23 → 2026-03-31

CVE-2024-56363 CVE ↗ STABLE

`CVE-2024-56363` : Server Side Template Injection (CVSS 7.8, affects `1.0`)

WAS THIS USEFUL? 👍 👎

pwndoc

Feedback ⓘ CVE-2025-27413 CVE ↗ STABLE

Pentest Report Generator

`CVE-2025-27413` : Arbitrary File Write to RCE using Path Traversal in template update from backup templates.json (CVSS 6.5, affects `<1.2.0`)

▾ **3 more releases in this issue** · 2024-12-10 → 2025-02-28

> CVE-2025-23044 CVE ↗ STABLE
>
> `CVE-2025-23044` : Cross-Site Request Forgery (CSRF) allows creating admin account with POST request (CVSS 6.8, affects `latest`)

> CVE-2024-55652 CVE ↗ STABLE
>
> `CVE-2024-55652` : Server-Side Template Injection - Sandbox Escape to RCE using custom filters (CVSS 6.5, affects `<1.0.0`)

> CVE-2024-55653 CVE ↗ STABLE
>
> ⋮
>
> `CVE-2024-55653` : UnhandledPromiseRejection on audits causes Denial of Service (DoS) (CVSS 6.5, affects `=< 0.5.3`)

WAS THIS USEFUL? 👍 👎

◆ **AI-Powered Offensive Security**

RedAmon

Feedback ⓘ CVE-2026-103015 CVE ↗

Open-source, self-hosted AI penetration testing framework: maps your attack surface into a graph, autonomously exploits it from a Kali sandbox with human approval gates, and opens PRs that fix what it finds. MCP both ways: plug in any MCP server as a tool, or drive RedAmon from Claude Code or your own agent.

`CVE-2026-103015` : Unauthenticated remote code execution via exposed Kali MCP tool servers (CVSS 9.8, affects `< 5.3.1`)

WAS THIS USEFUL? 👍 👎

PurpleAILAB Decepticon

Feedback ⓘ CVE-2026-61732 CVE ↗

Autonomous Hacking Agent for Red Team

`CVE-2026-61732` : Role-boundary forgery via ChatML special-token literals in web crawl output composed into LLM context (CVSS 10.0, affects `<= 1.1.16`)

WAS THIS USEFUL? 👍 👎

◆ **Post-Exploitation**

penelope

Feedback ⓘ CVE-2026-50558 CVE ↗

Penelope Shell Handler

`CVE-2026-50558` : Penelope unsafe tar extraction allows arbitrary local file write via crafted session archive (CVSS 5.9, affects `< 0.19.3`)

WAS THIS USEFUL? 👍 👎

chisel

Feedback ⓘ CVE-2026-48113 CVE ↗ STABLE

A fast TCP/UDP tunnel over HTTP

`CVE-2026-48113` : ACL Bypass via Post-Handshake SSH Channel ExtraData Injection (affects `1.11.4`)

▾ **1 more release in this issue** · 2024-08-26 → 2026-05-20

> CVE-2024-43798 CVE ↗ STABLE
>
> `CVE-2024-43798` : AUTH environment variable not respected in server entrypoint (CVSS 8.6, affects `< v1.10.0`)

WAS THIS USEFUL? 👍 👎

netexec

Feedback ⓘ CVE-2026-27884 CVE ↗

The Network Execution Tool

`CVE-2026-27884`: Arbitrary file write via path traversal in spider_plus module (CVSS 5.3, affects `< 1.5.0`)

WAS THIS USEFUL? 👍 👎

APPLICATION SECURITY

◆ SAST / SCA / Code Security

noir

Feedback ⓘ v1.5.0 NOTES ↗

Hunt every Endpoint in your code, expose Shadow APIs, map the Attack Surface.

noir adds query verbs (`noir trace` , `noir reach` , `noir query`), native Windows and npm installs, Anthropic and Gemini AI providers, and new AI flags for streaming and key-file auth.

└──▷ GET THIS VERSION ▾

Docker

```
$ docker pull ghcr.io/owasp-noir/noir:1.5.0
```

npm

```
$ npm install -g @owasp-noir/noir@1.5.0
```

git

```
$ git clone --branch v1.5.0 https://github.com/owasp-noir/noir.git
# already have the repo? check out this version:
$ git checkout v1.5.0
```

published under the project's GitHub account · signed build provenance · checked 2 Nov

Wrong command?

Match a request to its route with `noir trace` , list routes that reach a file with `noir reach FILE[:LINE]` , and filter by guard, sink, param, path or handler with `noir query` — all reading a saved report via `--from` or scanning live.

Control AI behaviour with new flags `--ai-stream` , `--ai-key-file` , and `--ai-temperature` , and attach per-endpoint review context using the new `ai_context` JSON Schema.

Use a native Anthropic provider or a Gemini preset alongside existing AI providers, with explicit provider errors when misconfigured.

TypeScript, TSX and Ruby now use their own tree-sitter grammars, improving AST-based parsing for NestJS-family decorators, Fastify, Feathers, tRPC, LoopBack, and Rails callbacks.

NEW DETECTION Large repositories now scan faster — GitLab drops from 13s to 4.3s, vikunja from 15.6s to 2.0s, qdrant from 4.2s to 1.8s, and n8n peak memory from 669

MB to 410 MB.

NEW INTEGRATION npm package

NEW SUPPORTED PLATFORM Native Windows build

WAS THIS USEFUL? 👍 👎

Mend.io Mend SCA Feedback ⓘ

Version 26.10.1 (01-November-2026) NOTES ↗ RANK

Mend sca is a traditional application security misses AI risk. Standalone AI security tools miss your code.

> Mend SCA introduces an Intelligent Agent that lets users query risk data in natural language and generate executive-level risk summaries across all applications and projects.

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

01 **Intelligent Agent for natural-language risk queries** NEW

50

Mend SCA now includes the Intelligent Agent, an AI assistant embedded in the platform that accepts natural language queries to explore capabilities, navigate to relevant views, and generate executive-level risk summaries across all applications and projects. It is enabled by default for organizations with a signed AI consent addendum.

– Describes function and activation condition but no UI path or command.

Version 26.10.1 (01-November-2026)

WAS THIS USEFUL? 👍 👎

zizmor

Feedback ⓘ CVE-2026-102289 CVE ↗

Static analysis for GitHub Actions (and more)

`CVE-2026-102289`: Debug logging prints available GitHub credentials in cleartext (affects `=1.27.0`)

WAS THIS USEFUL? 👍 👎

Cisco skill-scanner

Feedback ⓘ CVE-2026-26057 CVE ↗

The skill-scanner is a security scanner for AI agent skills

`CVE-2026-26057`: Skill-scanner Unsecured Network Binding Vulnerability (CVSS 6.5, affects `<= 1.0.1`)

WAS THIS USEFUL? 👍 👎

deepaudit

Feedback ⓘ CVE-2026-25729 CVE ↗

DeepAudit：人人拥有的 AI 黑客战队，让漏洞挖掘触手可及。小白一键部署运行，自主协作审计 + 自动化沙箱 PoC 验证。支持 Ollama 私有部署 ，一键生成报告。支持中转站。让安全不再昂贵，让审计不再复杂。

`CVE-2026-25729`: User Enumeration via Broken Access Control (CVSS 6.5, affects `<=3.0.5`)

WAS THIS USEFUL? 👍 👎

HashiCorp terraform

Feedback ⓘ CVE-2019-19316 CVE ↗

Terraform enables you to safely and predictably create, change, and improve infrastructure. It is a source-available tool that codifies APIs into declarative configuration files that can be shared amongst team members, treated as code, edited, reviewed, and versioned.

`CVE-2019-19316`: Cleartext transmission of Terraform state snapshots when using Azure backend with certain SAS tokens (CVSS 7.5, affects `< 0.12.17`)

WAS THIS USEFUL? 👍 👎

opentaint

Feedback ⓘ analyzer/2026.11.02.54ad708 NOTES ↗ RANK

The open source taint analysis engine for the AI era. A formal dataflow analysis tool you can customize and self-host, built so AI agents drive your application security analysis without burning tokens on every scan.

> opentaint's analyzer gains a formal models system (replacing the old approximations mechanism) and ships built-in Go models alongside its existing Java models, extending taint-flow analysis to Go codebases.

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

01 **Models support in analyzer (renamed from approximations)** 35

BREAKING

opentaint's analyzer now supports `models` (formerly called approximations), enabling taint-flow modelling at analysis time. The rename is breaking: any configuration or rules referencing `approximations` by name will need to be updated.

– Names the concept and rename but no config key or mechanism detail

analyzer/2026.11.02.54ad708

02 **Built-in Go models for taint analysis** NEW 35

opentaint adds built-in Go models, extending its taint analysis to Go codebases alongside the existing Java models.

– Names new language support but no usage specifics given analyzer/2026.11.02.54ad708

└──▷ **BREAKING ON UPGRADE**

! Approximations are renamed to models throughout the tool; any configuration or rules referencing `approximations` by name will need to be updated.

WAS THIS USEFUL? 👍 👎

◆ Secrets Detection & Management

openbao

Feedback ⓘ CVE-2026-104093 CVE ↗ STABLE

OpenBao is a software solution to manage, store, and distribute sensitive data including secrets, certificates, and keys.

`CVE-2026-104093`: ACL Bypass via Non-Canonical URL Access in OpenBao (affects `<2.6.3`)

▾ **13 more releases in this issue** · 2026-05-21 → 2026-09-23

> `CVE-2026-104092` CVE ↗ STABLE
>
> `CVE-2026-104092`: OpenBao's PKI ACME Issues Certificate With Unvalidated SANs (affects `<2.6.3`)

> `CVE-2026-104090` CVE ↗ STABLE
>
> `CVE-2026-104090`: Remote Code Execution via `sys/storage/raft/snapshot-force` Plugin Catalog Replacement in OpenBao (affects `<2.6.3`)

> `CVE-2026-104088` CVE ↗ STABLE
>
> `CVE-2026-104088`: OpenBao - Internal Operation Dispatching Leads to Token Creation (affects `<2.6.2`)

> `CVE-2026-63131` CVE ↗ STABLE
>
> `CVE-2026-63131`: OpenBao Skips Stricter Deny Policy for LIST operations (affects `<2.6.0`)

> `CVE-2026-63132` CVE ↗ STABLE
>
> `CVE-2026-63132`: OpenBao's Recovery Mode Vulnerable To Token Leakage via Timing Attack (affects `<2.6.0`)

> `CVE-2026-71543` CVE ↗ STABLE
>
> `CVE-2026-71543`: OpenBao's Templated Policies Allow Privilege Escalation via Wildcard Characters (affects `<2.6.0`)

> `CVE-2026-77285` CVE ↗ STABLE
>
> `CVE-2026-77285`: OpenBao Agent Writes Secrets to Stdout (affects `<2.6.0`)

CVE-2026-55775 CVE ↗ STABLE

`CVE-2026-55775` : OpenBao's System Backend allows Unauthorized Management of the containing Namespace (affects `<=2.5.4`)

CVE-2026-55776 CVE ↗ STABLE

`CVE-2026-55776` : OpenBao crashes on Transit engine key creation with `derived=true` for RSA key types (CVSS 6.5, affects `<=2.5.4`)

CVE-2026-55774 CVE ↗ STABLE

`CVE-2026-55774` : Cross-namespace lease revocation via lease ID in path bypasses ACL (affects `<=2.5.4`)

CVE-2026-55770 CVE ↗ STABLE

`CVE-2026-55770` : LDAPi ldaputil (wrong escape func) (CVSS 6.8, affects `<=2.5.4`)

CVE-2026-46405 CVE ↗ STABLE

`CVE-2026-46405` : OpenBao's Kerberos Auth Method Accumulates Unaccessible Tokens (CVSS 5.3, affects `<=2.5.3`)

CVE-2026-46358 CVE ↗ STABLE

`CVE-2026-46358` : OpenBao's Inline Auth Incorrectly Redacted Headers (affects `<=2.5.3`)

WAS THIS USEFUL? 👍 👎

Bitnami Sealed Secrets

Feedback ⓘ CVE-2026-59341 CVE ↗

STABLE

A Kubernetes controller and tool for one-way encrypted Secrets

`CVE-2026-59341`: Internal POST endopints leaks sealed-secret plaintext through a template-injection oracle in sealed-secrets (CVSS 4.2, affects `<= v0.38.4`)

▾ **1 more release in this issue** · 2026-02-25 → 2026-09-11

> CVE-2026-22728 CVE ↗ STABLE
>
> `CVE-2026-22728`: sealed-secrets `/v1`/rotate can widen sealing scope to cluster-wide via attacker-controlled template annotations (CVSS 4.9, affects `sealed-secrets`)

WAS THIS USEFUL? 👍 👎

◆ Web Application Security

ProjectDiscovery nuclei

Feedback ⓘ CVE-2026-76805

CVE ↗ STABLE

Nuclei is a fast, customizable vulnerability scanner powered by the global security community and built on a simple YAML-based DSL, enabling collaboration to tackle trending vulnerabilities on the internet. It helps you find vulnerabilities in your applications, APIs, networks, DNS, and cloud configurations.

`CVE-2026-76805` : Environment Variable Disclosure via Response-Derived Data in DAST/Fuzz Mode (CVSS 5.3, affects `>= 3.0.0, < 3.10.0`)

▾ **6 more releases in this issue** · 2023-08-04 → 2026-07-16

> CVE-2026-76804 CVE ↗ STABLE
>
> `CVE-2026-76804` : Local File Read via Workflow File-Protocol Gate Bypass (CVSS 5.5, affects `>= 3.0.0, < 3.10.0`)

> CVE-2026-76802 CVE ↗ STABLE
>
> `CVE-2026-76802` : Arbitrary Command Execution via DAST Code Signature Bypass (CVSS 4.7, affects `>= 3.0.0, < 3.10.0`)

> CVE-2026-76819 CVE ↗ STABLE
>
> `CVE-2026-76819` : Arbitrary Code Execution via Goja JavaScript Engine Vulnerability (CVSS 8.6, affects `>= 3.0.0, < 3.10.0`)

> CVE-2024-43405 CVE ↗ STABLE
>
> `CVE-2024-43405` : Nuclei Template Signature Verification Bypass (CVSS 7.4, affects `> 3.0.0`)

> CVE-2024-40641 CVE ↗ STABLE
>
> `CVE-2024-40641` : Unsigned code template execution through workflows in projectdiscovery/nuclei (CVSS 7.4, affects `> 3.0.0`)

> CVE-2023-37896 CVE ↗ STABLE
>
> `CVE-2023-37896` : Nuclei < 2.9.9 - Sandbox restriction bypass (CVSS 5.9, affects `< 2.9.9`)

WAS THIS USEFUL?  

ffuf Feedback ⓘ CVE-2026-73232 CVE ↗

Fast web fuzzer written in Go

`CVE-2026-73232`: ffuf denial of service (OOM) via HTTP response decompression bomb (CVSS 7.5, affects `<= 2.1.0`)

WAS THIS USEFUL?  

Cure53 DOMPurify

Feedback ⓘ CVE-2026-49978 CVE ↗ STABLE

DOMPurify - a DOM-only, super-fast, uber-tolerant XSS sanitizer for HTML, MathML and SVG. DOMPurify works with a secure default, but offers a lot of configurability and hooks. Demo:

`CVE-2026-49978`: DOMPurify `IN_PLACE` Sanitization Bypass via Attached Shadow Root Inside <template>.content (CVSS 6.1, affects `<3.4.6`)

▾ **8 more releases in this issue** · 2024-10-11 → 2026-05-27

> CVE-2026-49459 CVE ↗ STABLE
>
> `CVE-2026-49459`: `IN_PLACE` mode preserves attributes of a clobbered root element, allowing XSS via attacker-controlled root DOM (CVSS 6.1, affects `<= 3.4.5`)

> CVE-2026-49458 CVE ↗ STABLE
>
> `CVE-2026-49458`: Cross-realm `IN_PLACE` sanitization leaves executable markup intact via realm-bound `instanceof` checks (CVSS 6.1, affects `<= 3.4.5`)

> CVE-2026-47423 CVE ↗ STABLE
>
> `CVE-2026-47423`: DOMPurify XSS via `selectedcontent` re-clone (CVSS 8.2, affects `3.4.4`)

> CVE-2026-41240 CVE ↗ STABLE
>
> `CVE-2026-41240`: `FORBID_TAGS` bypassed by function-based `ADD_TAGS` predicate (asymmetry with `FORBID_ATTR` fix) (CVSS 6.1, affects `<= 3.2.6`)

> CVE-2026-41239 CVE ↗ STABLE
>
> `CVE-2026-41239`: Dompurify `SAFE_FOR_TEMPLATES` bypass in `RETURN_DOM` mode (CVSS 6.8, affects `< 3.3.3`)

> CVE-2026-41238 CVE ↗ STABLE
>
> `CVE-2026-41238`: Prototype Pollution to XSS Bypass via `CUSTOM_ELEMENT_HANDLING` Fallback (CVSS 6.9, affects `3.0.1 through 3.3.3`)

> CVE-2024-48910 CVE ↗ STABLE
>
> `CVE-2024-48910`: Tampering by prototype polution (CVSS 9.1, affects `< 2.4.2`)

CVE-2024-47875 CVE ↗ STABLE

`CVE-2024-47875` : nesting-based mXSS (CVSS 10.0, affects `<2.5.0`)

WAS THIS USEFUL? 👍 👎

Dalfox Feedback ⓘ CVE-2026-45088 CVE ↗ STABLE

Dalfox is an XSS scanner that automates parameter analysis, reflected/stored/DOM-based XSS detection, and WAF fingerprinting for web apps.

`CVE-2026-45088` : Unauthenticated Arbitrary File Read with Out-of-Band Exfiltration via `custom-payload-file` in Dalfox Server Mode (CVSS 7.5, affects `<= 2.12.0`)

▾ **1 more release in this issue** · 2026-05-07

CVE-2026-45090 CVE ↗ STABLE

`CVE-2026-45090` : Unauthenticated Remote DoS via Closed-Channel Write in `ParameterAnalysis` (server mode) (CVSS 7.5, affects `<= 2.12.0`)

WAS THIS USEFUL? 👍 👎

mitmproxy Feedback ⓘ CVE-2026-40606 CVE ↗ STABLE

An interactive TLS-capable intercepting HTTP proxy for penetration testers and software developers.

`CVE-2026-40606`: LDAP Injection in mitmproxy (CVSS 4.8, affects `<=12.2.1`)

▾ **3 more releases in this issue** · 2022-03-19 → 2026-04-12

> CVE-2025-57804 CVE ↗ STABLE
>
> `CVE-2025-57804`: Vulnerable python-hyper/h2 dependency embedded in mitmproxy binaries (affects `<= 12.1.1`)

> CVE-2025-23217 CVE ↗ STABLE
>
> `CVE-2025-23217`: Mitmweb API Authentication Bypass Using Proxy Server (affects `< 11.1.1`)

> CVE-2022-24766 CVE ↗ STABLE
>
> `CVE-2022-24766`: Insufficient Protection against HTTP Request Smuggling in mitmproxy (CVSS 9.8, affects `<=7.0.4`)

WAS THIS USEFUL? 👍 👎

caido

Feedback ⓘ CVE-2026-24853 CVE ↗ STABLE

Caido releases, wiki and roadmap

`CVE-2026-24853` : Insufficient patch for DNS rebind leading to RCE (CVSS 8.1, affects `<0.55.0`)

▾ **4 more releases in this issue** · 2025-01-17 → 2026-02-13

> CVE-2025-66025 CVE ↗ STABLE
>
> `CVE-2025-66025` : Improper Handling of External Links in Markdown (CVSS 4.3, affects `<=0.52.0`)

> CVE-2025-53834 CVE ↗ STABLE
>
> `CVE-2025-53834` : Reflected XSS in Caido Toast (CVSS 6.3, affects `<0.49.0`)

> CVE-2025-49004 CVE ↗ STABLE
>
> `CVE-2025-49004` : Hijacking Caido instance during the initial setup via DNS Rebinding to achieve RCE (CVSS 7.5, affects `< 0.48.0`)

> CVE-2025-23039 CVE ↗ STABLE
>
> `CVE-2025-23039` : Cross Site Scripting on URL decode Tooltip (CVSS 5.2, affects `= 0.45.0`)

WAS THIS USEFUL? 👍 👎

◆ WAF, Bot & API Protection

Bunkerity BunkerWeb

Feedback ⓘ CVE-2026-75514 CVE ↗

STABLE

Open-source and cloud-native Web Application Firewall (WAF)

`CVE-2026-75514` : rDNS bypass via missing forward-confirmation (FCrDNS) in blacklist, greylist, whitelist and antibot (CVSS 5.9, affects `< 1.6.13`)

▾ **3 more releases in this issue** · 2024-11-27 → 2026-07-16

> CVE-2026-54728 CVE ↗ STABLE
>
> `CVE-2026-54728` : Authenticated privilege escalation via Host header handling in BunkerWeb UI and API (affects `< 1.6.12`)

> CVE-2026-61718 CVE ↗ STABLE
>
> `CVE-2026-61718` : Read-only Web UI users can delete job cache files due to missing authorization on `/cache` / routes (CVSS 5.4, affects `>= 1.6.2, < 1.6.12`)

> CVE-2024-53264 CVE ↗ STABLE
>
> `CVE-2024-53264` : Open Redirect Vulnerability in Loading Page (affects `<=1.5.11`)

WAS THIS USEFUL? 👍 👎

◆ Software Supply Chain Security

Datadog GuardDog

Feedback ⓘ CVE-2026-44971 CVE ↗ STABLE

GuardDog is a CLI tool to Identify malicious PyPI and npm packages

`CVE-2026-44971`: Blind GitHub URL rewrite in remote project scanning causes SSRF and `GH_TOKEN` exfiltration (CVSS 8.2, affects `>= 1.0.0, <= 2.9.0`)

▾ **4 more releases in this issue** · 2022-12-05 → 2026-05-06

> CVE-2026-44972 CVE ↗ STABLE
>
> `CVE-2026-44972`: Unsanitized human-readable scan output allows terminal escape injection from malicious package content (CVSS 5.0, affects `>= 2.6.0, <= 2.9.0`)

> CVE-2026-22871 CVE ↗ STABLE
>
> `CVE-2026-22871`: Path Traversal Vulnerability Leads to Arbitrary File Overwrite and RCE (CVSS 9.8, affects `2.7.0 and below`)

> CVE-2026-22870 CVE ↗ STABLE
>
> `CVE-2026-22870`: Zip Bomb Vulnerability in safe_extract() Allows DoS (CVSS 7.5, affects `2.7.0 and below`)

> CVE-2022-23530 CVE ↗ STABLE
>
> `CVE-2022-23530`: Arbitrary file write when scanning a specially-crafted remote PyPI package (CVSS 5.8, affects `<v0.1.7`)

WAS THIS USEFUL? 👍 👎

zarf

Feedback ⓘ CVE-2026-40090 CVE ↗ STABLE

The Airgap Native Package Manager for Kubernetes

`CVE-2026-40090`: Path Traversal via Malicious Package Metadata.Name — Arbitrary File Write (CVSS 7.1, affects `>=v0.23.0, <v0.74.2`)

▾ **1 more release in this issue** · 2026-03-06 → 2026-04-14

> CVE-2026-29064 CVE ↗ STABLE
>
> `CVE-2026-29064`: Symlink targets in archives are not validated against destination directory (CVSS 8.2, affects `>=v0.54.0, < v0.73.1`)

WAS THIS USEFUL? 👍 👎

Sigstore cosign

Feedback ⓘ CVE-2026-39395 CVE ↗ STABLE

Code signing and transparency for containers and binaries

`CVE-2026-39395`: verify-blob-attestation reports false positive when payload parsing fails (CVSS 4.3, affects `<= v3.0.5, <= v2.6.2`)

▾ **4 more releases in this issue** · 2022-08-04 → 2026-04-06

> CVE-2026-22703 CVE ↗ STABLE
>
> `CVE-2026-22703`: Verification accepts any valid Rekor entry under certain conditions (CVSS 5.5, affects `<= 2.6.1, <= 3.0.3`)

> CVE-2024-29903 CVE ↗ STABLE
>
> `CVE-2024-29903`: Malicious artifacts can cause machine-wide DoS (CVSS 4.2, affects `<= 2.2.3`)

> CVE-2022-36056 CVE ↗ STABLE
>
> `CVE-2022-36056`: Vulnerabilities with blob verification (CVSS 5.5, affects `<=1.11.1`)

> CVE-2022-35929 CVE ↗ STABLE
>
> `CVE-2022-35929`: `cosign verify-attestation --type` can report a false positive if any attestation exists (CVSS 9.8, affects `< 1.10.0`)

WAS THIS USEFUL? 👍 👎

Anchore syft

Feedback ⓘ CVE-2026-33481 CVE ↗ STABLE

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

`CVE-2026-33481`: Syft improper temporary file cleanup (CVSS 5.3, affects `< v1.42.3`)

▾ **1 more release in this issue** · 2023-02-06 → 2026-03-20

> CVE-2023-24827 CVE ↗ STABLE
>
> `CVE-2023-24827`: Credential disclosure in syft when `SYFT_ATTEST_PASSWORD` environment variable set (CVSS 6.5, affects `>= v0.69.0 && < v0.70.0`)

WAS THIS USEFUL? 👍 👎

go-tuf Feedback ⓘ CVE-2026-24686 CVE ↗ STABLE

Go implementation of The Update Framework (TUF)

`CVE-2026-24686`: go-tuf TAP 4 multirepo repoName path traversal escapes local metadata cache directory (CVSS 4.7, affects `<= 2.4.0`)

▾ **4 more releases in this issue** · 2022-05-05 → 2026-01-26

> CVE-2026-23992 CVE ↗ STABLE
>
> `CVE-2026-23992`: Improper validation of configured threshold for delegations (CVSS 5.9, affects `< v2.3.1`)

> CVE-2026-23991 CVE ↗ STABLE
>
> `CVE-2026-23991`: Client DoS via malformed server response (CVSS 5.9, affects `< v2.3.1`)

> CVE-2024-47534 CVE ↗ STABLE
>
> `CVE-2024-47534`: Incorrect delegation lookups can make go-tuf download the wrong artifact (affects `<=v2.0.0`)

> CVE-2022-29173 CVE ↗ STABLE
>
> `CVE-2022-29173`: No protection against rollback attacks for roles other than root (CVSS 8.8, affects `v0.2.0`)

WAS THIS USEFUL? 👍 👎

cyclonedx-core-java Feedback ⓘ CVE-2025-64518 CVE ↗

STABLE

CycloneDX SBOM Model and Utils for Creating and Validating BOMs

`CVE-2025-64518` : BOM validation is vulnerable to XML External Entity injection (CVSS 7.5, affects `<11.0.1`)

▾ **1 more release in this issue** · 2024-06-24 → 2025-11-10

> CVE-2024-38374 CVE ↗ STABLE
>
> `CVE-2024-38374` : Improper Restriction of XML External Entity Reference in org.cyclonedx:cyclonedx-core-java (CVSS 7.5, affects `>= 2.1.0, < 9.0.4`)

WAS THIS USEFUL? 👍 👎

OWASP dependency-track

Feedback ⓘ CVE-2025-61776 CVE ↗

STABLE

Dependency-Track is an intelligent Component Analysis platform that allows organizations to identify and reduce risk in the software supply chain.

`CVE-2025-61776` : Possible disclosure of private NuGet repository credentials to `api.nuget.org` (CVSS 4.7, affects `< 4.13.5`)

▾ **4 more releases in this issue** · 2022-10-11 → 2025-10-07

> CVE-2025-27137 CVE ↗ STABLE
>
> `CVE-2025-27137` : Local file inclusion via custom notification templates (CVSS 4.4, affects `< 4.12.6`)

> CVE-2024-54002 CVE ↗ STABLE
>
> `CVE-2024-54002` : Enumeration of managed users via `/api`/v1/user/login endpoint (CVSS 5.3, affects `< 4.12.2`)

> CVE-2024-38515 CVE ↗ STABLE
>
> `CVE-2024-38515` : Possible XML External Entity injection via upload of CycloneDX BOMs in XML format (CVSS 5.4, affects `>= 3.6.0, < 4.11.4`)

> CVE-2022-39351 CVE ↗ STABLE
>
> `CVE-2022-39351` : Logging of API keys in clear text when handling API requests using keys with insufficient permissions (CVSS 4.4, affects `< 4.6.0`)

WAS THIS USEFUL? 👍 👎

REVERSE ENGINEERING, MALWARE & FORENSICS

◆ Reverse Engineering

HyperDbg

Feedback ⓘ v0.25 NOTES ↗ RANK

State-of-the-art native debugging tools

> HyperDbg v0.25 brings Linux host support, allowing practitioners to debug a Windows guest over a serial connection from a Linux machine, alongside improved anti-detection coverage.

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

01 **Linux host support for debugging Windows guests** NEW

65

HyperDbg now supports running as a Linux host to debug a Windows guest machine over a serial kernel debugger connection. The `.debug` command on Linux now accepts device and socket paths, enabling serial connections over termios devices and UNIX sockets.

— Names command and connection types but no full syntax v0.25

THINNER COVERAGE BELOW

02 **XSETBV handling in hyperevade** IMPROVED

35

HyperDbg's `hyperevade` module now handles XSETBV instructions to improve anti-detection coverage.

— Names module and instruction but lacks mechanism detail v0.25

WAS THIS USEFUL? 👍 👎

National Security Agency ghidra

Feedback ⓘ

CVE-2026-100504 CVE ↗ STABLE

Ghidra is a software reverse engineering (SRE) framework

`CVE-2026-100504`: Out-of-bounds read and write in `leftshift128` during decompilation (CVSS 6.1, affects `< 12.2`)

▾ **3 more releases in this issue** · 2026-09-22 → 2026-10-22

> CVE-2026-100503 CVE ↗ STABLE
>
> `CVE-2026-100503`: Heap-use-after-free in the opInsertAfter via a stale INDIRECT effect-op reference (CVSS 6.1, affects `< 12.2`)

> CVE-2026-100505 CVE ↗ STABLE
>
> `CVE-2026-100505`: Heap out-of-bounds read in decompiler StringManager::getCodepoint() when reconstructing constant strings (CVSS 4.4, affects `< 12.2`)

> CVE-2026-96273 CVE ↗ STABLE
>
> `CVE-2026-96273`: Improper Array Index Validation in DB Unregistered Options parsing Leads to unreleased lock and Denial of Service (CVSS 5.5, affects `< 12.1.4`)

WAS THIS USEFUL? 👍 👎

Radare2 Feedback ⓘ CVE-2026-108387 CVE ↗ STABLE

UNIX-like reverse engineering framework and command-line toolset

`CVE-2026-108387` : Remote code execution when loading Pebble/SMD binary (affects `< 6.2.2`)

▾ **4 more releases in this issue** · 2020-07-20 → 2026-09-03

> CVE-2026-81885 CVE ↗ STABLE
>
> `CVE-2026-81885` : Infinite relocation-chain loop causes denial of service in radare2 NE parser (CVSS 5.5, affects `<6.1.9`)

> CVE-2026-81886 CVE ↗ STABLE
>
> `CVE-2026-81886` : Uncontrolled memory allocation in radare2 dmp64 parser (CVSS 5.5, affects `<6.1.9`)

> CVE-2026-81879 CVE ↗ STABLE
>
> `CVE-2026-81879` : Heap out-of-bounds read in radare2 ELF `PN_XNUM` handling (CVSS 5.5, affects `<6.1.9`)

> CVE-2020-15121 CVE ↗ STABLE
>
> `CVE-2020-15121` : Command injection during opening PE file with malformed debug symbol information (PDB) - `idpd` command (CVSS 9.6, affects `<4.5.0`)

WAS THIS USEFUL? 👍 👎

jadx Feedback ⓘ CVE-2026-42049 CVE ↗ STABLE

Dex to Java decompiler

`CVE-2026-42049` : RCE Via Groovy Code Injection in Gradle Export (affects `<= 1.5.5`)

▾ **4 more releases in this issue** · 2022-07-20 → 2026-07-10

> CVE-2026-54684 CVE ↗ STABLE
>
> `CVE-2026-54684` : XAPK archive entries with absolute paths can plant drop-in plugins and achieve code execution on the next jadx run (CVSS 7.0, affects `v1.5.2 through v1.5.5`)

> CVE-2024-32653 CVE ↗ STABLE
>
> `CVE-2024-32653` : Insufficient input filtering of `package name` allows command execution in the device with shell privileges (CVSS 6.1, affects `<=1.4.7`)

> CVE-2022-39259 CVE ↗ STABLE
>
> `CVE-2022-39259` : Jadx-gui: Swing HTML DOS attack (CVSS 5.5, affects `<= 1.4.4`)

> CVE-2021-22569 CVE ↗ STABLE
>
> `CVE-2021-22569` : Vulnerable library protobuf-java 3.11.4 (CVSS 5.5, affects `3.11.4`)

WAS THIS USEFUL? 👍 👎

Capstone

Feedback ⓘ CVE-2026-55893 CVE ↗ STABLE

Capstone disassembly/disassembler framework for ARM, ARM64 (ARMv8), Alpha, BPF, Ethereum VM, HPPA, LoongArch, M68K, M680X, Mips, MOS65XX, PPC, RISC-V(rv32G/rv64G), SH, Sparc, SystemZ, TMS320C64X, TriCore, Webassembly, XCore and X86.

`CVE-2026-55893`: Capstone SH disassembler `set_reg_n` heap buffer overflow via crafted SH2A FPU bytecode (affects `<= v6.0.0-Alpha9`)

▾ **5 more releases in this issue** · 2025-12-17 → 2026-06-18

> CVE-2026-49263 CVE ↗ STABLE
>
> `CVE-2026-49263`: Capstone WASM `br_table` instruction-size truncation can cause no-progress disassembly and parser desynchronization (affects `commit 511ba599951113828c4e8edd262ee363395bd81d`)

> CVE-2026-49282 CVE ↗ STABLE
>
> `CVE-2026-49282`: Capstone M68K and RISCV cs_insn_name() invalid IDs can trigger out-of-bounds reads and process crashes (CVSS 5.1, affects `commit 511ba599951113828c4e8edd262ee363395bd81d`)

> CVE-2026-47143 CVE ↗ STABLE
>
> `CVE-2026-47143`: NULL Pointer Dereference with 3DNow! opcodes (CVSS 5.1, affects `6.0.0-Alpha5`)

> CVE-2025-68114 CVE ↗ STABLE
>
> `CVE-2025-68114`: Unchecked vsnprintf return in SStream_concat allows stack buffer underflow&overflow (CVSS 4.8, affects `6.0.0-Alpha5`)

> CVE-2025-67873 CVE ↗ STABLE
>
> `CVE-2025-67873`: Skipdata length unchecked leads to cs_insn.bytes heap buffer overflow (CVSS 4.8, affects `6.0.0-Alpha5`)

WAS THIS USEFUL? 👍 👎

Rizin

Feedback ⓘ CVE-2026-22780 CVE ↗ STABLE

UNIX-like reverse engineering framework and command-line toolset.

`CVE-2026-22780`: Heap overflow on mach0_chained_fixups.c (CVSS 4.4, affects `< 0.8.2`)

▾ **6 more releases in this issue** · 2021-12-13 → 2026-02-01

> CVE-2024-53256 CVE ↗ STABLE
>
> `CVE-2024-53256`: Command injection via RzBinInfo bclass due legacy code (CVSS 7.3, affects `< 0.7.3`)

> CVE-2023-40022 CVE ↗ STABLE
>
> `CVE-2023-40022`: Integer Overflow in C++ demangler logic (CVSS 7.3, affects `<=0.6.0`)

> CVE-2023-27590 CVE ↗ STABLE
>
> `CVE-2023-27590`: Stack-based buffer overflow when parsing GDB registers profile files (CVSS 7.8, affects `<=v0.5.1`)

> CVE-2022-36043 CVE ↗ STABLE
>
> `CVE-2022-36043`: Double Free in bobj.c when using QNX binary plugin (CVSS 7.8, affects `<=0.4.0`)

> CVE-2022-36040 CVE ↗ STABLE
>
> `CVE-2022-36040`: Out-of-bounds Write in pyc/marshal.c (CVSS 7.8, affects `<=0.4.0`)

> CVE-2021-43814 CVE ↗ STABLE
>
> `CVE-2021-43814`: Heap-based OOB write when parsing dwarf DIE info in Rizin (CVSS 7.8, affects `<=0.3.1`)

WAS THIS USEFUL? 👍 👎

bytecode-viewer

Feedback ⓘ CVE-2022-21675 CVE ↗

A Java 8+ Jar & Android APK Reverse Engineering Suite (Decompiler, Editor, Debugger & More)

`CVE-2022-21675`: Bytecode Viewer v2.10.x Zip Slip (CVSS 7.8, affects `v2.10.16`)

WAS THIS USEFUL? 👍 👎

◆ **Digital Forensics & Incident Response**

Velocidex Velociraptor

Feedback ⓘ CVE-2026-85737 CVE ↗

Digging Deeper....

`CVE-2026-85737`: Low-priv analyst reads arbitrary server files via ungated sql() VQL plugin (CVSS 6.5, affects `<= 0.77.1`)

WAS THIS USEFUL? 👍 👎

DFIR ORC

Feedback ⓘ CVE-2026-11958 CVE ↗

Forensics artefact collection tool for systems running Microsoft Windows

`CVE-2026-11958`: Local privilege escalation via DLL side-loading when executed as SYSTEM or from a user-writable directory (affects `<10.2.8`)

WAS THIS USEFUL? 👍 👎

Mobile Verification Toolkit Feedback ⓘ

CVE-2026-46486 CVE ↗

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

`CVE-2026-46486`: Path Traversal via unsanitized File identifiers in iOS Backup processing (affects `<=2026.4.28`)

WAS THIS USEFUL? 👍 👎

bulk-extractor Feedback ⓘ CVE-2026-24857 CVE ↗

This is the development tree. Production downloads are at:

`CVE-2026-24857`: Heap-based Buffer Overflow in bulk_extractor (CVSS 9.8, affects `>= 1.4, < 2.2.0`)

WAS THIS USEFUL? 👍 👎

◆ Malware Analysis

malcontent

Feedback ⓘ CVE-2026-28407 CVE ↗ STABLE

#supply #chain #attack #detection

`CVE-2026-28407` : Nested archive extraction failure can drop content from scan inputs (CVSS 5.3, affects `< v1.21.0`)

▾ **2 more releases in this issue** · 2026-01-29 → 2026-02-27

> CVE-2026-24845 CVE ↗ STABLE
>
> `CVE-2026-24845` : OCI image scanning could expose registry credentials (CVSS 6.5, affects `>= 0.10.0, < 1.20.3`)

> CVE-2026-24846 CVE ↗ STABLE
>
> `CVE-2026-24846` : Archive extraction could write outside extraction directory (CVSS 5.5, affects `>= 1.8.0, < 1.20.3`)

WAS THIS USEFUL? 👍 👎

CAPEv2 Feedback ⓘ changes since 2026-10-27 CODE ↗

Malware Configuration And Payload Extraction

CAPEv2 adds multi-tenancy isolation with per-group sandbox policies, a reconcile CLI, and a generic plugin hook/startup extension loader

└──▷ **TRY IT**

Dry-run the tenancy reconcile tool to preview which MongoDB/Elasticsearch reports would be restamped before committing changes on an upgraded install.

```
$ python utils/tenancy_reconcile.py --dry-run --adopt-public-from-reports
```

Reconcile a single task's ACL and visibility after migrating from inline tenancy SQL columns to the new `task_acl` side-table.

```
$ python utils/tenancy_reconcile.py --task 14
```

Manage multi-tenancy entitlements with `GroupSandboxPolicy` to assign per-group VM allocations, network routes, and machine tags, backed by a side-table `TaskAcl` with monotonic `visibility_seq` compare-and-swap synchronization, under the `[multitenancy]` and `[object_storage]` config sections in `lib/tenancy/`.

Run `utils/tenancy_reconcile.py` with `--dry-run`, `--adopt-public-from-reports`, `--demote-public`, or `--task <id>` to restamp MongoDB/Elasticsearch reports, preserve public task visibility in `task_acl`, and drop legacy inline-tenancy SQL columns.

CAPEv2 now supports vendor-neutral object storage backends — `s3`, `gcs`, `azure`, and `local` — configured under the `[object_storage]` section via the opt-in `lib.tenancy` package.

CAPEv2 adds a generic plugin hook system and startup extension loader in `lib/cuckoo/common/hooks.py`, letting single-tenant installs opt in to extensions without incurring runtime or schema overhead.

CAPEv2 adds `lib/cuckoo/common/pebble_utils.py` with teardown_pool() and is_pool_healthy() to give the `PebbleEngine` and extractor pool bounded teardown and a single shared health check, preventing permanent hangs on D-state workers.

WAS THIS USEFUL?  

NETWORK SECURITY

◆ OT / ICS Security

cisagov Malcolm

Feedback ⓘ CVE-2026-107362 CVE ↗ STABLE

Malcolm is a powerful, easily deployable network traffic analysis tool suite for full packet capture artifacts (PCAP files), Zeek logs and Suricata alerts.

`CVE-2026-107362`: SSRF with full response-body readback via the FilePond fetch API in the file-upload component (CVSS 7.1, affects `<= 26.08.0`)

▾ **8 more releases in this issue** · 2026-07-15 → 2026-09-30

> CVE-2026-107333 CVE ↗ STABLE
>
> `CVE-2026-107333`: Authorization bypass: an unresolved `/./` segment defeats every nginx RBAC role restriction (CVSS 8.1, affects `<= v26.08.0`)

> CVE-2026-107361 CVE ↗ STABLE
>
> `CVE-2026-107361`: Missing Server-to-Server (s2s) Authentication Configuration on Hedgehog Sensor Arkime Reachback Port (CVSS 4.2, affects `<= v26.07.1`)

> CVE-2026-107337 CVE ↗ STABLE
>
> `CVE-2026-107337`: Unauthenticated script execution via CSRF in kiosk `/script` _call endpoint (CVSS 7.1, affects `<= v26.07.1`)

> CVE-2026-107336 CVE ↗ STABLE
>
> `CVE-2026-107336`: Unauthenticated bypass of the nginx auth gate on the `/iddash2ark` / Arkime shortcut (regex case-sensitivity mismatch + forwarded-identity confused deputy) (CVSS 6.5, affects = v26.07.1 (current CalVer line; also present in nginx_readonly.conf — note: pre-CalVer v6.4.3 is NOT affected))

> CVE-2026-107334 CVE ↗ STABLE
>
> `CVE-2026-107334`: Percent-Encoded Request Paths Bypass Malcolm's nginx RBAC (CVSS 5.4, affects `<= v26.07.1`)

> CVE-2026-107335 CVE ↗ STABLE
>
> `CVE-2026-107335`: Raw-stream and Lzip Uploads Bypass Malcolm's Archive-Bomb Protections (CVSS 6.5, affects `<= v26.07.1`)

> CVE-2026-63133 CVE ↗ STABLE

> `CVE-2026-63133` : Uncontrolled Resource Consumption in Archive Extraction (Inode-Exhaustion DoS) (CVSS 6.5, affects `<= v26.06.1`)

> `CVE-2026-63134` CVE ↗ STABLE
>
> `CVE-2026-63134` : Path Traversal in Archive Extraction Allows Arbitrary Directory Creation (CVSS 5.4, affects `<= v26.06.1`)

WAS THIS USEFUL? 👍 👎

◆ IDS / IPS

OISF Suricata

Feedback ⓘ CVE-2026-94084 CVE ↗ STABLE

Suricata is a network Intrusion Detection System, Intrusion Prevention System and Network Security Monitoring engine developed by the OISF and the Suricata community.

`CVE-2026-94084` : detect/http2: header inspection can trigger a use-after-free (CVSS 9.1, affects `>= 8.0.4, < 8.0.7`)

▾ 1 more release in this issue · 2026-09-21

> `CVE-2026-94083` CVE ↗ STABLE
>
> `CVE-2026-94083` : DoH2: upgrade from HTTP2 to DoH2 can cause a type-confused free (CVSS 9.1, affects `>= 8.0.0, < 8.0.7`)

WAS THIS USEFUL? 👍 👎

CrowdSec

Feedback ⓘ CVE-2026-44982 CVE ↗ STABLE

Open-source IDS/IPS, WAF and bot detection for Linux, Windows, Docker and Kubernetes, with a crowdsourced blocklist of malicious IPs.

`CVE-2026-44982`: CrowdSec AppSec silently drops request body for chunked / HTTP-2 requests (CVSS 7.2, affects `=>1.5.0, =<1.7.7`)

▾ **1 more release in this issue** · 2026-05-27

> CVE-2026-44981 CVE ↗ STABLE
>
> `CVE-2026-44981`: CrowdSec LAPI: Denial of Service via Unbounded Gzip Decompression (affects `>= 1.7.0`)

WAS THIS USEFUL? 👍 👎

Fail2ban

Feedback ⓘ CVE-2021-32749 CVE ↗

Daemon to ban hosts that cause multiple authentication errors

`CVE-2021-32749`: Possible RCE vulnerability in mailing action using mailutils (mail-whois) (CVSS 8.1, affects `<= 9.7, <= 10.6, <= 11.2`)

WAS THIS USEFUL? 👍 👎

◆ Network Analysis & Monitoring

tcpreplay

Feedback ⓘ CVE-2026-102897 CVE ↗ STABLE

Edit and replay captured network traffic at arbitrary speeds — a suite of pcap tools for *NIX and Windows.

`CVE-2026-102897`: Heap Out-of-Bounds Read up via `--pktlen` combined with `--preload-pcap` in tcpreplay (CVSS 7.7, affects `<= 4.6.0-beta2`)

▾ 9 more releases in this issue · 2026-07-23 → 2026-07-24

> CVE-2026-102898 CVE ↗ STABLE
>
> `CVE-2026-102898`: Heap Out-of-Bounds Write in ARP Address Rewriting via Unvalidated ar_hln/ar_pln (CVSS 7.1, affects `<= 4.6.0-beta2`)

> CVE-2026-102896 CVE ↗ STABLE
>
> `CVE-2026-102896`: Stack Buffer Overflow in tcpprep `--services` File Parser via Unbounded Regex Match Copied with strncpy() (CVSS 7.8, affects `<= 4.6.0-beta2`)

> CVE-2026-102754 CVE ↗ STABLE
>
> `CVE-2026-102754`: SEGV in `DLT_JUNIPER_ETHER` Plugin When Used as Decoder (affects `<= 4.5.3`)

> CVE-2026-102752 CVE ↗ STABLE
>
> `CVE-2026-102752`: Double free in tcpedit_dlt_cleanup in tcprewrite (CVSS 4.0, affects `<= 4.5.0`)

> CVE-2026-102753 CVE ↗ STABLE
>
> `CVE-2026-102753`: Heap-Buffer-Overflow in tcpreplay's get_layer4_v6 Function (affects `<= 4.5.4`)

> CVE-2026-102751 CVE ↗ STABLE
>
> `CVE-2026-102751`: NULL Pointer Dereference in `remove_settings` (affects `<= 4.5.3`)

> CVE-2026-102749 CVE ↗ STABLE

> `CVE-2026-102749` : Heap buffer overflow in tcprewrite fragroute ip6_opt module when inserting IPv6 extension headers (CVSS 8.4, affects `<= 4.5.3`)

> `CVE-2026-102746` CVE ↗ STABLE
>
> `CVE-2026-102746` : Heap Buffer Overflow via Negative Fragment/Segment Size in fragroute tcp_seg/ip_frag Modules (CVSS 8.4, affects `<= 4.5.4`)

> `CVE-2026-102747` CVE ↗ STABLE
>
> `CVE-2026-102747` : Out-of-Bounds Write in tcprewrite Fragroute Rules Parser on an Empty Rules File (affects `<= 4.5.4`)

WAS THIS USEFUL? 👍 👎

nfdump

Feedback ⓘ CVE-2026-102733 CVE ↗ STABLE

Netflow processing tools

`CVE-2026-102733`: Integer overflow in NetFlow v9 option template offset accumulation leads to heap OOB read (CVSS 7.5, affects `Version 1.7.8 and earlier`)

▾ **6 more releases in this issue** · 2026-07-22 → 2026-07-23

> CVE-2026-102694 CVE ↗ STABLE
>
> `CVE-2026-102694`: NULL pointer dereference in NetFlow v9 sub-template sequencer traversal (CVSS 7.5, affects `Version 1.7.8 and earlier`)

> CVE-2026-102691 CVE ↗ STABLE
>
> `CVE-2026-102691`: Integer overflow in PushArrayNextElement leads to array record header corruption in NBAR/ifvrf option data processing (CVSS 7.5, affects `<= 1.7.8`)

> CVE-2026-94558 CVE ↗ STABLE
>
> `CVE-2026-94558`: Legacy v1-layout file header ident field causes stack out-of-bounds read in nfdump (CVSS 5.5, affects `Version 1.7.8 and earlier`)

> CVE-2026-94557 CVE ↗ STABLE
>
> `CVE-2026-94557`: Heap out-of-bounds read parsing the interface/VRF name array record in nfdump (nfdump `-r`) (CVSS 5.5, affects `Version 1.7.8 and earlier`)

> CVE-2026-94559 CVE ↗ STABLE
>
> `CVE-2026-94559`: Malformed appendix block causes an excessive loop and log-flood denial of service in nfdump (CVSS 5.5, affects `Version 1.7.8 and earlier`)

> CVE-2026-94553 CVE ↗ STABLE
>
> `CVE-2026-94553`: Unauthenticated IPFIX withdraw-all leaves dangling template pointers, causing remote use-after-free in nfcapd (CVSS 7.5, affects `Version 1.7.8 and earlier 1.7.x`)

WAS THIS USEFUL? 👍 👎

tcpflow Feedback ⓘ CVE-2026-25061 CVE ↗

TCP/IP packet demultiplexer. Download from:

`CVE-2026-25061`: TIM Element OOB Write in wifipcap (CVSS 7.5, affects `<= 1.61`)

WAS THIS USEFUL? 👍 👎

Cilium hubble Feedback ⓘ CVE-2025-48056 CVE ↗

Hubble - Network, Service & Security Observability for Kubernetes using eBPF

`CVE-2025-48056`: Character injection in Hubble CLI (CVSS 5.3, affects `< v1.17.2`)

WAS THIS USEFUL? 👍 👎

ecapture Feedback ⓘ CVE-2024-24790 CVE ↗

Capture SSL/TLS plaintext with eBPF—no MITM proxy or custom CA installation. Supports Linux and Android on x86_64 and arm64.

`CVE-2024-24790`: ecapture docker images CVE-2024-24790 (CVSS 9.8, affects `>=1.22.0-0,<1.22.4`)

WAS THIS USEFUL? 👍 👎

Security Onion

Feedback ⓘ CVE-2020-27985 CVE ↗

Security Onion is a free and open platform for threat hunting, enterprise security monitoring, and log management. It includes our own interfaces for alerting, dashboards, hunting, PCAP, detections, and case management.

`CVE-2020-27985`: Security Onion v2 prior to 2.3.10 has an incorrect sudo configuration (CVSS 7.8, affects `< 2.3.10`)

WAS THIS USEFUL? 👍 👎

CLOUD & CONTAINER SECURITY

◆ Container & Image Security

Buildah

Feedback ⓘ CVE-2026-79705 CVE ↗ STABLE

A tool that facilitates building OCI images.

`CVE-2026-79705` : Local file overwrite by extracting a malicious tar archive (CVSS 6.1, affects `< 1.43.4`)

▾ **5 more releases in this issue** · 2021-07-15 → 2026-09-17

> CVE-2026-44517 CVE ↗ STABLE
>
> `CVE-2026-44517` : Build breakout using a Git repository or a tar archive fetched over the network (CVSS 6.3, affects `>= v1.38.1`)

> CVE-2024-11218 CVE ↗ STABLE
>
> `CVE-2024-11218` : Build breakout using malicious Containerfiles and concurrent builds (CVSS 8.6, affects `< 1.38.1`)

> CVE-2024-1753 CVE ↗ STABLE
>
> `CVE-2024-1753` : CVE-2024-1753 container escape at build time (CVSS 8.6, affects `1.35.0 through and including v1.24.0`)

> CVE-2022-27651 CVE ↗ STABLE
>
> `CVE-2022-27651` : Default inheritable capabilities for linux container should be empty (CVSS 6.8, affects `< 1.25.0`)

> CVE-2021-3602 CVE ↗ STABLE
>
> `CVE-2021-3602` : chroot isolation: environment value leakage to intermediate processes (CVSS 5.5, affects `1.21.2, 1.20.0, 1.19.8, 1.18.0, 1.17.1, 1.16.7`)

WAS THIS USEFUL? 👍 👎

kata-containers

Feedback ⓘ CVE-2026-77176 CVE ↗ STABLE

Kata Containers is an open source project and community working to build a standard implementation of lightweight Virtual Machines (VMs) that feel and perform like containers, but provide the workload isolation and security advantages of VMs. https://katacontainers.io/

`CVE-2026-77176` : generated policy allows mounting attacker-chosen guest paths to specific locations (CVSS 8.1, affects `<= 4.0.0`)

▾ **10 more releases in this issue** · 2025-09-23 → 2026-08-20

> CVE-2026-86072 CVE ↗ STABLE
>
> `CVE-2026-86072` : Untrusted pod annotation bind-mounts any host path into the Kata guest, bypassing the operator allowlist (affects `<= 3.32.0`)

> CVE-2026-93417 CVE ↗ STABLE
>
> `CVE-2026-93417` : Dragonball: missing length validation in virtio-blk allows guest-to-host VM escape (affects `>= 3.0.0`)

> CVE-2026-64676 CVE ↗ STABLE
>
> `CVE-2026-64676` : kata-agent mem-agent ttRPC methods are not subject to agent-policy enforcement, letting an untrusted host tamper with confidential-guest memory management (CVSS 5.7, affects `<= 3.31.0`)

> CVE-2026-50540 CVE ↗ STABLE
>
> `CVE-2026-50540` : Config Path Annotation Arbitrary File Loading (CVSS 9.6, affects `<=3.32.0`)

> CVE-2026-47243 CVE ↗ STABLE
>
> `CVE-2026-47243` : runtime-rs: Guest-root to host-root escape via virtiofs (affects `<= 3.30.0`)

> CVE-2026-44210 CVE ↗ STABLE
>
> `CVE-2026-44210` : VM Escape via virtiofsd Argument Injection through Default-Enabled Pod Annotations (CVSS 9.9, affects `<= 3.29.0`)

> CVE-2026-41326 CVE ↗ STABLE

> `CVE-2026-41326` : CopyFile Policy Subversion via Symlinks (CVSS 8.2, affects `v3.4.0 - v3.28.0`)

> `CVE-2026-24834` CVE ↗ STABLE
>
> `CVE-2026-24834` : Kata Container to Guest micro VM privilege escalation (CVSS 9.3, affects `<= 3.26.0`)

> `CVE-2026-24054` CVE ↗ STABLE
>
> `CVE-2026-24054` : Runtime: Host block device can be hotplugged to the VM if the container image is malformed or contains no layers (CVSS 10.0, affects `<= 3.25.0`)

> `CVE-2025-58354` CVE ↗ STABLE
>
> `CVE-2025-58354` : coco-tdx: malicious host can circumvent initdata verification (affects `<=v0.15.0`)

WAS THIS USEFUL? 👍 👎

Inspektor Gadget

Feedback ⓘ CVE-2026-53941 CVE ↗ STABLE

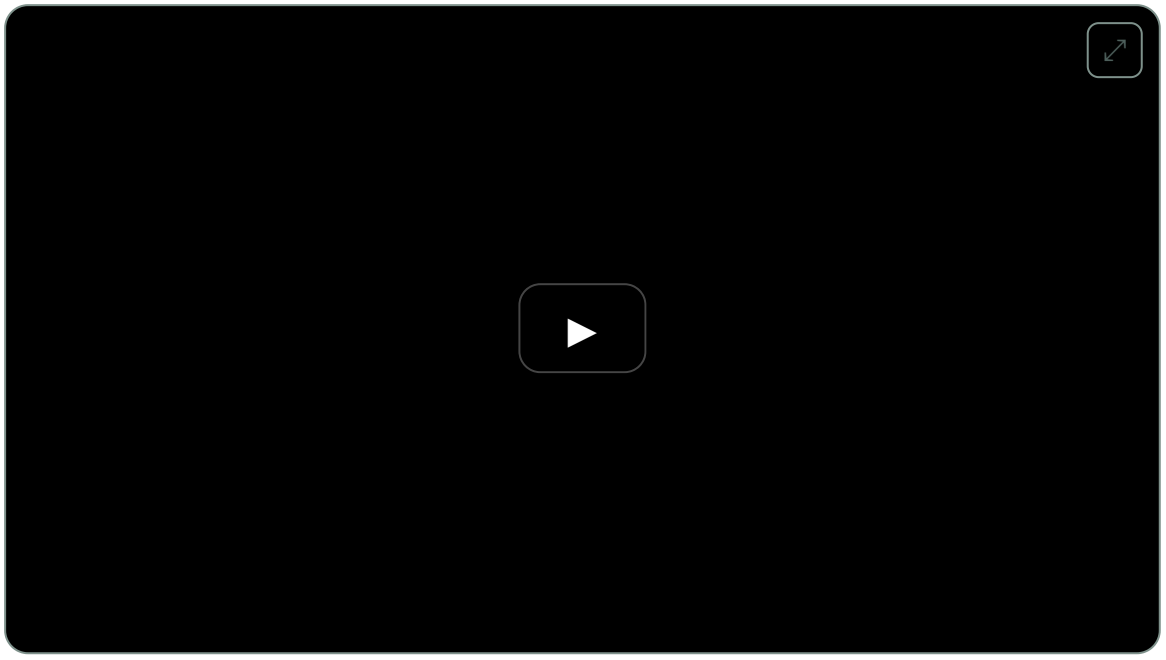
Inspektor Gadget is a set of tools and framework for data collection and system inspection on Kubernetes clusters and Linux hosts using eBPF

`CVE-2026-53941` : Uprobe gadgets: unprivileged container's `ld.so.cache` causes high CPU utilization and container startup DoS (affects `>= v0.27.0`)

▾ **4 more releases in this issue** · 2026-01-29 → 2026-06-16

> CVE-2026-44778 CVE ↗ STABLE
>
> `CVE-2026-44778` : Unprivileged container can crash USDT note parser via crafted ELF (no shipped gadget affected) (affects `>= v0.28.0`)

> CVE-2026-31890 CVE ↗ STABLE
>
> `CVE-2026-31890` : Tracing Denial of Service via Event Flooding (CVSS 5.5, affects `<v0.50.1`)

> CVE-2026-25996 CVE ↗ STABLE
>
> 
>
> `CVE-2026-25996` : Unsanitized ANSI Escape Sequences In `columns` Output Mode (CVSS 9.8, affects `<=v0.49.0`)

> CVE-2026-24905 CVE ↗ STABLE
>
> `CVE-2026-24905` : Command Injection in Makefile.build (CVSS 7.8, affects `<v0.51.1`)

WAS THIS USEFUL? 👍 👎

adm-controller

Feedback ⓘ CVE-2026-42541 CVE ↗ STABLE

Manage admission policies in your Kubernetes cluster with ease

`CVE-2026-42541`: RBAC Reconnaissance via unchecked can_i host capability call (CVSS 4.3, affects `v1.32.0`)

▾ **3 more releases in this issue** · 2025-01-30 → 2026-04-27

> CVE-2026-29773 CVE ↗ STABLE
>
> `CVE-2026-29773`: Cross-namespace data exfiltration via deprecated host callback binding (CVSS 4.3, affects `v1.6.0`)

> CVE-2025-24784 CVE ↗ STABLE
>
> `CVE-2025-24784`: Information leak via AdmissionPolicyGroup Resource (CVSS 4.3, affects `>= 1.17.0`)

> CVE-2025-24376 CVE ↗ STABLE
>
> `CVE-2025-24376`: AdmissionPolicy and AdmissionPolicyGroup policies can be used to alter PolicyReport resources (CVSS 6.5, affects `>= 1.7.0`)

WAS THIS USEFUL? 👍 👎

Anchore Grype

Feedback ⓘ CVE-2025-65965 CVE ↗

A vulnerability scanner for container images and filesystems

`CVE-2025-65965`: Credential disclosure vulnerability in Grype JSON output (affects `< 0.104.1`)

WAS THIS USEFUL? 👍 👎

Docker Compose

Feedback ⓘ CVE-2025-62725 CVE ↗

Define and run multi-container applications with Docker

`CVE-2025-62725`: Path Traversal via OCI Artifact Layer Annotations (affects `< v2.40.2`)

WAS THIS USEFUL? 👍 👎

cilium-cli

Feedback ⓘ CVE-2023-28114 CVE ↗

CLI to install, manage & troubleshoot Kubernetes clusters running Cilium

`CVE-2023-28114`: `cilium-cli` disables etcd authorization for clustermesh clusters (CVSS 4.8, affects `< 0.13.2`)

WAS THIS USEFUL? 👍 👎

◆ Runtime Security

Bubblewrap

Feedback ⓘ CVE-2026-87766 CVE ↗ STABLE

Low-level unprivileged sandboxing tool used by Flatpak and similar projects

`CVE-2026-87766`: CVE-2026-87766: Sandbox escape: symlink traversal via `/oldroot` allows writing files outside sandbox during setup (CVSS 8.8, affects `< 0.12.0`)

▾ 1 more release in this issue · 2026-04-23 → 2026-08-26

> CVE-2026-41163 CVE ↗ STABLE
>
> `CVE-2026-41163`: CVE-2026-41163: Privilege escalation in setuid mode via ptrace (CVSS 7.0, affects `0.11.0`)

WAS THIS USEFUL? 👍 👎

Cilium tetragon

Feedback ⓘ CVE-2026-65960 CVE ↗

Tetragon is an eBPF-based security observability and runtime enforcement tool for Kubernetes and cloud-native environments.

`CVE-2026-65960`: Unauthenticated Tetragon gRPC admin API accessible from hostNetwork pods (CVSS 8.8, affects `< v1.7.0`)

WAS THIS USEFUL? 👍 👎

Falco

Feedback ⓘ CVE-2022-26316 CVE ↗

Cloud Native Runtime Security

`CVE-2022-26316`: TOCTOU issue that could lead to rule bypass (affects `<0.31.1`)

WAS THIS USEFUL? 👍 👎

◆ Cloud Security Posture

Prowler

Feedback ⓘ CVE-2026-73262 CVE ↗ STABLE

This repo hosts Prowler OSS (CLI and Local Server). Prowler is the world's most widely used open-source cloud security platform that automates security and compliance across any cloud environment for Humans and AI Agents.

`CVE-2026-73262`: Stored XSS in HTML reports through unescaped cloud resource tags (CVSS 5.4, affects `<= 5.36.0`)

▾ **3 more releases in this issue** · 2026-06-22 → 2026-08-03

> CVE-2026-73263 CVE ↗ STABLE
>
> `CVE-2026-73263`: RCE on Prowler App workers via kubeconfig auth-provider cmd-path (CVSS 9.9, affects `< 5.36.0`)

> CVE-2026-73264 CVE ↗ STABLE
>
> `CVE-2026-73264`: Server-Side Request Forgery (SSRF) in Lighthouse Provider (CVSS 7.6, affects `<=5.33.0`)

> CVE-2026-59151 CVE ↗ STABLE
>
> `CVE-2026-59151`: SAML Domain Claiming Enables Cross-Tenant Account Takeover (CVSS 9.6, affects `<= 5.30.2`)

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ Threat Intelligence

World Monitor

Feedback ⓘ v2.11.7 NOTES ↗ RANK

Real-time global intelligence dashboard. AI-powered news aggregation, geopolitical monitoring, and infrastructure tracking in a unified situational awareness interface

> World Monitor's v2.11.7 release adds Arabic spoken answers to MCP, a Gemini CLI extension manifest, new procurement and food-price sources, expanded energy feeds, and removes the deprecated `/api/fwdstart` endpoint.

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

01 **Arabic language support for MCP spoken answers** NEW

70

MCP spoken answers now support Arabic by setting `spoken_language` to `"ar"`.

— Names exact config key and value to enable it v2.11.7

THINNER COVERAGE BELOW

02 **National energy feeds in fuel panel and country brief** NEW

55

Shows national energy feeds in the fuel panel and country brief, and adds Guatemala MEM fuel prices to the regional energy feeds.

— Names UI surfaces and a specific new source v2.11.7

03 **Removal of /api/fwdstart endpoint** BREAKING

55

The `/api/fwdstart` endpoint and the unused tech/finance variant FEEDS have been removed — any client calling `/api/fwdstart` will break.

— Names exact removed endpoint, no migration guidance v2.11.7

04 **New procurement feed sources for Georgia and Armenia** NEW

45

Adds EPADS, Georgia, and Armenia tender sources to the procurement feed.

— Names sources but no access path or format v2.11.7

05 **Expanded official food-price data** NEW

35

Adds 11 batch-2 official food-price sources and official local prices with weekly comparisons.

— Gives scope and count but no usage path v2.11.7

06 **Gemini CLI extension manifest** NEW 10

Adds a Gemini CLI extension manifest.

— Only named, no mechanism or usage detail given v2.11.7

└──▷ **BREAKING ON UPGRADE**

! The `/api/fwdstart` endpoint and the unused tech/finance variant FEEDS have been removed — any client calling `/api/fwdstart` will break.

WAS THIS USEFUL? 👍 👎

OpenCTI

Feedback ⓘ CVE-2026-104258 CVE ↗ STABLE

Open Cyber Threat Intelligence Platform

`CVE-2026-104258` : SSRF via webhook notifier allows authenticated users to reach internal services (CVSS 5.5, affects `<= 7.260722.0`)

▾ **20 more releases in this issue** · 2025-05-19 → 2026-10-22

> CVE-2026-114505 CVE ↗ STABLE
>
> `CVE-2026-114505` : Acceptance of GraphQL Operations via HTTP GET Method (affects `< 7.260722.0`)

> CVE-2026-104253 CVE ↗ STABLE
>
> `CVE-2026-104253` : Profile page reflects MFA secret in response (CVSS 5.2, affects `< 7.260715.0`)

> CVE-2026-63477 CVE ↗ STABLE
>
> `CVE-2026-63477` : Organization administrator can escalate to global administrator via unvalidated `grantable_groups` write (incomplete fix of CVE-2026-44730) (CVSS 8.8, affects `< 7.260624.0`)

> CVE-2026-76823 CVE ↗ STABLE
>
> `CVE-2026-76823` : Elasticsearch credentials disclosed to connector tokens through logsWorkerConfig (affects `< 7.260706.0`)

> CVE-2026-76822 CVE ↗ STABLE
>
> `CVE-2026-76822` : Authorisation vulnerability in case creation (CVSS 4.3, affects `< 7.260701.0`)

> CVE-2026-76820 CVE ↗ STABLE
>
> `CVE-2026-76820` : Synchronizer SSRF: stream fetch has no URL validation (CVSS 7.7, affects `< 7.260701.0`)

> CVE-2026-76821 CVE ↗ STABLE
>
> `CVE-2026-76821` : User-Controlled ReDoS in JSON Ingestion Mapper (affects `< 7.260706.0`)

CVE-2026-104840 CVE ↗ STABLE

`CVE-2026-104840` : No rate limiting on authentication endpoint allows credential brute-forcing (affects `< 7.260428.0`)

CVE-2026-102892 CVE ↗ STABLE

`CVE-2026-102892` : TAXII Public Collection Incorrect Authorization & Data Leak (CVSS 5.3, affects `< 7.260416.0`)

CVE-2026-35211 CVE ↗ STABLE

`CVE-2026-35211` : Elasticsearch Painless Script Injection via GraphQL `script` filter operator allows authenticated user to exfiltrate data and cause DoS (CVSS 6.5, affects `< 7.260401.0`)

CVE-2026-35210 CVE ↗ STABLE

`CVE-2026-35210` : Authorization Bypass via `synchronized-upsert` HTTP Header Injection (CVSS 7.1, affects `< 7.260326.0`)

CVE-2026-35212 CVE ↗ STABLE

`CVE-2026-35212` : XSS in the rendering of email-message observable body data (CVSS 6.1, affects `< 7.260227.0`)

CVE-2026-44730 CVE ↗ STABLE

`CVE-2026-44730` : Privilege escalation via graphQL API abusable by organization admins, due to incorrect ACL on userEdit relationAdd (CVSS 7.2, affects `< 6.9.7`)

CVE-2026-27960 CVE ↗ STABLE

`CVE-2026-27960` : Priviledge escalation and unauthenticated access using default admin (CVSS 9.8, affects `>= 6.6.0, < 6.9.13`)

CVE-2026-39980 CVE ↗ STABLE

`CVE-2026-39980` : RCE via notifier template (CVSS 9.1, affects `< 6.9.5`)

CVE-2026-21886 CVE ↗ STABLE

`CVE-2026-21886` : GraphQL Mutations Allow Deletion of Unrelated Entities (CVSS 6.5, affects `< 6.9.1`)

CVE-2026-21887 CVE ↗ STABLE

`CVE-2026-21887` : Semi-Blind SSRF via Unvalidated External URL in Data Ingestion Feature (CVSS 7.7, affects `< 6.8.16`)

CVE-2025-61782 CVE ↗ STABLE

`CVE-2025-61782` : Open Redirect in OpenCTI's SAML Authentication Flow (CVSS 5.4, affects `< 6.8.3`)

CVE-2025-61781 CVE ↗ STABLE

`CVE-2025-61781` : GraphQL IDOR allows authenticated user to delete workspace content of other users (CVSS 7.1, affects `< 6.8.1`)

CVE-2025-26621 CVE ↗ STABLE

`CVE-2025-26621` : Denial of Service through web hook (CVSS 7.6, affects `< 6.5.2`)

WAS THIS USEFUL? 👍 👎

Lookyloo

Feedback ⓘ CVE-2026-66913 CVE ↗ STABLE

Lookyloo is a web interface that allows users to capture a website page and then display a tree of domains that call each other.

`CVE-2026-66913` : Unauthenticated Upload Decompression Resource Exhaustion (DoS) in `/json/upload` and `/submit_capture` (affects `<1.40.1`)

▾ **5 more releases in this issue** · 2025-11-18 → 2026-07-28

> CVE-2026-55835 CVE ↗ STABLE
>
> `CVE-2026-55835` : Potential sub-system DoS due to parameter missmatch in notification (affects `<=1.39.3`)

> CVE-2025-66460 CVE ↗ STABLE
>
> `CVE-2025-66460` : XSS due to lack of escaping in HTML elements passed to Datatables (CVSS 6.1, affects `<=1.35.2`)

> CVE-2025-66459 CVE ↗ STABLE
>
> `CVE-2025-66459` : XSS due to unescaped error message passed to innerHTML (CVSS 6.1, affects `<=1.35.2`)

> CVE-2025-66458 CVE ↗ STABLE
>
> `CVE-2025-66458` : Multiple XSS due to unsafe use of f-strings in Markup (CVSS 6.1, affects `<=1.35.2`)

> CVE-2025-65095 CVE ↗ STABLE
>
> `CVE-2025-65095` : HTML injection due to improper user input sanitization (affects `<=1.35.0`)

WAS THIS USEFUL? 👍 👎

Yeti

Feedback ⓘ CVE-2026-63502 CVE ↗ STABLE

Your Everyday Threat Intelligence

`CVE-2026-63502` : Path traversal in ExportTask name allows authenticated arbitrary file read and write (CVSS 8.3, affects `<= 2.5.0`)

▾ **5 more releases in this issue** · 2024-09-10 → 2026-07-01

> CVE-2026-63489 CVE ↗ STABLE
>
> `CVE-2026-63489` : Authenticated AQL injection via unvalidated search sorting and filter_aliases parameters (CVSS 7.6, affects `<= 2.5.0`)

> CVE-2026-63482 CVE ↗ STABLE
>
> `CVE-2026-63482` : Unauthenticated Access to Full Audit Timeline Discloses All Threat Intelligence Data (CVSS 7.5, affects `commit 1f5b1261b1ae862423b1226e3447182e7df12dcf`)

> CVE-2024-46508 CVE ↗ STABLE
>
> `CVE-2024-46508` : Insecure default secret key specified in config (CVSS 7.5, affects `- 2.3.3`)

> CVE-2024-46507 CVE ↗ STABLE
>
> `CVE-2024-46507` : Server Side Template Injection in Exports (CVSS 8.1, affects `- 2.1.12`)

> CVE-2024-45412 CVE ↗ STABLE
>
> `CVE-2024-45412` : CVE-2024-45412: Potential Denial of Service due to the One Milion Unicode characters attack (CVSS 4.3, affects `- 2.1.10`)

WAS THIS USEFUL? 👍 👎

MISP

Feedback ⓘ CVE-2026-44381 CVE ↗ STABLE

MISP (core software) - Open Source Threat Intelligence and Sharing Platform

`CVE-2026-44381`: MISP - SQL injection via unvalidated ordering parameters in event and shadow attribute listings (CVSS 5.3, affects `< 2.5.37`)

▾ **3 more releases in this issue** · 2026-04-08 → 2026-04-29

> CVE-2026-44380 CVE ↗ STABLE
>
> `CVE-2026-44380`: MISP - Improper access control in auth key reset allows privilege escalation to site administrator (CVSS 7.2, affects `< 2.5.37`)

> CVE-2026-44379 CVE ↗ STABLE
>
> `CVE-2026-44379`: Improper UUID validation in MISP Collections (CVSS 5.3, affects `< 2.5.37`)

> CVE-2026-39962 CVE ↗ STABLE
>
> `CVE-2026-39962`: LDAP injection in MISP ApacheAuthenticate when using a user-controlled Apache environment variable (CVSS 9.6, affects `2.5.35`)

WAS THIS USEFUL? 👍 👎

ransomlook

Feedback ⓘ CVE-2026-40584 CVE ↗

Yet another Ransomware gang tracker

`CVE-2026-40584`: RansomLook - Improper Filtering of Private Location Entries in API Endpoints Leads to Information Exposure (CVSS 7.5, affects `< 1.9.0`)

WAS THIS USEFUL? 👍 👎

◆ Endpoint Security (EDR/XDR)

clamui

Feedback ⓘ v0.5.0 NOTES ↗ RANK

ClamAV Desktop application (GUI)

> ClamUI v0.5.0 rebuilds the desktop app on a Rust/Tauri core and adds a Network view with VirusTotal IP lookups, read-only firewall auditing, and safer configuration recovery tooling.

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

01 **Save & Apply configuration recovery flow** NEW 80

A new Save & Apply recovery flow exposes a See Configuration panel showing the exact native ClamAV configuration attempted for each full target path, with separate copy actions for manual recovery after partial or failed writes.

After a failed configuration write, inspect exactly what ClamAV configuration ClamUI attempted before manually editing the file on disk.

📍 In ClamUI, open Preferences and trigger Save & Apply. If a write fails, click See Configuration to view the exact native ClamAV configuration attempted for each full target path, then use the separate copy action to paste it into the file manually.

— Includes exact UI steps and a runnable recovery workflow v0.5.0

02 **Network view with listener snapshots and VirusTotal lookups** NEW 77

A new Network view shows current TCP/UDP listeners and connections with filtering, copying, and permission-aware process attribution. It can open VirusTotal IP reports in the browser after explicit confirmation for accepted public IP addresses, without sending port or process information.

Review active TCP/UDP listeners and attribute them to processes to spot unexpected network exposure on a host.

📍 In ClamUI, open the Network view to see current TCP/UDP listeners and connections. Use the filter controls to narrow results, and copy rows of interest for reporting.

— Describes mechanism and privacy scope plus a usage walkthrough v0.5.0

03 **Native packaging across Debian, AppImage, Flatpak, RPM** NEW 70

Adds native Debian application and helper packages, an x86_64 AppImage with `.zsync` metadata, Flatpak bundles for `x86_64` and `aarch64`, and helper-only Fedora RPM support for `x86_64` and `aarch64` with protected-preference recovery requiring the matching signed RPM and detached `.rpm.asc` asset for the host architecture.

— Names exact package formats and architectures supported v0.5.0

04 **Rust/Tauri rewrite of the desktop core** BREAKING 65

ClamUI now uses a headless Rust core with a Tauri 2/WebKitGTK and React desktop, replacing the Python/PyGObject runtime while retaining existing XDG JSON and SQLite data layouts, scanning, history, quarantine, profiles, exports, clipboard actions, tray controls, and file-manager integration.

— Explains before/after architecture but no migration action v0.5.0

THINNER COVERAGE BELOW

05 **Read-only firewall audit across UFW, firewalld, nftables** NEW 55

ClamUI's firewall audit now inventories UFW, firewalld, nftables, IPv4/IPv6 iptables, and supported management interfaces in a read-only, non-interactive view.

— Names surfaces covered but no navigation path given v0.5.0

06 **Helper trust distinction with Polkit-confirmed install** NEW 45

ClamUI now distinguishes missing helpers from untrusted helpers and, on supported hosts, can offer a Polkit-confirmed installation of a verified matching signed helper package.

— Explains behaviour but no concrete command or path v0.5.0

07 **Nine active UI locales** NEW 30

The interface now supports nine active locales: German, English, Spanish, French, Hungarian, Italian, Norwegian Bokmål, Brazilian Portuguese, and Simplified Chinese.

— Simple list with no further mechanism v0.5.0

WAS THIS USEFUL? 👍 👎

osctrl Feedback ⓘ CVE-2026-28280 CVE ↗ STABLE

Fast and efficient osquery management

`CVE-2026-28280`: Stored Cross-Site Scripting (XSS) in On-Demand Query List (CVSS 6.1, affects `< 0.5.0`)

▾ **1 more release in this issue** · 2026-02-26

> CVE-2026-28279 CVE ↗ STABLE
>
> `CVE-2026-28279`: OS Command Injection via Environment Configuration in `osctrl-admin` (CVSS 7.3, affects `< 0.5.0`)

WAS THIS USEFUL?  

Sophos Central

Feedback ⓘ October 12, 2026 NOTES ↗ RANK

Sophos Central is a cloud-based management console for Sophos security products, letting administrators deploy, monitor, and manage endpoint, firewall, email, and server protection from one place.

> Sophos Central's October release adds visibility into AI agents and non-human identities created in Microsoft Entra, shows per-policy application status on endpoint details pages, and expands Protected Browser with phishing protection, standalone DNS protection, an MSI installer, and data boundary controls.

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

01 **Non-human identity visibility for Microsoft Entra** NEW

57

Sophos ITDR now surfaces AI agents, blueprints, and apps created by Microsoft Entra — including ownership and sponsorship details — under Non-Human Identities in the Directory.

— Names the UI location but not mechanism behind detection October 12, 2026

02 **Protected Browser phishing, DNS, and deployment updates**

IMPROVED

57

Protected Browser adds Phishing Protection to guard organizational credentials, direct DNS Protection that works independent of endpoint or network policies, a new MSI installer for Windows deployment, and more flexible data boundary controls.

— Names four distinct additions but no config or command specifics October 12, 2026

03 **Policy application status on endpoint details** NEW

48

The Policies tab of an endpoint's details page now shows the application status for each policy, including confirmation that updated policies (such as exclusions) have been applied.

— Clear UI path but no mechanism detail beyond that October 12, 2026

WAS THIS USEFUL? 👍 👎

◆ SIEM

Wazuh

Feedback ⓘ CVE-2026-74041 CVE ↗ STABLE

Wazuh - The Open Source Security Platform. Unified XDR and SIEM protection for endpoints and cloud workloads.

`CVE-2026-74041` : Case-sensitivity mismatch bypasses remote-command validation, allowing command execution as root (CVSS 7.2, affects `>= 4.14.3`)

▾ **18 more releases in this issue** · 2026-08-18 → 2026-10-13

> CVE-2026-74033 CVE ↗ STABLE
>
> `CVE-2026-74033` : Missing destination-path validation in CDB list cluster-callable handlers allows arbitrary file read/delete on the manager (CVSS 6.1, affects `>= 4.1.1`)

> CVE-2026-74037 CVE ↗ STABLE
>
> ▶ Watch video
>
> `CVE-2026-74037` : Improper session invalidation in check_token: revoking a run_as user's administrator grant does not invalidate their token, enabling permanent self-re-grant of administrator (CVSS 7.2, affects `>= 4.0.0, <= 4.14.7`)

> CVE-2026-74045 CVE ↗ STABLE
>
> ▶ Watch video
>
> `CVE-2026-74045` : Heap buffer overflow in wazuh-analysisd fim_generate_alert() lets an enrolled agent corrupt manager heap memory and terminate the analysis engine (CVSS 7.1, affects `>= 3.12.0`)

> CVE-2026-74035 CVE ↗ STABLE
>
> `CVE-2026-74035` : An empty password bypasses both the password policy and the reserved user guard in `security.update_user`, allowing a delegated user administrator to take over the `wazuh` superuser account (CVSS 7.2, affects `>= 4.6.0`)

> CVE-2026-93346 CVE ↗ STABLE

`CVE-2026-93346` : API brute-force protection is still bypassable by concurrent login requests, the `asyncio.Lock` fix for GHSA-m2mr-xhhv-jx58 serializes the counter but does not close the check-then-count race (CVSS 5.3, affects `>= 4.0.0`)

`CVE-2026-74034` CVE ↗ STABLE

`CVE-2026-74034` : Arbitrary file read as root via agent-injected upgrade_custom command (CVSS 7.5, affects `>= 4.1.0`)

`CVE-2026-74032` CVE ↗ STABLE

`CVE-2026-74032` : RBAC Authorization Bypass in Wazuh API (CVSS 4.3, affects `>= 4.0.0`)

`CVE-2026-74047` CVE ↗ STABLE

`CVE-2026-74047` : authd.pass disclosed to low-privileged users through the per-agent active configuration endpoint (CVSS 6.5, affects `>= 4.0.0`)

`CVE-2026-74040` CVE ↗ STABLE

`CVE-2026-74040` : Cluster worker can overwrite arbitrary master files (incl. ossec.conf) → root RCE on manager and every agent — bypass of #36296 excluded_files guard + missing extra_valid enforcement (CVSS 9.1, affects `>= 3.9.0`)

`CVE-2026-74030` CVE ↗ STABLE

`CVE-2026-74030` : SCA YAML alias expansion causes memory exhaustion (CVSS 4.9, affects `>= 3.9.0`)

`CVE-2026-62365` CVE ↗ STABLE

`CVE-2026-62365` : Heap Buffer Overflow in DecodeWinevt() join_data Accumulation via Crafted EventChannel XML (CVSS 5.3, affects `>= 3.8.0`)

`CVE-2026-61811` CVE ↗ STABLE

`CVE-2026-61811` : Unbounded Recursion in os_xml _getattributes() Causes analysisd Worker Thread Stack Exhaustion (CVSS 6.5, affects `>= 3.8.0`)

`CVE-2026-61783` CVE ↗ STABLE

`CVE-2026-61783` : RBAC permission-effect check in mask_sensitive_config allows low-privilege users to read cluster.key (CVSS 6.5, affects `>= 4.14.0`)

`CVE-2026-54084` CVE ↗ STABLE

`CVE-2026-54084` : Wazuh agent enrollment NULL pointer dereference via malformed manager response (CVSS 5.3, affects `>= 4.0.0`)

`CVE-2026-54085` CVE ↗ STABLE

`CVE-2026-54085` : Missing input validation in multiple active response scripts allows argument injection (CVSS 5.9, affects `>= 4.2.0`)

`CVE-2026-61800` CVE ↗ STABLE

`CVE-2026-61800` : Incomplete fix for CVE-2026-30893: missing directory confinement in cluster worker file sync allows arbitrary file write under `/var`/ossec on worker nodes (CVSS 8.0, affects `>= 4.4.0`)

`CVE-2026-74046` CVE ↗ STABLE

`CVE-2026-74046` : zlib decompression bomb in cluster archive processing lets authenticated peer exhaust wazuh-clusterd memory (CVSS 4.9, affects `>= 4.4.0`)

`CVE-2026-74039` CVE ↗ STABLE

`CVE-2026-74039` : Authenticated denial-of-service of the Wazuh API via `POST /security/user/authenticate/run_as` (CVSS 6.5, affects `>= 4.0.0, <= 5.0.0-beta2`)

WAS THIS USEFUL? 👍 👎

graylog2-server

Feedback ⓘ CVE-2026-69190 CVE ↗ STABLE

Free and open log management

`CVE-2026-69190` : Manager-to-Owner privilege escalation on saved searches and dashboards (CVSS 6.3, affects `>= 6.3.0`)

▾ **10 more releases in this issue** · 2023-07-05 → 2026-07-07

> CVE-2026-55425 CVE ↗ STABLE
>
> `CVE-2026-55425` : System Catalog titles endpoint can be used to retrieve values of protected database fields (CVSS 5.0, affects `7.1.0 - 7.1.3`)

> CVE-2026-55841 CVE ↗ STABLE
>
> `CVE-2026-55841` : Fortigate syslog message parser can be exploited to modify or delete fields from the original message (CVSS 7.5, affects `< 6.3.12, < 7.0.7, < 7.1.2`)

> CVE-2026-55867 CVE ↗ STABLE
>
> `CVE-2026-55867` : Graylog token revocation endpoint allows authenticated users to delete other users' access tokens (affects `>=6.2.0`)

> CVE-2025-53106 CVE ↗ STABLE
>
> `CVE-2025-53106` : Privilege escalation through API tokens (CVSS 8.8, affects `>=6.2.0`)

> CVE-2025-46827 CVE ↗ STABLE
>
> `CVE-2025-46827` : Session Takeover via Insufficient HTML Sanitization (CVSS 8.0, affects `<= 6.0.13, <= 6.1.9`)

> CVE-2025-30373 CVE ↗ STABLE
>
> `CVE-2025-30373` : Authenticated HTTP inputs do ingest message even if Authorization header is missing or has wrong value (CVSS 6.5, affects `>= 6.1.0`)

> CVE-2024-52506 CVE ↗ STABLE
>
> `CVE-2024-52506` : Concurrent PDF report rendering can leak other users' reports (CVSS 6.5, affects `6.1.0, 6.1.1`)

CVE-2024-24823 CVE ↗ STABLE

`CVE-2024-24823` : Session fixation vulnerability through cookie injection (CVSS 5.7, affects `4.3.0 - 5.2.3`)

CVE-2024-24824 CVE ↗ STABLE

`CVE-2024-24824` : Instantiation of arbitrary classes triggered by API request (CVSS 8.8, affects `>= 2.0.0, <=5.2.3`)

CVE-2023-41045 CVE ↗ STABLE

.

`CVE-2023-41045` : Insecure source port usage for DNS queries (CVSS 5.3, affects `<= 5.1.0`)

WAS THIS USEFUL? 👍 👎

ClickHouse Feedback ⓘ CVE-2025-1385 CVE ↗ STABLE

ClickHouse® is a real-time analytics database management system

`CVE-2025-1385` : CVE-2025-1385- Fail input validation in clickhouse-library-bridge API could lead to RCE (affects `< 24.3.18.6`)

▾ **2 more releases in this issue** · 2023-12-18 → 2025-03-20

CVE-2024-6873 CVE ↗ STABLE

`CVE-2024-6873` : Specially crafted request could caused undefined behavior which may lead to Remote Code Execution. (CVSS 8.1, affects `< v24.5.1.1763`)

CVE-2023-47118 CVE ↗ STABLE

`CVE-2023-47118` : Heap buffer overflow in T64 codec decompression (CVSS 7.0, affects `< v23.10.2.13`)

WAS THIS USEFUL? 👍 👎

Sumo Logic

Feedback

Apps, Collection, and Automation Service Integrations - October Release (2026-10-30)

BLOG ↗

Sumo Logic is a cloud-native machine data analytics platform that collects, searches, and analyzes logs and metrics for security monitoring, troubleshooting, and operational insights.

Sumo Logic adds user metrics dashboards to the GitHub Copilot app and migrates its C2C source to current endpoints with user metrics support.

Sumo Logic's GitHub Copilot app (v1.0.1) now adds user metrics dashboards and reflects the updated data schema.

Sumo Logic's GitHub Copilot C2C source (v2.0.0) migrates from legacy endpoints and adds user metrics support.

UPDATED INTEGRATION ZeroFox V2

UPDATED INTEGRATION CrowdStrike Falcon

UPDATED INTEGRATION Atlassian Jira Cloud

UPDATED INTEGRATION Atlassian Jira V2

UPDATED INTEGRATION ThreatConnect V3

WAS THIS USEFUL? 👍 👎

◆ Detection Engineering

Thinkst OpenCanary

Feedback ⓘ CVE-2026-16551 CVE ↗

STABLE

Modular and decentralised honeypot

`CVE-2026-16551`: Denial-of-Service in MongoDB module (affects `0.9.8`)

▾ **1 more release in this issue** · 2024-10-14 → 2026-07-22

> CVE-2024-48911 CVE ↗ STABLE
>
> `CVE-2024-48911`: OpenCanary Executes Commands From Potentially Writable Config File (CVSS 7.8, affects `< 0.9.5`)

WAS THIS USEFUL? 👍 👎

rsigma

Feedback ⓘ v0.26.0 NOTES ↗ RANK

A complete Sigma detection engineering toolkit: parser, linter, evaluator, correlation engine, conversion framework, streaming daemon, MCP and LSP servers

> rsigma v0.26.0 adds strict rule-load validation with a new parse-error gauge, and reshapes how EVTX records are presented to rules to match Windows' native rendering more closely.

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

01 EVTX record shape now matches Windows rendering

BREAKING

85

`engine eval -e @file.evtx` now passes EVTX records to rules closer to how Windows renders them: GUIDs are lowercase and wrapped in braces (e.g. `{54849625-5478-4994-a5ba-3e3b0328c30d}`), unset `Data`, `Binary`, and optional `System` fields are omitted instead of present-and-empty, consecutive `Data` elements with the same name collapse into an array with a numbered suffix for later duplicates (e.g. `LogonGuid_1`), and bool fields with values other than 0 and 1 now arrive as integers instead of `true`. Rules matching whole unbracketed GUIDs, empty field values, or boolean truthiness on non-0/1 values must be updated.

— Concrete before/after examples but no migration command given. v0.26.0

02 Strict rule-load validation and parse-error gauge

BREAKING

84

A new `--strict-rules` flag (config key `daemon.engine.strict_rules`) makes rsigma refuse a rule load where every rule fails to parse, exiting with code `2` at startup or keeping the current rules on reload; a new `rsigma_rule_parse_errors` gauge counts skipped rules during partial-failure loads. `RuntimeEngine::load_rules` now returns an error when every rule fails to parse or when any parse error occurs after RuntimeEngine::set_strict_rules(true), and `EngineStats` gains a new `parse_errors` field that struct-literal callers must set.

— Names flag, config key, exit code, gauge, and API changes precisely. v0.26.0

└──▷ **BREAKING ON UPGRADE**

! `RuntimeEngine::load_rules` now returns an error when every rule fails to parse, or when any parse error occurs after RuntimeEngine::set_strict_rules(true). Code that relied on a silent empty engine must handle the new error path.

! `EngineStats` gains a new `parse_errors` field; code that constructs `EngineStats` with a struct literal must set it.

! EVTX bool fields with values other than 0 and 1 now reach rules as integers instead of `true`.

! EVTX GUIDs are now lowercase and in braces (e.g. `{54849625-5478-4994-a5ba-3e3b0328c30d}`); rules that match a whole GUID without braces must be updated.

! Unset `Data`, `Binary`, and optional `System` EVTX fields are now omitted rather than present and empty; rules that match on empty values for these fields will no longer fire.

! Consecutive `Data` elements with the same name in EVTX records now become a single array field; a later occurrence gets a numbered suffix (e.g. `LogonGuid_1`).

WAS THIS USEFUL? 👍 👎

◆ SOAR

Tines Feedback ⓘ

Set default fallback models for your whole tenant (2026-11-02) BLOG ↗ RANK

Tines lets teams put AI to work across their most sensitive systems, data, and processes, with the security and governance to do it safely.

> Tines now lets tenant owners configure automatic fallback models for their default AI models, improving resilience when a primary model is unavailable.

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

01 **Tenant-wide fallback models for default AI** NEW 55

Tenant owners can set an ordered list of up to five fallback models for the tenant's default smart and fast AI models, so requests automatically fall back if the primary model is unavailable.



— Explains mechanism and limit but no exact UI path or config key

Set default fallback models for your wh…

WAS THIS USEFUL? 👍 👎

◆ Endpoint Management (UEM/RMM)

Jamf Pro

Feedback ⓘ announced · Oct 30, 2026 BLOG ↗ RANK

Jamf Pro, enterprise-level Mobile Device Management (MDM) software, manages and secures Apple devices with advanced tools and integrations.

> Jamf Pro introduces declarative, vendor-direct deployment and auto-updating of non-App Store Mac apps through a new App Lifecycle Management Engine (ALME), removing the need for manual repackaging.

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

01 Declarative Mac app deployment via ALM Engine NEW

90

Jamf Pro can deploy and automatically update non-App Store Mac apps by declaring them in blueprints through the App Lifecycle Management Engine (ALME), eliminating manual repackaging for third-party apps. Apps are downloaded directly from vendors over TLS with checksum and signature verification before install. The ALME binary ships inside Self Service+ 2.33.0 at `/Applications/Self Service+.app/Contents/MacOS/ALME.app` (bundle ID `com.jamf.alme`), launched via `/Library/LaunchDaemons/com.jamf.alme.plist` and `/Library/LaunchAgents/com.jamf.alme.agent.plist`, and signed by JAMF Software team ID `483DWKW443`.

Add a third-party Mac app to a blueprint so ALME installs and keeps it current automatically, without repackaging.

> 📍 In Jamf Pro, go to Blueprints › select a blueprint › App Catalog › search for the app › add it to the blueprint. Set a maintenance window to control when downloads occur, then deploy.

— Names blueprints, binary paths, bundle ID, team ID, and gives UI steps.

launch-20261030-0de4af72

02 Automatic Full Disk Access for ALME via PPPC profile NEW

60

Jamf Pro 11.33.0 automatically delivers Full Disk Access for ALME via a Privacy Preferences Policy Control (PPPC) profile for Self Service+, enabling updates to apps stored in Desktop, Documents, and Downloads folders.

— Names exact mechanism and version but no manual configuration steps.

launch-20261030-0de4af72

THINNER COVERAGE BELOW

03 **Maintenance windows for ALME app updates** NEW 45

Admins can control when app updates download and install using maintenance windows, with default notifications alerting users when an update is waiting for an app to close.

— Describes behavior but no config key or exact setup steps. launch-20261030-0de4af72

WAS THIS USEFUL? 👍 👎

Fleet

Feedback ⓘ CVE-2026-103264 CVE ↗ STABLE

Open device management

`CVE-2026-103264`: Unauthenticated iOS/iPadOS device API access via non-secret host identifiers (CVSS 9.1, affects `< 4.87.0`)

▾ **11 more releases in this issue** · 2026-03-27 → 2026-09-15

> CVE-2026-48786 CVE ↗ STABLE
>
> `CVE-2026-48786`: Observer-class users can view team enroll secrets and credential-bearing configuration via target search endpoint (CVSS 6.5, affects `< 4.87.0`)

> CVE-2026-54245 CVE ↗ STABLE
>
> `CVE-2026-54245`: SQL injection in Okta conditional access policy evaluation allows an enrolled host to compromise the Fleet database (affects `< 4.86.2`)

> CVE-2026-41262 CVE ↗ STABLE
>
> `CVE-2026-41262`: Cross-Team Policy Data Exposure via Global Policy Read Endpoint (CVSS 4.3, affects `< 4.85.0`)

> CVE-2026-46371 CVE ↗ STABLE
>
> `CVE-2026-46371`: Observer-level enrollment secret extraction via ORDER BY oracle on Apple MDM commands endpoint (CVSS 6.5, affects `<= 4.84.1`)

> CVE-2026-46356 CVE ↗ STABLE
>
> `CVE-2026-46356`: IP spoofing allows bypassing API rate limiting (CVSS 7.5, affects `< 4.80.1`)

> CVE-2026-26191 CVE ↗ STABLE
>
> `CVE-2026-26191`: OS command injection in software packages (CVSS 9.8, affects `< 4.81.1`)

> CVE-2026-34391 CVE ↗ STABLE
>
> `CVE-2026-34391`: Windows MDM cross-device command disclosure (CVSS 7.5, affects `< 4.81.1`)

CVE-2026-34388 CVE ↗ STABLE

`CVE-2026-34388`: Denial of Service via unhandled gRPC log type in launcher endpoint (CVSS 7.5, affects `< 4.81.0`)

CVE-2026-29180 CVE ↗ STABLE

`CVE-2026-29180`: Team maintainer can transfer hosts from any team via missing source team authorization (CVSS 8.8, affects `< 4.81.1`)

CVE-2026-34386 CVE ↗ STABLE

`CVE-2026-34386`: SQL injection in MDM bootstrap package by authenticated team or global admin (CVSS 8.8, affects `< 4.81.0`)

CVE-2026-34385 CVE ↗ STABLE

`CVE-2026-34385`: Second-order SQL injection in Fleet's Apple MDM profile delivery can compromise the database (CVSS 8.1, affects `< 4.81.0`)

WAS THIS USEFUL? 👍 👎

Sophos Mobile

Feedback ⓘ 2026.44Released on November 2, 2026

NOTES ↗

Sophos Mobile is an enterprise mobile device management (MDM) and unified endpoint management tool that secures, configures, and monitors smartphones and tablets against threats and policy violations.

Sophos Mobile adds Android Enterprise restrict-assist and kiosk Home button settings, EAS proxy version display, and removes the Intune App Protection Policy integration.

Restrict assist content sharing with privileged apps (such as Google Assistant) via the 'Allow assist content sharing with privileged apps' setting in Android Enterprise Restrictions configuration.

Control kiosk navigation with the `Allow Home button` setting in Android Enterprise Kiosk mode configuration for use with custom launchers.

View the EAS proxy version on the EAS proxy tab of the Sophos setup page for troubleshooting.

The Microsoft Intune App Protection Policy integration has been removed; manage Intune App Protection Policies directly in the Microsoft Intune admin center.

UPDATED SUPPORTED PLATFORM Android 17 ADB compliance rule restriction

└──▷ BREAKING ON UPGRADE

! The Microsoft Intune App Protection Policy integration has been removed from Sophos Mobile. Admins who used it to view or edit Intune App Protection Policies must now manage those policies directly in the Microsoft Intune admin center.

WAS THIS USEFUL? 👍 👎

◆ Vulnerability Management

OpenCVE

Feedback ⓘ CVE-2026-92764 CVE ↗ STABLE

Vulnerability Intelligence Platform

`CVE-2026-92764` : Organization API ignores org-scoped token on `/api` /organizations (CVSS 4.3, affects `≥ 2.4.0, < 3.1.0`)

▾ 1 more release in this issue · 2026-06-25 → 2026-09-19

> CVE-2026-62282 CVE ↗ STABLE
>
> `CVE-2026-62282` : Server-Side Request Forgery (SSRF) in notifications (CVSS 6.5, affects `< 3.0.0`)

WAS THIS USEFUL? 👍 👎

◆ Attack Surface & Exposure Management

syzkaller

Feedback ⓘ changes since 2026-10-30 CODE ↗

syzkaller is an unsupervised coverage-guided kernel fuzzer

syzkaller's executor cover filter now uses a hash table, removing the 8-region PC limit; aflow separates impact analysis from root cause.

syzkaller's executor now uses an open-addressed hash table instead of a fixed 3-level region table in `cover_filter.h`, removing the previous limit of 8 distinct 1 GB PC regions.

syzkaller's `aflow` package now separates impact analysis from root cause analysis.

NEW DETECTION Binder generic netlink report descriptions

UPDATED DETECTION Binder and binderfs syscall descriptions

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Identity & Access Management

authentik

Feedback ⓘ CVE-2026-94613 CVE ↗ STABLE

The authentication glue you need.

`CVE-2026-94613`: Denial of Service via Malformed SAML Messages (CVSS 7.5, affects `<= 2026.8.1`)

▾ **23 more releases in this issue** · 2024-11-21 → 2026-09-09

> CVE-2026-94611 CVE ↗ STABLE
>
> `CVE-2026-94611`: Certain stored credentials readable with view permission alone (CVSS 8.1, affects `<= 2026.2.6`)

> CVE-2026-94612 CVE ↗ STABLE
>
> `CVE-2026-94612`: Authentication bypass in SAML Sources via assertion confusion and replay (CVSS 7.4, affects `<= 2026.2.6`)

> CVE-2026-94609 CVE ↗ STABLE
>
> `CVE-2026-94609`: Privilege escalation via delegated group and user management (CVSS 8.8, affects `<= 2026.5.6`)

> CVE-2026-94606 CVE ↗ STABLE
>
> `CVE-2026-94606`: MFA bypass via recipient override in the email authenticator (CVSS 8.9, affects `<= 2026.8.1`)

> CVE-2026-61574 CVE ↗ STABLE
>
> `CVE-2026-61574`: RAC endpoints and their stored credentials are exposed to any authenticated user, and connections can cross application boundaries (CVSS 8.8, affects `<= 2026.5.4`)

> CVE-2026-57580 CVE ↗ STABLE
>
> `CVE-2026-57580`: Account Takeover via SAML NameID Comment Truncation (CVSS 8.7, affects `<= 2026.5.4`)

> CVE-2026-54730 CVE ↗ STABLE

`CVE-2026-54730`: Google Chrome device trust stages can be bypassed (affects `<= 2026.2.5`)

`CVE-2026-55106` `CVE ↗` `STABLE`

`CVE-2026-55106`: LDAP Source debug endpoint accessible without authorization (CVSS 5.3, affects `<= 2026.2.5`)

`CVE-2026-49443` `CVE ↗` `STABLE`

`CVE-2026-49443`: `UserSourceConnection.user` and `GroupSourceConnection.group` are changeable through the API (CVSS 8.8, affects `<=2025.12.5`)

`CVE-2026-49448` `CVE ↗` `STABLE`

`CVE-2026-49448`: SourceStage bypass via empty POST (CVSS 9.8, affects `<=2025.12.5`)

`CVE-2026-47201` `CVE ↗` `STABLE`

`CVE-2026-47201`: XML Signature Wrapping in SAML Source ACS allows authentication as arbitrary federated user (CVSS 8.5, affects `<= 2025.12.5`)

`CVE-2026-41569` `CVE ↗` `STABLE`

`CVE-2026-41569`: WS-Federation wreply origin bypass can exfiltrate signed login responses to attacker-controlled endpoints (CVSS 6.1, affects `<= 2026.2.2`)

`CVE-2026-42849` `CVE ↗` `STABLE`

`CVE-2026-42849`: Reflected XSS in SFE (CVSS 9.3, affects `<= 2026.2.2`)

`CVE-2026-41577` `CVE ↗` `STABLE`

`CVE-2026-41577`: SAML source does not validate Conditions, timing, or audience on assertions (CVSS 7.5, affects `<= 2025.2.4`)

`CVE-2026-40166` `CVE ↗` `STABLE`

`CVE-2026-40166`: Non-admin user can retrieve confidential OAuth client_secret via `/api`/v3/oauth2/access_tokens/ (affects `<= 2026.2.2`)

`CVE-2026-25227` `CVE ↗` `STABLE`

`CVE-2026-25227`: Authenticated Remote Code Execution via Policy/Property Mapping test endpoint (CVSS 9.1, affects `>= 2021.3.1, < 2025.8.6`)

`CVE-2026-25748` CVE ↗ STABLE

`CVE-2026-25748`: Forward authentication bypass with malformed session cookie on Traefik and Caddy (CVSS 8.6, affects `<= 2025.10.3`)

`CVE-2025-64708` CVE ↗ STABLE

`CVE-2025-64708`: Invitation expiry is delayed by at least 5 minutes (CVSS 5.8, affects `<= 2025.10.1`)

`CVE-2025-64521` CVE ↗ STABLE

`CVE-2025-64521`: Deactivated service account can authenticate to OAuth (CVSS 4.8, affects `<= 2025.10.1`)

`CVE-2025-53942` CVE ↗ STABLE

`CVE-2025-53942`: Insufficient check for account active status when authenticating with OAuth/SAML Sources (CVSS 7.4, affects `< 2025.6.4`)

`CVE-2025-52553` CVE ↗ STABLE

`CVE-2025-52553`: Insufficient Session verification for Remote Access Control endpoint access (CVSS 9.6, affects `< 2025.6.3`)

`CVE-2025-29928` CVE ↗ STABLE

`CVE-2025-29928`: Deletion of sessions did not revoke sessions when using database session storage (CVSS 8.0, affects `< 2025.2.3`)

`CVE-2024-52307` CVE ↗ STABLE

`CVE-2024-52307`: Timing attack due to a lack of constant time comparison for metrics view (CVSS 5.6, affects `< 2024.10.3`)

WAS THIS USEFUL? 👍 👎

openfga

Feedback ⓘ CVE-2026-61709 CVE ↗ STABLE

A high-performance and flexible authorization/permission engine built for developers and inspired by Google Zanzibar.

`CVE-2026-61709`: OpenFGA Improper Policy Enforcement (CVSS 5.3, affects `<= 1.18.0`)

▾ **1 more release in this issue** · 2023-09-26 → 2026-07-16

> CVE-2023-43645 CVE ↗ STABLE
>
> `CVE-2023-43645`: DoS from circular relationship definitions (CVSS 5.9, affects `<1.3.1`)

WAS THIS USEFUL? 👍 👎

JumpCloud

Feedback ⓘ Release Notes 2026 (2026-11-02) BLOG ↗

RANK

JumpCloud makes it simple to manage Windows, Apple, Linux, and Android devices and to deliver secure access with SSO, MFA, Zero Trust, RADIUS, and more.

> JumpCloud shipped new REST APIs for managing AI agent identities, agent uninstall protection with maintenance tokens, and a batch of User Portal, policy, and JumpCloud Go improvements.

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

01 Agent Uninstall Protection for managed devices NEW

95

Blocks unauthorized removal of the JumpCloud agent, on by default for agent v2.179.2 or later on macOS, Windows, and Linux, requiring a per-device maintenance token to authorize uninstall. Admins manage exemptions using the `Disable Agent Uninstall Protection` policy and view protection status (`On` , `Off` , or `Failed`) from device details or the Devices list.

Retrieve a device's maintenance token to authorize agent uninstall on a specific managed device during maintenance.

> 📍 In the Admin Portal, go to Device Management › Devices, select the device, open device details, and under Settings › Agent Uninstall Protection, click View Maintenance Token.

— Exact policy name, version threshold, and token retrieval steps given.

Release Notes 2026 (2026-11-02)

02 New Windows user-level MDM and registry policies NEW

80

Two new Windows user-level policies: the User Level Custom Windows MDM (`OMA-URI`) Policy for configuring custom MDM settings on a user's profile, assignable to users or user groups on MDM-enrolled devices, and the User Level Windows Custom Registry Keys Policy for managing Windows registry values under `HKEY_CURRENT_USER` for an assigned user's profile at sign-in, requiring no MDM enrollment or device restart.

— Names both policies and the registry path precisely. Release Notes 2026 (2026-11-02)

03 Custom login banners and announcements in User Portal NEW

75

Admins can create login dialogs and announcement banners for users in the User Portal, targeted by user group with configurable severity and message type, via the new Custom Messaging feature under `Settings > User Portal > Custom Messaging`.

— Exact UI path given, limited mechanism beyond that. Release Notes 2026 (2026-11-02)

---

04 **Automatic device registration and browser discovery in JumpCloud Go**

IMPROVED

75

JumpCloud Go now automatically registers managed Windows, macOS, and Linux devices after user sign-in, with admin control over device eligibility via device exclusion groups. It also enables browser discovery deployment for AI and SaaS Management through third-party MDM by copying the Client ID and Client secret from Settings into the JumpCloud Go extension distribution policy.

— Names config elements but no exact endpoint or UI path. Release Notes 2026 (2026-11-02)

---

05 **Personal folders for applications in User Portal** NEW

60

Users can create personal folders to organize assigned applications on the All Applications page in the User Portal, accessible at `All Applications > Folders`.

— Exact UI path given, otherwise thin. Release Notes 2026 (2026-11-02)

THINNER COVERAGE BELOW

---

06 **Custom banned password list in Password Policies** NEW

45

Admins can block specific words, terms, and phrases from user passwords with a new Custom Banned Password List in Password Policies.

— Thin description, no config path or limits given. Release Notes 2026 (2026-11-02)

└──▷ ALSO FROM THESE RELEASES

.
.
.
.

WAS THIS USEFUL? 👍 👎

◆ Backup & Recovery

BorgBackup

Feedback ⓘ CVE-2026-62268 CVE ↗ STABLE

BorgBackup is an open-source deduplicating archiver with compression and authenticated encryption, used for space-efficient, verifiable backups.

`CVE-2026-62268`: borg extract might modify or disclose out-of-tree files when extracting maliciously crafted archives (affects `< 1.4.5`)

▾ **1 more release in this issue** · 2023-08-30 → 2026-08-26

> CVE-2023-36811 CVE ↗ STABLE
>
> `CVE-2023-36811`: Pre-1.2.5 archives spoofing vulnerability (CVSS 4.7, affects `<1.2.5`)

WAS THIS USEFUL? 👍 👎

Velero

Feedback ⓘ CVE-2026-32637 CVE ↗ STABLE

Velero is an open-source tool that backs up, restores, and migrates Kubernetes cluster resources and persistent volumes.

`CVE-2026-32637`: File path traversal when extracting from backup's tarball (affects `< 1.18.1`)

▾ **1 more release in this issue** · 2020-10-21 → 2026-08-19

> CVE-2020-3996 CVE ↗ STABLE
>
> `CVE-2020-3996`: Restored PersistentVolumes may be bound to wrong PersistentVolumeClaims (CVSS 5.5, affects `v0.*, v1.*`)

WAS THIS USEFUL? 👍 👎

Kopia

Feedback ⓘ CVE-2026-45695 CVE ↗

Kopia is an open-source backup tool for Windows, macOS, and Linux with incremental snapshots, client-side end-to-end encryption, compression, and deduplication, with both a CLI and a GUI.

`CVE-2026-45695`: RCE via SSH ProxyCommand Injection (CVSS 9.8, affects `<= 0.22.3`)

WAS THIS USEFUL? 👍 👎

◆ **Public Key Infrastructure (PKI)**

cert-manager

Feedback ⓘ CVE-2026-62290 CVE ↗ STABLE

Automatically provision and manage TLS certificates in Kubernetes

`CVE-2026-62290`: Direct ACME Challenge resources can bypass Issuer DNS01 solver policy and use ClusterIssuer DNS credentials (CVSS 7.3, affects `>= 1.18.0, <= 1.20.2`)

▾ **1 more release in this issue** · 2026-02-02 → 2026-06-25

> CVE-2026-25518 CVE ↗ STABLE
>
> `CVE-2026-25518`: cert-manager-controller DoS via Specially Crafted DNS Response (CVSS 5.9, affects `v1.18.0,v1.18.1,v1.18.2,v1.18.3,v1.18.4,v1.19.0,v1.19.1,v1.19.2`)

WAS THIS USEFUL? 👍 👎

lego

Feedback ⓘ CVE-2026-40611 CVE ↗ STABLE

Let's Encrypt/ACME client and library written in Go

`CVE-2026-40611`: Arbitrary File Write via Path Traversal in Webroot HTTP-01 Provider (CVSS 8.8, affects `all`)

▾ **1 more release in this issue** · 2025-08-06 → 2026-04-15

> CVE-2025-54799 CVE ↗ STABLE
>
> `CVE-2025-54799`: github.com/go-acme/lego/v4/acme/api does not enforce HTTPS (affects `<=4.25.1`)

WAS THIS USEFUL? 👍 👎

Smallstep step-ca

Feedback ⓘ CVE-2026-30836 CVE ↗

STABLE

A private certificate authority (X.509 & SSH) & ACME server for secure automated certificate management, so you can use TLS everywhere & SSO for SSH.

`CVE-2026-30836`: Authorization bypass in SCEP provisioner (CVSS 10.0, affects `< v0.30.0`)

▾ **1 more release in this issue** · 2025-12-03 → 2026-03-19

> CVE-2025-66406 CVE ↗ STABLE
>
> `CVE-2025-66406`: Improper Authorization Check for SSH Certificate Revocation (CVSS 5.0, affects `<= v0.28.4`)

WAS THIS USEFUL? 👍 👎

opensc

Feedback ⓘ CVE-2023-5992 CVE ↗

Open source smart card tools and middleware. PKCS#11/MiniDriver

`CVE-2023-5992` : Side-channel leaks while removing encryption RSA PKCS#1 v1.5 padding in OpenSC (CVSS 5.9, affects `0.24.0 and before`)

WAS THIS USEFUL? 👍 👎

◆ Data Security & DLP

cryptomator

Feedback ⓘ CVE-2026-33472 CVE ↗ STABLE

Cryptomator for Windows, macOS, and Linux: Secure client-side encryption for your cloud storage, ensuring privacy and control over your data.

`CVE-2026-33472`: Bypass of CVE-2026-32303 fix: getAuthority() port-based scheme confusion allows HTTP downgrade of Hub token exchange (CVSS 4.8, affects `= 1.19.1`)

▾ **4 more releases in this issue** · 2023-08-07 → 2026-04-16

> CVE-2026-32310 CVE ↗ STABLE
>
> `CVE-2026-32310`: Unverified masterkeyfile key IDs can access arbitrary local or UNC paths (CVSS 4.1, affects `>= 1.6.0, <= 1.19.0`)

> CVE-2026-32303 CVE ↗ STABLE
>
> `CVE-2026-32303`: Tampered vault configuration allows MITM attack on Hub API (CVSS 7.6, affects `< 1.19.1`)

> CVE-2026-32309 CVE ↗ STABLE
>
> `CVE-2026-32309`: Hub unlocking accepts plaintext HTTP and unvalidated endpoint schemes (CVSS 7.5, affects `<= 1.19.0`)

> CVE-2023-39520 CVE ↗ STABLE
>
> `CVE-2023-39520`: MSI installer allows Local Elevation of Privileges #2 (CVSS 7.8, affects `<=1.9.2`)

WAS THIS USEFUL? 👍 👎

◆ Secure Access (VPN / SASH / ZTNA)

Slack Nebula

Feedback ⓘ CVE-2026-25793 CVE ↗

A scalable overlay networking tool with a focus on performance, simplicity and security

`CVE-2026-25793` : Blocklist Bypass possible via ECDSA Signature Malleability (CVSS 8.1, affects `>= 1.7.0, <= 1.10.2`)

WAS THIS USEFUL? 👍 👎

tailscale

Feedback ⓘ CVE-2023-28436 CVE ↗ STABLE

Tailscale creates private WireGuard-based mesh networks with centralized identity and access controls.

`CVE-2023-28436` : Non-interactive Tailscale SSH sessions on FreeBSD may use the effective group ID of the tailscaled process (CVSS 5.7, affects `>=1.34.0, <1.38.2`)

▾ 1 more release in this issue · 2022-11-21 → 2023-03-22

> CVE-2022-41924 CVE ↗ STABLE
>
> `CVE-2022-41924` : Tailscale Windows daemon is vulnerable to RCE via CSRF (CVSS 9.6, affects `<1.32.3`)

WAS THIS USEFUL? 👍 👎

◆ Privileged Access Management

Teleport

Feedback ⓘ CVE-2025-49825 CVE ↗

The easiest, and most secure way to access and protect all of your infrastructure.

`CVE-2025-49825` : Remote authentication bypass (CVSS 9.8, affects `<17.5.2`)

WAS THIS USEFUL? 👍 👎

◆ Non-Human & Agent Identity

SPIFFE spire

Feedback ⓘ CVE-2021-44716 CVE ↗ STABLE

The SPIFFE Runtime Environment

`CVE-2021-44716`: Unbounded memory usage on exposed HTTP/2 (non-gRPC) endpoints (CVSS 7.5, affects `Before 1.0.3 and 1.1.x before 1.1.3`)

▾ **2 more releases in this issue** · 2021-03-04 → 2022-01-07

> CVE-2021-27099 CVE ↗ STABLE
>
> `CVE-2021-27099`: Path Normalization issue in `aws_iid` Node Attestor (CVSS 6.8, affects `<0.8.4, <0.9.4, <0.10.2, <0.11.3, <0.12.1`)

> CVE-2021-27098 CVE ↗ STABLE
>
> `CVE-2021-27098`: Legacy Node API Allows Impersonation (CVSS 8.1, affects `0.8.1-0.8.4, <0.9.4, <0.10.2, <0.11.3, <0.12.1`)

WAS THIS USEFUL? 👍 👎

DEPLOY

◆ Agentic Infrastructure

microsandbox

Feedback ⓘ CVE-2026-61669 CVE ↗ STABLE

easy, fast, programmable and local-first microVM runtime and library

`CVE-2026-61669`: Snapshot Import Symlink Traversal Arbitrary File Write (CVSS 7.1, affects `>= 0.4.4, < 0.5.8`)

▾ **2 more releases in this issue** · 2026-06-23 → 2026-10-09

> CVE-2026-103034 CVE ↗ STABLE
>
> `CVE-2026-103034`: Guest-controlled symlinks in msb copy allow arbitrary file write on the host (CVSS 7.1, affects `>= 0.5.3, < 0.6.7`)

> CVE-2026-61670 CVE ↗ STABLE
>
> `CVE-2026-61670`: Secret values exposed in world-readable process arguments (CVSS 6.5, affects `>= 0.3.0, < 0.5.10`)

WAS THIS USEFUL? 👍 👎

GOVERN

◆ AI Red Teaming & Testing

NVIDIA SkillSpector

Feedback ⓘ v2.13.3 NOTES ↗ RANK

Security scanner for AI agent skills. Detect vulnerabilities, malicious patterns, security risks, prompt injection, data exfiltration, and supply-chain risks in Claude Code, Codex, and MCP skills before you install them.

> SkillSpector's latest release adds configurable scan-performance limits alongside new detections for npx-based MCP configs, agent-memory file writes, ransomware-like file behavior, Pipenv dependencies, and credentials flowing through urllib request headers.

└──▷ **WHAT SHIPPED · 9 FEATURES** most completely described first ? what's the number?

01 Configurable batch, workflow and LLM concurrency limits NEW

90

Control the tool-description comparison batch limit with `SKILLSPECTOR_TP4_MAX_BATCHES` (default 256), the workflow deadline with `SKILLSPECTOR_MAX_WORKFLOW_SECONDS` (default 1,080 seconds), and LLM concurrency with `SKILLSPECTOR_MAX_LLM_CONCURRENCY`.

Run a large skill collection scan without hitting the default 256-batch or 18-minute limits by raising both caps for a provider with high throughput.

```
$ SKILLSPECTOR_TP4_MAX_BATCHES=512
SKILLSPECTOR_MAX_WORKFLOW_SECONDS=3600
SKILLSPECTOR_MAX_LLM_CONCURRENCY=8 skillspector scan ./my-large-
skill/
```

— Named env vars with defaults and a runnable example v2.13.3

THINNER COVERAGE BELOW

02 npx inspection and credential filename recognition in MCP configs

NEW

50

SkillSpector now inspects `npx` commands in JSON MCP configurations and recognizes additional Claude, Cline, and Roo Code credential and configuration filenames.

— Names targets but no flag or command shown v2.13.3

03 Bounded YARA signal for ransomware-like behavior NEW

45

SkillSpector adds a bounded YARA signal for nearby directory walking, encryption, and binary writes across lines to surface potential ransomware-like behavior alongside existing stronger rules.

— Explains detection logic, no user-facing control v2.13.3

04 **Report destination overwrite protection** NEW 45

SkillSpector now rejects baseline and recursive report destinations that would overwrite the primary input or a discovered child skill's input, including file aliases.

— Describes the safety check's exact conditions v2.13.3

05 **Detection of writes to agent-memory files** NEW 40

SkillSpector now detects writes to known agent-memory files and directories from automatically run test carriers, including raw Windows paths.

— Describes mechanism but no configurable surface v2.13.3

06 **Pipenv dependency extraction and locked version checks** NEW 40

SkillSpector now extracts Pipenv dependencies and checks locked versions, preserving incomplete coverage for malformed or unsupported dependency declarations.

— States scope and caveat but no command shown v2.13.3

07 **Non-English findings included in batch-scan verdicts** IMPROVED 40

Non-English gap-fill findings are now included in contributed batch-scan scores, recommendations, and exit status instead of retaining a stale SAFE verdict.

— Describes the fix but no reproduction steps v2.13.3

08 **Tracks credentials through urllib request headers** IMPROVED 35

SkillSpector now follows credential reads nested in `urllib` request headers into network sinks.

— Names the library but no further detail v2.13.3

09 **Incomplete-inspection reporting for missing YARA rule directory**

IMPROVED 35

SkillSpector now reports incomplete inspection when a requested custom YARA rule directory is unavailable.

— Thin single-sentence behavior change v2.13.3

WAS THIS USEFUL? 👍 👎

humanbound

Feedback ⓘ CVE-2026-102652 CVE ↗

Open-source adversarial testing engine, SDK, and CLI for AI agents. Runs locally or against the Humanbound Platform.

`CVE-2026-102652`: Credential leak to attacker-controlled host via redirect in humanbound (affects `< 2.7.0`)

WAS THIS USEFUL? 👍 👎

Giskard

Feedback ⓘ CVE-2026-40319 CVE ↗ STABLE

Giskard tests and evaluates LLM applications for performance, bias, and security issues.

`CVE-2026-40319`: Regular Expression Denial of Service (ReDoS) in RegexMatching Check (CVSS 5.5, affects `<= 1.0.1b1`)

▾ **3 more releases in this issue** · 2024-11-14 → 2026-04-13

> CVE-2026-40320 CVE ↗ STABLE
>
> `CVE-2026-40320`: Unsandboxed Jinja2 Template Rendering in ConformityCheck (CVSS 7.8, affects `<= 1.0.1b1`)

> CVE-2026-34172 CVE ↗ STABLE
>
> `CVE-2026-34172`: Server-side template injection via ChatWorkflow.chat() using non-sandboxed Jinja2 Environment (CVSS 8.8, affects `<= 0.3.3`)

> CVE-2024-52524 CVE ↗ STABLE
>
> `CVE-2024-52524`: ReDoS in Giskard Scan text perturbation (affects `<= 2.15.4`)

WAS THIS USEFUL? 👍 👎

◆ AI Runtime Defense & Guardrails

pipelock

Feedback ⓘ CVE-2026-91179 CVE ↗ STABLE

Open-source AI agent firewall for MCP security and agent egress. Scans mediated HTTP, MCP, A2A, and WebSocket traffic for exfiltration, SSRF, and prompt injection, and emits mediator-signed action receipts: verifiable audit evidence from outside the agent.

`CVE-2026-91179` : hostile-model preset: shell-profile destination-write bypass via MCP move_file (equivalent-operation coverage gap) (affects `<= 3.5.0`)

▾ **3 more releases in this issue** · 2026-08-20 → 2026-10-03

> CVE-2026-91180 CVE ↗ STABLE
>
> `CVE-2026-91180` : Pipelock media policy bypass through mismatched response content types (CVSS 5.3, affects `>= 2.2.0, < 3.5.0`)

> CVE-2026-91178 CVE ↗ STABLE
>
> `CVE-2026-91178` : URL DLP Scanner Bypass via Path-Query Secret Splitting (CVSS 5.8, affects `< 3.4.0`)

> CVE-2026-92145 CVE ↗ STABLE
>
> `CVE-2026-92145` : Hot-reload can silently retain stale security config under burst edits (affects `< 2.6.0`)

WAS THIS USEFUL? 👍 👎

◆ AI/LLM Security

NoLabs nono

Feedback ⓘ CVE-2026-47128 CVE ↗

The nono runtime runs AI agents in isolated environments with policy-controlled filesystem, network, and credential access.

`CVE-2026-47128` : nono: Sandbox escape on Linux via D-Bus: `systemd-run --user` (CVSS 6.1, affects `< 0.55.0`)

WAS THIS USEFUL? 👍 👎

◆ General Utilities & Libraries

Microsoft code-oss

Feedback ⓘ CVE-2026-78461 CVE ↗

STABLE

The code-oss project is an open-source code editor combining editing, debugging, and extensibility for developers across Windows, macOS, and Linux.

`CVE-2026-78461`: Security Feature Bypass via Notebooks (CVSS 7.4, affects `< 1.136.2`)

▾ **7 more releases in this issue** · 2026-08-11 → 2026-10-13

> CVE-2026-69370 CVE ↗ STABLE
>
> `CVE-2026-69370`: Remote Code Execution via Workspace-injected Error Notification Link (CVSS 8.8, affects `< 1.141.1`)

> CVE-2026-102229 CVE ↗ STABLE
>
> `CVE-2026-102229`: Information Disclosure via Remote Webview Resource Path Traversal (CVSS 6.8, affects `< 1.141.1`)

> CVE-2026-102233 CVE ↗ STABLE
>
> `CVE-2026-102233`: Workspace Trust Bypass via Terminal Relaunch and Reuse (CVSS 7.8, affects `< 1.141.1`)

> CVE-2026-81380 CVE ↗ STABLE
>
> `CVE-2026-81380`: Information Disclosure through Automatic Remote Image Fetch in Chat (CVSS 5.3, affects `< 1.136.2`)

> CVE-2026-81377 CVE ↗ STABLE
>
> `CVE-2026-81377`: Visual Studio Code MCP gallery metadata path traversal (CVSS 6.5, affects `>= 1.0.0, < 1.136.2`)

> CVE-2026-81381 CVE ↗ STABLE
>
> `CVE-2026-81381`: Azure DevOps access token disclosure through GitHub Copilot Chat workspace settings (CVSS 6.5, affects `< 1.136.2`)

> CVE-2026-69320 CVE ↗ STABLE

> `CVE-2026-69320` : Visual Studio Code web deployments - `environmentService.ts` - RCE via `NODE_OPTIONS` `--import` from URL payload (CVSS 8.8, affects `<` `1.132.1`)

WAS THIS USEFUL?  

joplin Feedback ⓘ CVE-2026-105786 CVE ↗ STABLE

Joplin - the privacy-focused note taking app with sync capabilities for Windows, macOS, Linux, Android and iOS.

.
.
.
.

`CVE-2026-105786` : Unauthenticated account takeover via an attacker-chosen application-authorisation identifier (affects `<= 3.7.1`)

▾ **21 more releases in this issue** · 2024-06-21 → 2026-09-09

> CVE-2026-105785 CVE ↗ STABLE
>
> `CVE-2026-105785` : Password reset accepts any valid per-user token including CSRF tokens and email-confirmation tokens because the token store has no purpose/type field, enabling full account takeover from a leaked CSRF token or a scanned confirmation-email link (CVSS 4.8, affects `3.7.0`)

> CVE-2026-105783 CVE ↗ STABLE
>
> `CVE-2026-105783` : Any website open in the browser can trigger and win Joplin's Web Clipper pairing dialog, stealing the permanent full-access API token, because the local server has no Origin/Referer restriction and the confirmation dialog shows no identifying information (CVSS 8.0, affects `3.7.0`)

> CVE-2026-105784 CVE ↗ STABLE
>
> `CVE-2026-105784` : Whiteboard note content is rendered into the main application document, bypassing the note-viewer origin isolation and allowing CSS injection with a remote-controlled exfiltration channel (CVSS 4.6, affects `current dev`)

> CVE-2026-46649 CVE ↗ STABLE
>
> `CVE-2026-46649` : SSO Auth Code Login Missing Rate Limiting — 9-Digit Numeric Code Brute-Forceable via Unprotected Endpoint (affects `<= 3.3.0`)

> CVE-2026-46650 CVE ↗ STABLE
>
> `CVE-2026-46650` : Stored XSS in public share viewer via javascript: URL bypass in isAcceptedUrl (CVSS 4.4, affects `<= 3.5.2`)

> CVE-2026-49450 CVE ↗ STABLE

`CVE-2026-49450` : Joplin desktop Windows auto-updater accepts signed installer from any publisher because app-update.yml has no publisherName (CVSS 7.1, affects `<= 3.6.14`)

`CVE-2026-49453` `CVE ↗` `STABLE`

`CVE-2026-49453` : Path traversal in resource sync — silent arbitrary file write outside the resource directory (CVSS 7.0, affects `<=3.7.1`)

`CVE-2026-55105` `CVE ↗` `STABLE`

`CVE-2026-55105` : Fountain embeds allow arbitrary script execution in published notes and the note viewer (CVSS 7.7, affects `<=3.7.1`)

`CVE-2026-55210` `CVE ↗` `STABLE`

`CVE-2026-55210` : SAML SSO account takeover via email-based account linking (missing is_external check in ssoLogin) (CVSS 7.4, affects `<= 3.7.1`)

`CVE-2026-55179` `CVE ↗` `STABLE`

▶ Watch video

`CVE-2026-55179` : Logic error in Joplin Server allows a signed-in user to read any note from its internal server ID (CVSS 6.5, affects `<=3.7.1`)

`CVE-2026-55456` `CVE ↗` `STABLE`

▶ Watch video

`CVE-2026-55456` : Path traversal vulnerability in sync logic allows a malicious sync target to create and overwrite arbitrary files (CVSS 8.8, affects `<=3.7.1`)

`CVE-2026-59814` `CVE ↗` `STABLE`

`CVE-2026-59814` : Stored XSS via inline-served note attachment on published shares (CVSS 7.6, affects `<= 3.7.1`)

`CVE-2026-59816` `CVE ↗` `STABLE`

`CVE-2026-59816` : Path traversal in transcribe proxy endpoint via URL-encoded slash (CWE-22) (CVSS 4.3, affects `<= 3.7.1`)

`CVE-2026-59815` `CVE ↗` `STABLE`

`CVE-2026-59815` : Pending share recipients can write items into shared folders before accepting invitations (CVSS 4.3, affects `<= v3.6.15`)

`CVE-2025-57798` CVE ↗ STABLE

`CVE-2025-57798` : Denial of Service (DoS) via Uncontrolled Resource Allocation in Joplin Title Input (CVSS 5.5, affects `< 3.3.13`)

`CVE-2025-27409` CVE ↗ STABLE

`CVE-2025-27409` : Path traversal in Joplin Server (CVSS 7.5, affects `<= 3.3.3`)

`CVE-2025-24028` CVE ↗ STABLE

`CVE-2025-24028` : XSS in Rich Text Editor allows arbitrary code execution (CVSS 7.8, affects `3.2.6 - 3.2.11`)

`CVE-2024-53268` CVE ↗ STABLE

`CVE-2024-53268` : Lack of validation on openExternal allows XSS (CVSS 7.2, affects `<3.0.3`)

`CVE-2024-49362` CVE ↗ STABLE

`CVE-2024-49362` : XSS on <a> Link in markdown preview (CVSS 7.7, affects `3.0`)

`CVE-2024-40643` CVE ↗ STABLE

`CVE-2024-40643` : Parsing error leading to XSS (CVSS 8.6, affects `3.0.13`)

`CVE-2023-39517` CVE ↗ STABLE

`CVE-2023-39517` : XSS when clicking on an untrusted `<map>` link (CVSS 7.3, affects `< 2.12.8`)

WAS THIS USEFUL? 👍 👎

GitHub CLI Feedback ⓘ CVE-2026-72924 CVE ↗ STABLE

GitHub's official command line tool

`CVE-2026-72924`: `gh codespace ports forward` exposes forwarded services on all network interfaces by default (affects `>=v2.28.0`)

▾ **8 more releases in this issue** · 2024-11-27 → 2026-08-20

> CVE-2026-64655 CVE ↗ STABLE
>
> `CVE-2026-64655`: Attestation verification bypass via unescaped regex metacharacters in SAN matching (affects `<=2.96.0`)

> CVE-2026-64653 CVE ↗ STABLE
>
> `CVE-2026-64653`: Unescaped variable components in request URLs could allow path traversal in GitHub CLI (affects `<=v2.96.0`)

> CVE-2026-64654 CVE ↗ STABLE
>
> `CVE-2026-64654`: Terminal escape sequence injection in multiple `gh` commands (affects `<= v2.96.0`)

> CVE-2026-59831 CVE ↗ STABLE
>
> `CVE-2026-59831`: Connecting to a malicious Codespace via `gh codespace jupyter` could allow command execution on the user's computer (CVSS 4.4, affects `>= v2.10.0`)

> CVE-2026-48501 CVE ↗ STABLE
>
> `CVE-2026-48501`: Incorrect authorization header in API requests to TUF repository mirrors via `gh attestation`, `gh release verify`, and `gh release verify-asset` commands (CVSS 7.4, affects `<= v2.92.0`)

> CVE-2025-25204 CVE ↗ STABLE
>
> `CVE-2025-25204`: `gh attestation verify` returns incorrect exit code during verification when predicate types mismatch (CVSS 6.3, affects `>= v2.49.0`)

> CVE-2024-54132 CVE ↗ STABLE

> `CVE-2024-54132`: Downloading malicious GitHub Actions workflow artifact results in path traversal vulnerability (affects `<= 2.63.0`)

> CVE-2024-53858 CVE ↗ STABLE
>
> `CVE-2024-53858`: Recursive repository cloning can leak authentication tokens to non-GitHub submodule hosts (CVSS 6.5, affects `<= 2.62.0`)

WAS THIS USEFUL? 👍 👎

Syslifters SysReptor

Feedback ⓘ CVE-2026-81182 CVE ↗

STABLE

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

`CVE-2026-81182` : Unauthorized file disclosure by broken access control in writable shared notes (CVSS 4.2, affects `<=2026.61`)

▾ **6 more releases in this issue** · 2024-05-21 → 2026-08-20

> CVE-2026-81180 CVE ↗ STABLE
>
> `CVE-2026-81180` : Authenticated RCE by insecure image processing (CVSS 8.8, affects `<=2026.55`)

> CVE-2026-81179 CVE ↗ STABLE
>
> `CVE-2026-81179` : Host header injection might allow account takeover (CVSS 8.1, affects `<=2026.55`)

> CVE-2026-42291 CVE ↗ STABLE
>
> `CVE-2026-42291` : Read-write access to personal notes by sharing-link creation with no authorization in SysReptor Professional (CVSS 6.8, affects `>=2026.4;<2026.27`)

> CVE-2025-66561 CVE ↗ STABLE
>
> `CVE-2025-66561` : Authenticated Stored Cross-Site Scripting (XSS) (CVSS 7.3, affects `<=2025.96`)

> CVE-2025-59945 CVE ↗ STABLE
>
> `CVE-2025-59945` : Privilege Escalation by Authenticated Users (CVSS 8.1, affects `2024.74-2025.81`)

> CVE-2024-36076 CVE ↗ STABLE
>
> `CVE-2024-36076` : Cross-Site Websocket Hijacking in SysReptor (CVSS 6.8, affects `>= 2024.28 <= 2024.30`)

WAS THIS USEFUL? 👍 👎

goshs

Feedback ⓘ CVE-2026-114518 CVE ↗ STABLE

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

`CVE-2026-114518`: Unauthenticated attackers can bypass basic auth via the ConPtyShell route exemption (CVSS 9.8, affects `>= 2.1.1, <= 2.1.4`)

▾ **2 more releases in this issue** · 2026-07-27 → 2026-07-29

> CVE-2026-114504 CVE ↗ STABLE
>
> `CVE-2026-114504`: goshs `--no-delete` / `--upload-only` bypass: PUT/POST overwrite of existing files destroys contents (HTTP and WebDAV) (CVSS 9.1, affects `<= 2.1.4`)

> CVE-2026-66063 CVE ↗ STABLE
>
> `CVE-2026-66063`: Path Traversal (CVSS 6.5, affects `<= 2.1.4`)

WAS THIS USEFUL? 👍 👎

wsgidav

Feedback ⓘ CVE-2026-55560 CVE ↗ STABLE

A generic and extendable WebDAV server based on WSGI

`CVE-2026-55560`: FilesystemProvider: `follow_symlinks=false` guard is leaf-only — root escape via intermediate symlink (read/write/delete) (CVSS 7.4, affects `<= 4.3.4`)

▾ **3 more releases in this issue** · 2022-11-11 → 2026-06-27

> CVE-2026-55509 CVE ↗ STABLE
>
> `CVE-2026-55509`: Blind SQL injection in WsgiDAV MySQL provider (affects `<= 4.3.4`)

> CVE-2026-48099 CVE ↗ STABLE
>
> `CVE-2026-48099`: Encoded dot segments can escape WsgiDAV filesystem share roots (CVSS 7.1, affects `<= 4.3.3`)

> CVE-2022-41905 CVE ↗ STABLE
>
> `CVE-2022-41905`: Cross Site Scripting vulnerability in wsgidav when directory browsing is enabled (CVSS 8.2, affects `>=3.0.0a1,<4.1.0`)

WAS THIS USEFUL? 👍 👎

kubernetes-helm

Feedback ⓘ CVE-2026-35206 CVE ↗ STABLE

The Kubernetes Package Manager

`CVE-2026-35206`: Helm Chart extraction output directory collapse via `Chart.yaml` name dot-segment (CVSS 4.4, affects `<=3.20.1,<=4.1.3`)

▾ **16 more releases in this issue** · 2020-04-22 → 2026-04-09

> CVE-2026-35204 CVE ↗ STABLE
>
> `CVE-2026-35204`: Path traversal in plugin metadata version enables arbitrary file write outside Helm plugin directory (CVSS 8.6, affects `>=4.0.0,<=4.1.3`)

> CVE-2026-35205 CVE ↗ STABLE
>
> `CVE-2026-35205`: Plugin verification fails open when `.prov` is missing, allowing unsigned plugin install (CVSS 7.8, affects `>=4.0.0,<=4.1.3`)

> CVE-2025-55198 CVE ↗ STABLE
>
> `CVE-2025-55198`: Incorrect YAML Content Leads To Panic (CVSS 6.5, affects `<= 3.18.4`)

> CVE-2025-55199 CVE ↗ STABLE
>
> `CVE-2025-55199`: Helm Charts with Specific JSON Schema Values Can Cause Memory Exhaustion (CVSS 6.5, affects `<= 3.18.4`)

> CVE-2025-53547 CVE ↗ STABLE
>
> `CVE-2025-53547`: Chart Dependency Updating With Malicious Chart.yaml Content And Symlink (CVSS 8.5, affects `<= 3.17.3, >= 3.18.0, <= 3.18.3`)

> CVE-2025-32386 CVE ↗ STABLE
>
> `CVE-2025-32386`: Specially Crafted Chart Archive Can Cause Out Of Memory Termination (CVSS 6.5, affects `< 3.17.2`)

> CVE-2025-32387 CVE ↗ STABLE
>
> `CVE-2025-32387`: Specially Crafted JSON Schema Can Cause Stack Overflow (CVSS 6.5, affects `< 3.17.3`)

CVE-2024-25620 CVE ↗ STABLE

`CVE-2024-25620` : Dependency management path traversal (CVSS 6.4, affects `< 3.14.0`)

CVE-2023-25165 CVE ↗ STABLE

`CVE-2023-25165` : getHostByName Function Information Disclosure (CVSS 4.3, affects `v3.0.0 - v3.11.0`)

CVE-2022-23524 CVE ↗ STABLE

`CVE-2022-23524` : Denial of service through string value parsing (CVSS 7.5, affects `<= v3.10.2`)

CVE-2021-32690 CVE ↗ STABLE

`CVE-2021-32690` : Repository credentials passed to alternate domain (CVSS 8.6, affects `<=3.6.0`)

CVE-2021-21303 CVE ↗ STABLE

`CVE-2021-21303` : Unsanitized data displayed directly to user's terminal (CVSS 6.8, affects `>3.0 and < 3.5.1`)

CVE-2020-15187 CVE ↗ STABLE

`CVE-2020-15187` : plugin.yaml file allows for duplicate entries (CVSS 4.7, affects `2.0.0-2.16.10, 3.0.0-3.3.1`)

CVE-2020-4053 CVE ↗ STABLE

`CVE-2020-4053` : Plugin archive directory traversal (CVSS 6.8, affects `3.0.0-3.2.3`)

CVE-2020-7919 CVE ↗ STABLE

`CVE-2020-7919` : CVE-2020-7919 (CVSS 7.5, affects `2.0.0-2.16.7,3.0.0-3.0.3`)

CVE-2020-11013 CVE ↗ STABLE

`CVE-2020-11013` : lookup Function Information Discolosure (CVSS 5.0, affects `3.1.0-3.1.2`)

WAS THIS USEFUL? 👍 👎

gss-ntlmssp Feedback ⓘ CVE-2023-25566 CVE ↗ STABLE

A complete implementation of the MS-NLMP documents as a GSSAPI mechanism

`CVE-2023-25566`: Memory leak when parsing usernames (CVSS 7.5, affects `<= 1.1.0`)

▾ **1 more release in this issue** · 2023-02-12

> CVE-2023-25567 CVE ↗ STABLE
>
> `CVE-2023-25567`: Out-of-bounds read when decoding target information (CVSS 7.5, affects `<= 1.1.0`)

WAS THIS USEFUL? 👍 👎

bpf-linker

Feedback ⓘ v0.13.0 NOTES ↗ RANK

BPF static linker

> bpf-linker v0.13.0 adds support for the static relocation model and speeds up BTF sanitization by reusing LLVM metadata.

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

01 **Faster BTF sanitization via LLVM metadata reuse** IMPROVED

35

bpf-linker's BTF sanitizer now reuses LLVM metadata, reducing redundant processing during BTF generation.

— Explains mechanism but no numbers or config surface. v0.13.0

02 **Static relocation model support** NEW

10

bpf-linker adds the static relocation model, per the release summary, though no further mechanism or usage detail is given.

— Named only in summary, no detail provided. v0.13.0

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · November 2, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe Feedback on this issue