THE CYBER TOOLCHAIN

NO. 007

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED JULY 6, 2026 · EVERY WEEKDAY

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

▸ // HOW THIS ISSUE IS MADE SHOW

VIEW

ISSUE VIEW

scroll



SCROLL | EXPAND IN PLACE | PREVIEW PANE

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 15 tools

OFFENSIVE SECURITY

◆ Reconnaissance & OSINT

Maigret v0.6.2

Collect a dossier on a person by username from 3000+ sites

Maigret v0.6.2 adds keyword filtering, Neo4j Cypher export, ORCID support, FlareSolverr bypass, and a threaded DNS fallback.

└──▷ GET THIS VERSION

```
$ git clone --branch v0.6.2 https://github.com/soxoj/maigret.git
# already have the repo? check out this version:
$ git checkout v0.6.2
```

└──▷ TRY IT

Narrow a username search to profiles that mention specific keywords — useful for confirming identity across common-name accounts.

```
$ maigret johndoe --keywords hacker,security
```

Export OSINT findings directly into Neo4j for graph-based link analysis across discovered accounts.

```
$ maigret johndoe --neo4j
```

Switch to the threaded DNS resolver when aiodns failures are causing sites to be skipped on your network.

```
$ maigret johndoe --dns-resolver threaded
```

- Adds `--keywords` flag to filter results by matching keywords found in profile pages.
- Adds `--neo4j` flag to export search results as a Neo4j Cypher file for graph database ingestion.
- Adds ORCID as a supported site for academic researcher identity lookups.
- Adds FlareSolverr integration in the web UI to bypass Cloudflare challenges.
- Adds `--dns-resolver threaded` fallback option to recover from aiodns DNS resolution failures.

+4 more

WAS THIS USEFUL? 👍 👎

APPLICATION SECURITY

◆ Web Application Security

ProjectDiscovery nuclei v3.11.0

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.

v3.11.0 requires digital signatures on all custom JavaScript-protocol templates before Nuclei will load them.

└──▷ GET THIS VERSION

```
$ git clone --branch v3.11.0
https://github.com/projectdiscovery/nuclei.git
# already have the repo? check out this version:
$ git checkout v3.11.0
```

└──▷ TRY IT

Sign a custom JavaScript-protocol template so it is accepted by Nuclei v3.11.0+ before running it against a target.

```
$ nuclei -sign -t /path/to/your-template.yaml
```

- Breaking change: Custom templates using the `javascript:` protocol must now be digitally signed; unsigned JavaScript templates are skipped at load time and when referenced from workflows.
- Enforces signature verification for JavaScript templates, extending the code-protocol signing requirement to the JavaScript protocol and its Go-backed runtime modules.

└──▷ BREAKING ON UPGRADE

! Custom templates that use the `javascript:` protocol must be digitally signed before Nuclei will load or execute them; unsigned JavaScript templates are skipped during template loading and when referenced from workflows.

WAS THIS USEFUL? 👍 👎

Bunkerity BunkerWeb v1.6.12

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

BunkerWeb v1.6.12 adds upstream TLS verification, per-path mTLS, a full logs viewer overhaul, and tightened API token security.

└──▷ GET THIS VERSION

```
$ git clone --branch v1.6.12
https://github.com/bunkerity/bunkerweb.git
# already have the repo? check out this version:
$ git checkout v1.6.12
```

└──▷ USE IT

Enforce TLS verification when BunkerWeb proxies to an internal HTTPS backend, supplying a custom CA bundle.

```ini
REVERSE_PROXY_SSL_VERIFY=yes
REVERSE_PROXY_SSL_VERIFY_DEPTH=2
REVERSE_PROXY_SSL_TRUSTED_CERTIFICATE=/etc/bunkerweb/certs/internal-ca.pem
```

Require mTLS only on sensitive API paths while leaving public endpoints unaffected.

```ini
MTLS_URL_1=^/api/admin.*
```

Cap scheduler thread-pool workers to limit database connection pressure in high-traffic deployments.

```ini
SCHEDULER_MAX_WORKERS=4
```

- Adds upstream HTTPS certificate verification for reverse proxy via `REVERSE_PROXY_SSL_VERIFY`, `REVERSE_PROXY_SSL_VERIFY_DEPTH`, `REVERSE_PROXY_SSL_TRUSTED_CERTIFICATE`, `REVERSE_PROXY_SSL_TRUSTED_CERTIFICATE_DATA`, and `REVERSE_PROXY_SSL_TRUSTED_CERTIFICATE_PRIORITY` settings.

- Adds `MTLS_URL_n` regex setting to enforce mTLS selectively per path rather than site-wide.
- Adds `SCHEDULER_MAX_WORKERS` to cap the job-executor thread pool and reduce database pool pressure under load.
- Extends `ANTIBOT_IGNORE_URI` to match full request URIs including query strings.
- Supports pre-hashed bcrypt values for `ADMIN_PASSWORD`, enabling secret-manager and GitOps workflows.

+7 more

WAS THIS USEFUL? 👍 👎

Dalfox v3.1.1 2 RELEASES · 2026-06-14 → 2026-06-21 LATEST STABLE

Dalfox is a powerful open-source XSS scanner and utility focused on automation.

Dalfox v3.1.1 unifies server/MCP scan target params, consolidates debug logging, and bounds request fan-out for safer large scans.

└──▷ GET THIS VERSION

```
$ git clone --branch v3.1.1 https://github.com/hahwul/dalfox.git
# already have the repo? check out this version:
$ git checkout v3.1.1
```

└──▷ TRY IT

Pipe a HAR capture through dalfox using an explicit input type — now correctly honoured by the `pipe` subcommand after the parity fix.

```
$ cat capture.har | dalfox pipe -i har --output results.json
```

Debug a scan against a REST API server using the unified `target` parameter (replacing the old `url` field for server/MCP calls).

```
$ curl -s -X POST http://localhost:6664/scan -H 'Content-Type:
application/json' -d '{"target": "https://example.com/search?
q=test"}'
```

- Unifies scan target parameter: Server and MCP modes now accept `target` (REST retains `url` as a backward-compatible alias).
- Consolidates all debug output through a single stderr `dbg_log!` macro, keeping JSON/JSONL/SARIF stdout clean under `--debug`.
- Aligns OOB/blind XSS lifecycle messages with the standard timestamped log format (`INF` / `WRN` / `OOB`), making output consistent across scan modes.
- Per-parameter payload safety cap and recall-preserving DOM-phase early-exit bound request fan-out, preventing runaway HTTP requests on wide parameter sets.
- Bounds unbounded task spawning in parameter mining and cuts server hot-path lock-hold and allocations, improving reliability under load.

▾ 1 more release in this issue · 2026-06-14 → 2026-06-21

v3.1.0 STABLE

Dalfox v3.1.0 adds blind/OOB XSS, HAR input, external JS analysis, CSP/Trusted Types payloads, and a global rate limiter.

└──▷ GET THIS VERSION

```
$ git clone --branch v3.1.0 https://github.com/hahwul/dalfox.git
# already have the repo? check out this version:
$ git checkout v3.1.0
```

└──▷ TRY IT

Detect stored/async XSS in a target that never reflects payloads back — catch blind execution via an interactsh OOB callback.

```
$ dalfox scan https://target.example.com --blind-oob
```

Replay every request captured in a proxy session (Burp/Caido/ZAP) as a scan source, feeding all recorded targets at once.

```
$ dalfox scan export.har --input-type har --output json -o
results.json
```

Cap aggregate outbound rate to 20 RPS across all workers while also pulling in external JS bundles for DOM-XSS analysis — useful for rate-sensitive bug-bounty targets.

```
$ dalfox scan https://target.example.com --rate-limit 20 --analyze-
external-js
```

- Adds `--blind-oob` for out-of-band (OAST) XSS detection via interactsh, catching stored and async sinks that never reflect.
- Adds `--input-type har` to accept HAR exports from Burp, Caido, ZAP, mitmproxy, or DevTools as a scan source.
- Adds `--analyze-external-js` to fetch and run AST DOM-XSS analysis on a target's same-origin `<script src>` bundles (capped at 16 files / 512 KiB).
- Adds `--detect-outdated-libs` (opt-in) to flag known-vulnerable front-end library versions as informational findings.
- Adds CSP & Trusted Types awareness: emits `strict-dynamic` / nonce gadget payloads and adapts when a Trusted Types policy is detected.

> +9 more

WAS THIS USEFUL? 👍 👎

◆ Secrets Detection & Management

Bitnami Sealed Secrets helm-v2.19.0 2 RELEASES · 2026-06-18

LATEST STABLE

A Kubernetes controller and tool for one-way encrypted Secrets

Helm chart v2.19.0 adds ppc64le support, default Prometheus alerting rules for out-of-sync secrets, and tightened pod security defaults.

└──▷ GET THIS VERSION

```
$ git clone --branch helm-v2.19.0 https://github.com/bitnami/sealed-secrets.git
# already have the repo? check out this version:
$ git checkout helm-v2.19.0
```

- Adds ppc64le architecture support, enabling Sealed Secrets controller deployment on IBM POWER clusters.
- Adds default PrometheusRule to the Helm chart that alerts when SealedSecrets are out of sync with their unsealed counterparts.
- Updates security context defaults to comply with the Kubernetes restricted pod security standard profile.

▾ 1 more release in this issue · 2026-06-18

v0.38.0 STABLE

Sealed Secrets v0.38.0 adds ppc64le support, default Prometheus alerting rules for out-of-sync secrets, and hardened pod security defaults.

└──▷ GET THIS VERSION

```
$ git clone --branch v0.38.0 https://github.com/bitnami/sealed-secrets.git
# already have the repo? check out this version:
$ git checkout v0.38.0
```

- Adds ppc64le architecture support, enabling Sealed Secrets controller and kubeseal to run on IBM Power (ppc64le) nodes.
- Adds a default PrometheusRule to the Helm chart that alerts when SealedSecrets are out of sync with their unsealed counterparts.

> › Updates security context defaults in the Helm chart to comply with the Kubernetes restricted pod security standard profile.

WAS THIS USEFUL? 👍 👎

REVERSE ENGINEERING, MALWARE & FORENSICS

◆ Reverse Engineering

Radare2 6.1.8

UNIX-like reverse engineering framework and command-line toolset

Radare2 6.1.8 adds JWT decoding, new demanglers, type-lookup commands, FTAB/idd/ `R_DYLDCACHE_NO_DEPS` , ESIL stepback, and PPC ESIL coverage.

└──▷ GET THIS VERSION

```
$ git clone --branch 6.1.8 https://github.com/radareorg/radare2.git
# already have the repo? check out this version:
$ git checkout 6.1.8
```

└──▷ TRY IT

Decode a JWT token found in a binary at the current seek position to inspect its header and claims.

```
$ r2 /path/to/binary
> s <address_of_jwt>
> pFJ
```

Look up which struct in the type database matches a known size (e.g., 16 bytes) — useful when reversing packed structures with no symbols.

```
$ r2 /bin/ls
> aaa
> tsn 16
```

Resolve an unknown numeric constant to its enum name to understand protocol or syscall values at a glance.

```
$ r2 /bin/ls
> aaa
> ten 3
```

- Adds `pFJ` command for JWT token decoding in the print subsystem.
- Adds `CLd` command for source-baked decompiler output.
- Adds `tsn` command to look up struct names by size.

› Adds `ten` command for enum lookup by numeric value.

› Adds `idd` command for binary info inspection.

+19 more

└──▷ BREAKING ON UPGRADE

! The `sdb_remove` function has been deprecated as a duplicate of `sdb_unset`

! The `asm.addr.base10` and `asm.addr.base36` config keys are unified into `asm.addr.base`

! The `esil.verbose` config key has been removed

! The default CPU for AVR is now `ATxmega128a4u`

! The `iz+` command now requires spaced arguments

WAS THIS USEFUL? 👍 👎

NETWORK SECURITY

◆ Firewalls & Network Defense

Rspamd 4.1.1

Rapid spam filtering system.

Rspamd 4.1.1 adds pluggable Neural registries, richer CSS text-hiding detection, zip-bomb limits, and new byte-analysis APIs.

└──▷ GET THIS VERSION

```
$ git clone --branch 4.1.1 https://github.com/rspamd/rspamd.git
# already have the repo? check out this version:
$ git checkout 4.1.1
```

- Adds pluggable feature-provider and ANN-architecture registries to the Neural module, plus a sequence output mode with SIF word selection for `fasttext_embed`, multi-head attention pooling in kann, and `slice` / `concat` graph transforms in lua_kann.
- Enables content-negotiation in checkv3 — representation and compression now negotiated via `Accept` / `Accept-Encoding` headers.
- Expands CSS text-hiding detection to cover off-screen positioning, clip, negative text-indent, and tiny fonts.
- Adds opt-in zip-bomb extraction limits (size, count, ratio) to `lua_archive` to bound archive expansion.
- New byte-distribution statistics methods in `lua_text`: entropy, byte mean/deviation, serial correlation, and Monte-Carlo Pi.

+2 more

WAS THIS USEFUL? 👍 👎

CLOUD & CONTAINER SECURITY

◆ Cloud Security Posture

Salesforce Cloudsplaining 0.9.0

Cloudsplaining is an AWS IAM Security Assessment tool that identifies violations of least privilege and generates a risk-prioritized report.

Cloudsplaining 0.9.0 adds 37 new privilege-escalation detections linked to pathfinding.cloud.

└──▷ GET THIS VERSION

```
$ git clone --branch 0.9.0
https://github.com/salesforce/cloudsplaining.git
# already have the repo? check out this version:
$ git checkout 0.9.0
```

└──▷ TRY IT

Generate a full account scan report that now includes pathfinding.cloud-linked privilege-escalation findings for all 37 new detection paths.

```
$ cloudsplaining scan --input-file examples/files/example.json --
exclusions-file examples/example-exclusions.yml --output
examples/report/
```

- Adds 37 new privilege-escalation path detections integrated with pathfinding.cloud, surfaced and linked directly in the HTML report.
- Enriches the built-in example dataset to produce a higher-quality demo report with more representative findings.

└──▷ BREAKING ON UPGRADE

! Python 3.9 is no longer supported

! Node 18 and Node 22 are no longer supported

WAS THIS USEFUL? 👍 👎

Prowler

5.32.0 | 3 RELEASES · 2026-06-11 → 2026-07-02 | LATEST | STABLE

Prowler is the world's most widely used open-source cloud security platform that automates security and compliance across any cloud environment.

Prowler 5.32.0 adds Kingfisher secret scanning, Azure resource-group scoping, Okta throttling, AWS resource caps, Neptune graph sink, and 6 new checks.

└─▷ GET THIS VERSION

```
$ git clone --branch 5.32.0 https://github.com/prowler-cloud/prowler.git
# already have the repo? check out this version:
$ git checkout 5.32.0
```

└─▷ TRY IT

Validate discovered secrets against live provider APIs so only working credentials are flagged critical — useful in CI to triage real leaks from noise.

```
$ prowler aws --scan-secrets-validate
```

Scope an Azure assessment to specific teams' resource groups to cut scan time and limit result scope during a targeted review.

```
$ prowler azure --az-cli-auth --azure-resource-group rg-prod1 rg-prod2
```

Prevent Okta rate-limit errors on large tenants by capping request rate and bounding retries.

```
$ prowler okta --okta-requests-per-second 2 --okta-retries-max-attempts 10
```

› New secret-scanning engine: replaces detect-secrets with Kingfisher, runs fully offline, suppresses placeholder false positives, and adds `--scan-secrets-validate` / `aws.secrets_validate` for live credential verification (confirmed live secrets reported as critical).

› Azure scans now support `--azure-resource-group` / `--azure-resource-groups` to scope assessments to one or more resource groups instead of the entire subscription.

› Okta provider adds configurable API request throttling (`--okta-requests-per-second` , default 4 req/s) and retry cap (`--okta-retries-max-attempts` , default 5) to survive rate limits on large tenant scans.

› AWS scans can now cap the number of resources analyzed per high-volume service via `max_scanned_resources_per_service` (global) or per-service limits: `max_ebs_snapshots` , `max_backup_recovery_points` , `max_cloudwatch_log_groups` , `max_lambda_functions` , `max_ecs_task_definitions` , `max_codeartifact_packages` .

› Attack Paths gains AWS Neptune as a persistent graph sink alongside Neo4j, selectable via `ATTACK_PATHS_SINK_DATABASE=neptune` , enabling managed, larger-scale cross-provider graph storage.

+13 more

└──▷ **BREAKING ON UPGRADE**

! The `detect_secrets_plugins` configuration option has been removed, as it is no longer used by the new secret-scanning engine (Kingfisher).

▾ **2 more releases in this issue** · 2026-06-11 → 2026-07-02

5.31.0 STABLE

Prowler 5.31.0 adds Linode provider, post-quantum AWS checks, DORA coverage for Azure/GCP/Cloudflare/Alibaba, and 30+ new checks across AWS, Azure, GCP, K8s, and M365.

└──▷ **GET THIS VERSION**

```
$ git clone --branch 5.31.0 https://github.com/prowler-cloud/prowler.git
# already have the repo? check out this version:
$ git checkout 5.31.0
```

.
.
.
.

└──▷ **TRY IT**

Scan a Linode account for security misconfigurations across administration, compute, and networking services.

```
$ prowler linode
```

Run all post-quantum cryptography readiness checks against your AWS environment to identify gaps before the quantum migration deadline.

```
$ prowler aws --checks cloudfront_distributions_pqc_tls_enabled
apigateway_domain_name_pqc_tls_enabled
transfer_server_pqc_ssh_kex_enabled
acmpca_certificate_authority_pqc_key_algorithm
rolesanywhere_trust_anchor_pqc_pki
```

Assess your AWS or Azure environment against the DORA regulatory framework to produce an EU Digital Operational Resilience Act compliance report.

```
$ prowler aws --compliance DORA_2022_2554
```

- New `linode` provider: scans Linode (Akamai Cloud) administration, compute, and networking services via `prowler linode`.
- New AWS post-quantum cryptography checks: `cloudfront_distributions_pqc_tls_enabled`, `apigateway_domain_name_pqc_tls_enabled`, `transfer_server_pqc_ssh_kex_enabled`, `acmpca_certificate_authority_pqc_key_algorithm` (new `acmpca` service), and `rolesanywhere_trust_anchor_pqc_pki` (new `rolesanywhere` service).
- New AWS org-wide governance checks: `securityhub_delegated_admin_enabled_all_regions` and `config_delegated_admin_and_org_aggregator_all_regions`.
- New AWS ML check: `sagemaker_clarify_exists` verifies at least one SageMaker Clarify processing job exists per region.
- Extends DORA (EU 2022/2554) compliance framework coverage to Azure, GCP, Cloudflare, and Alibaba Cloud under the `DORA_2022_2554` framework identifier.

`+9 more`

`5.30.0` STABLE

Prowler 5.30 adds full Okta DISA STIG coverage, a universal DORA compliance framework, 8 new checks across AWS/M365/GCP/StackIT, and self-healing background task recovery.

└──▷ **GET THIS VERSION**

```
$ git clone --branch 5.30.0 https://github.com/prowler-cloud/prowler.git
# already have the repo? check out this version:
$ git checkout 5.30.0
```

.
.

└──▷ **TRY IT**

Run all Okta DISA STIG V1R2 checks against your Okta tenant to assess compliance posture end-to-end.

```
$ prowler okta --compliance disa_okta_idaas_stig_v1r2_okta
```

Assess your AWS environment against DORA's five operational resilience pillars and export results in OCSF format for ingestion into a SIEM.

```
$ prowler aws --compliance dora_aws -M json-ocsf
```

Run the new ALB and SageMaker checks in isolation to validate specific FSBP and AI workload controls without a full scan.

```
$ prowler aws --check elbv2_alb_drop_invalid_header_fields_enabled sagemaker_models_monitor_enabled
```

- Adds complete DISA Okta IDaaS STIG V1R2 framework coverage for the Okta provider, spanning six new services: `user`, `authenticator`, `idp`, `network`, `apitoken`, and `systemlog` with 17 new checks covering account inactivity, MFA hardening, password policy, smart card, API token privilege, network zone enforcement, and log streaming.
- Introduces DORA (Digital Operational Resilience Act) as Prowler's first universal compliance framework — defined once and mapped across providers — currently covering AWS checks across the five DORA pillars and exportable in OCSF Compliance Finding format for SIEM ingestion.
- New AWS check `sagemaker_models_monitor_enabled` verifies each SageMaker monitoring schedule is in the `Scheduled` state to detect data and model drift.
- New AWS check `elbv2_alb_drop_invalid_header_fields_enabled` verifies Application Load Balancers drop invalid HTTP header fields to mitigate HTTP desync

attacks (AWS FSBP ELB.4).

› New AWS check `bedrock_agent_role_least_privilege` verifies Bedrock Agents run with a least-privilege IAM role.

+8 more

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ Endpoint Security (EDR/XDR)

CTFd 3.8.6

CTFs as you need them

CTFd 3.8.6 adds admin UI and API support for reclassifying correct submissions as incorrect.

└──▷ GET THIS VERSION

```
$ git clone --branch 3.8.6 https://github.com/CTFd/CTFd.git
# already have the repo? check out this version:
$ git checkout 3.8.6
```

└──▷ TRY IT

Programmatically revoke a correct submission (e.g., after detecting a flag-sharing violation) without touching the Admin UI.

```
$ curl -X PATCH https://<ctfd-host>/api/v1/submissions/42 \
  -H 'Authorization: Token <admin-token>' \
  -H 'Content-Type: application/json' \
  -d '{"correct": false}'
```

Manually invalidate a suspicious correct submission through the Admin Panel after reviewing solve logs.

> 📍 In the Admin Panel, go to Submissions, locate the correct submission, and click the new 'Mark as Incorrect' action.

- New Admin Panel UI to mark a previously correct submission as incorrect.
- PATCH `/api` /v1/submissions/[submission_id] now supports marking submissions as incorrect via the API.

WAS THIS USEFUL? 👍 👎

Fleet

fleet-v4.88.0 · 2 RELEASES · 2026-06-20 → 2026-07-02 · LATEST · STABLE

Open device management

Fleet v4.88.0 adds support for personal (BYOD) Apple MDM enrollment with per-host wipe/lock permission controls.

└──▷ GET THIS VERSION

```
$ git clone --branch fleet-v4.88.0
https://github.com/fleetdm/fleet.git
# already have the repo? check out this version:
$ git checkout fleet-v4.88.0
```

› Supports personal (BYOD) Apple MDM enrollment, tracking per-host enrollment permissions to prevent remote wipe or lock of personal devices, with permissions preserved across SCEP/ACME certificate renewal.

▾ 1 more release in this issue · 2026-06-20 → 2026-07-02

fleet-v4.87.0 · STABLE

Fleet 4.87.0 adds 963 new managed apps, Android MDM commands, Apple Business rebranding, GCS IAM auth, and a command palette.

└──▷ GET THIS VERSION

```
$ git clone --branch fleet-v4.87.0
https://github.com/fleetdm/fleet.git
# already have the repo? check out this version:
$ git checkout fleet-v4.87.0
```

└──▷ USE IT

Authenticate Fleet's software-installer storage to GCS using workload identity (ADC) instead of managing HMAC keys — useful in GKE or environments with Workload Identity Federation.

```yaml
s3_software_installers_gcs_iam_auth: true
```

Temporarily enable 100% trace sampling on a specific Fleet replica for a debug window without a restart.

```
$ curl -X PATCH https://fleet.example.com/debug/trace_sampler \
  -H 'Authorization: Bearer <admin-token>' \
  -H 'Content-Type: application/json' \
  -d '{"force_full": true}'
```

Target a configuration profile to hosts matching a label set while explicitly excluding hosts in a separate label group — combining include and exclude filters in a single profile upload.

```
$ fleetctl apply -f profile.yaml
# profile.yaml excerpt:
# labels_include_all: ["macOS 14+"]
# labels_exclude_any: ["Exempt from CIS benchmark"]
```

- Adds 236 new Fleet-maintained apps for Windows, including Microsoft Office, PowerShell, PowerToys, Power BI, Git, Node.js, Python 3.13/3.14, PostgreSQL 15–18, Nessus Agent, Bitwarden, and more.
- Adds 727 new Fleet-maintained apps for macOS, spanning development, security, productivity, and design tooling.
- Supports issuing Lock, Wipe, and Clear Passcode MDM commands to Android hosts; Wipe is available to Fleet Free users for company-owned Android devices.
- Enables deploying custom OS update configuration profiles for Apple and Windows hosts.
- Adds GCS IAM authentication (via Google Application Default Credentials) for software installers S3 storage, configurable via `s3_software_installers_gcs_iam_auth`.

+19 more

WAS THIS USEFUL? 👍 👎

EXPOSURE & VULNERABILITY MANAGEMENT

◆ Vulnerability Management

Future Architect Vuls v0.39.3

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

Vuls v0.39.3 switches Windows CVE detection to the vuls2 backend and expands EOL coverage for new OS versions.

└──▷ GET THIS VERSION

```
$ git clone --branch v0.39.3 https://github.com/future-architect/vuls.git
# already have the repo? check out this version:
$ git checkout v0.39.3
```

- Switches Windows KB-based CVE detection from gost to the vuls2 backend, now reading `vuls.db` built from `microsoft-*` sources (breaking change: gost is no longer used for Windows; a `vuls.db` containing `microsoft-*` data is required).
- Surfaces MSRC Exploit Status under `CveContent.Optional["exploit"]` for Windows detections, maintaining parity with the previous gost output.
- Adds EOL data for newly released OS versions via updated `GetEOL` configuration.

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Secure Access (VPN / SASE / ZTNA)

Headscale v0.29.0

An open source, self-hosted implementation of the Tailscale control server

Headscale v0.29.0 adds SSH check-mode auth, policy tests, grants, Taildrive, nodeAttrs, and HA subnet router health probing.

└──▷ GET THIS VERSION

```
$ git clone --branch v0.29.0
https://github.com/juanfont/headscale.git
# already have the repo? check out this version:
$ git checkout v0.29.0
```

└──▷ TRY IT

Approve a pending SSH check-mode or web auth request identified in server logs, granting the user access without re-keying.

```
$ headscale auth approve --auth-id <id>
```

Validate a policy file's `tests` and `sshTests` blocks before pushing it live, catching reachability regressions without affecting running nodes.

```
$ headscale policy check
```

- New `headscale auth` CLI command group: `approve`, `reject`, and `register` subcommands manage SSH check-mode and web auth approval flows.
- Supports Tailscale SSH `"action": "check"` rules, prompting OIDC or CLI approval before granting SSH access to a node.
- Evaluates the `tests` block in policy files (beta), asserting reachability between sources and destinations; failing tests block writes before they are applied.
- Evaluates the `sshTests` block in policy files (beta), asserting SSH reachability with `accept`, `deny`, and `check` user lists per source/destination pair.
- Adds support for Tailscale Grants (`grants` block in policy), enabling application-level controls like Taildrive file sharing and traffic steering via tagged subnet routers or exit nodes.

+12 more

└──▷ BREAKING ON UPGRADE

- ! MagicDNS `GivenName` collision suffix changed from 8-char random hash (`laptop-abc12xyz`) to monotonic numeric suffix (`laptop` , `laptop-1` , `laptop-2` , …); MagicDNS names change on upgrade for any node whose previous label was a random-suffix form
- ! Empty or all-non-ASCII hostnames now fall back to the literal `node` instead of `invalid-<rand>`
- ! Wildcard (`*`) in ACL sources and destinations now resolves to the Tailscale CGNAT range (`100.64.0.0/10`) and ULA range (`fd7a:115c:a1e0::/48`) instead of all IPs (`0.0.0.0/0` and `::/0`); policies relying on `*` to match all IP addresses must switch to `autogroup:danger-all` (source only) or explicit CIDR ranges (destinations)
- ! Policies using tags, hosts, or IP addresses as sources for `autogroup:self` destinations now fail validation
- ! `proto:icmp` now only includes ICMPv4 (protocol 1); ICMPv6 must be specified explicitly as `proto:ipv6-icmp` or protocol number `58`
- ! Skipping minor versions (e.g. 0.27 → 0.29) is blocked; upgrades must proceed one minor version at a time, and downgrading to a previous minor version is blocked
- ! The `randomize_client_port` server-config key was removed; headscale refuses to start when the old key is present — the toggle must be moved to the policy file as the top-level `randomizeClientPort` field
- ! Minimum supported Tailscale client version is now v1.80.0

WAS THIS USEFUL? 👍 👎

Tonari innernet v2.0.0

A private network system that uses WireGuard under the hood.

innernet v2.0.0 adds custom host suffix, client endpoint override, verbose full public keys, and a new innernet-client-core Rust library

└──▷ GET THIS VERSION

```
$ git clone --branch v2.0.0 https://github.com/tonarino/innernet.git
# already have the repo? check out this version:
$ git checkout v2.0.0
```

└──▷ TRY IT

Assign a custom DNS suffix (e.g. `.corp.example`) to all peers on the network instead of the default `<interface>.wg`.

```
$ sudo innernet-server serve <interface> --host-suffix corp.example
```

Inspect full public keys of all peers when diagnosing connectivity — useful when truncated keys are ambiguous.

```
$ sudo innernet --verbose list <interface>
```

Manually pin a peer's advertised endpoint (e.g. behind a NAT or load balancer) so other peers connect to the correct address.

```
$ sudo innernet override-endpoint <interface>
```

- Adds `--host-suffix` CLI option to client and server to override the default `<interface>.wg` hostname suffix.
- Adds `override-endpoint` command to the client, enabling manual peer endpoint specification without going through the server.
- Prints full WireGuard public keys (instead of truncated 10-char versions) when the global `--verbose` flag is used.
- Introduces new `innernet-client-core` Rust library crate exposing create_peer_and_invitation(), `set_listen_port`, `redeem_invite`, and `fetch` APIs for programmatic integration.

└──▷ **BREAKING ON UPGRADE**

! The Rust libraries `innernet-client-core`, `innernet-server`, and `innernet-shared` have semver-incompatible API changes requiring a major version bump for consumers of these crates

WAS THIS USEFUL? 👍 👎

BUILD

◆ **AI Coding Agents**

Windsurf `snapshot-20260706`

Windsurf is an AI-powered code editor that helps developers write, edit, and navigate code faster using intelligent autocomplete and agentic AI assistance.

└──▷ **TRY IT**

Check the live status of all connected MCP servers mid-session to verify tool availability before delegating a task.

```
$ /mcp
```

Review current ACU consumption without leaving the chat interface — useful for tracking usage against quota during a long autonomous session.

```
$ /usage
```

› Edits produced in autonomous (Devin Local) mode now generate reviewable diffs instead of silent changes.

› Enforces enterprise login policies in the CLI.

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

▷ Subscribe