CIRCL
Computer Incident
Response Center
Luxembourg

GCVE.eu

GCVE: Rebooting Vulnerability Tracking for an Open Security Ecosystem

From a decentralised identifier to running public infrastructure

https://gcve.eu – https://db.gcve.eu

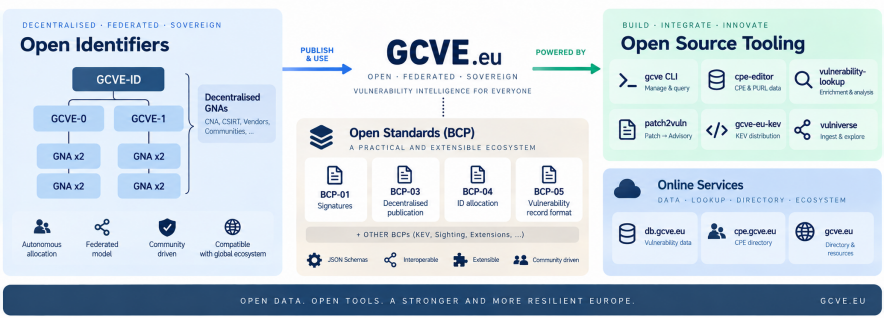
Alexandre Dulaunoy, CIRCL
Cedric Bonhomme, CIRCL

VulnOpticon 2026 – 23 September 2026

CIRCL – Computer Incident Response Center Luxembourg
https://gcve.eu – https://vulnerability-lookup.org

Why GCVE

The story in 30 minutes



The core message: **GCVE is not only a new identifier format**; it is a way to make vulnerability tracking open, attributable and operational.

Vulnerability tracking is public infrastructure

- Defenders need stable identifiers to know **what to patch**, **what is exploited**, and **what affects their assets**.
- Vendors and maintainers need a **publication path** that matches their disclosure process and timeline.
- Researchers and CSIRTs need a way to publish **structured facts** without waiting for a single global bottleneck.
- Regulators and communities increasingly rely on vulnerability data as **evidence**, not just as a catalogue.

When the **naming and publication layer** is slow or fragile, every downstream security process inherits that fragility.

The pressure on the old model

The ecosystem became faster

- More **code**, dependencies and suppliers.
- More **automated discovery**.
- More **open-source** and vendor disclosure flows.
- More **public vulnerability intelligence**.

The coordination path did not scale equally

- Central queues can become **operational chokepoints**.
- **Local evidence** may arrive before a central record exists.
- **Correction**, enrichment and exploitation signals evolve over time.

The question changed from "who may assign a number?" to "how can many trusted actors publish useful vulnerability knowledge without losing attribution?"

GCVE in one sentence

GCVE lets independent **GCVE Numbering Authorities**[1] allocate and publish vulnerability identifiers autonomously, while remaining interoperable through **open practices, feeds and tooling**.[2]

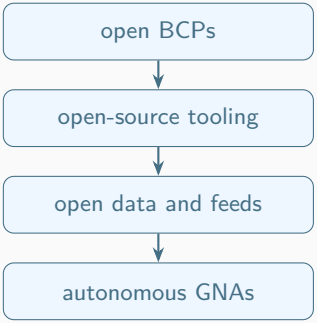
- Compatible with **CVE** and other vulnerability ecosystems.[3]
- Designed for **decentralised publication** and synchronisation.[4]
- Built around **attribution**, **provenance** and open implementation.

[1] https://gcve.eu/gna/
[2] https://gcve.eu/bcp/
[3] https://gcve.eu/bcp/gcve-bcp-04/
[4] https://gcve.eu/bcp/gcve-bcp-03/

Strategic intent

- **Sovereignty**: control the publication path.
- **Autonomy**: each GNA keeps its operational reality.
- **Independence**: open tooling and reproducible data flows.
- **Fast innovation**: standards shaped by **running code**.[a]

[a] https://gcve.eu/bcp/



The goal is not isolation. The goal is optionality: no single actor needs to control every stage of vulnerability tracking.

The model

The identifier model

`GCVE-<GNA>-<LOCAL-ID>`

GNA

The **globally assigned namespace** identifying an autonomous vulnerability publisher.

LOCAL-ID

The identifier is **defined and managed autonomously by the GNA**.

Convention

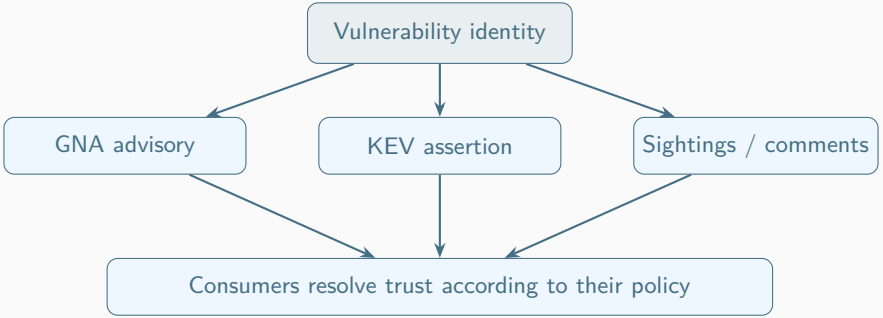
A GNA can use the familiar `YEAR-ID` model, or another locally appropriate scheme.

`GCVE-1-2026-12345` **or** `GCVE-<GNA>-<GNA-defined value>`

GCVE provides the **global GNA namespace**; each GNA remains autonomous in how identifiers are allocated within its namespace.[5]

[5] https://gcve.eu/bcp/gcve-bcp-04/

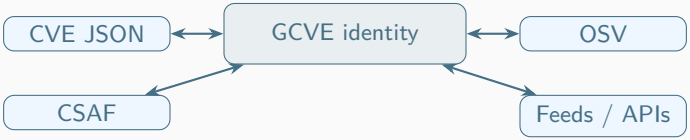
From central record to attributable views



Federation does not remove disagreement; it makes disagreement visible, attributable and machine-readable.

Format agnostic by design

- GCVE separates the **identifier and publication model** from any single record syntax.
- The core format is compatible with **CVE JSON 5.x**, with reusable extensions for additional evidence and provenance.[6]
- GCVE identifiers can be referenced from **CSAF**, **OSV**, vulnerability databases, advisories and local workflows.



[6] https://gcve.eu/bcp/gcve-bcp-05/

One year of execution

From announcement to ecosystem

Date	Milestone
Apr 2025	**GCVE announced** as a decentralised vulnerability identifier and allocation system.[7]
Jan–Feb 2026	db.gcve.eu becomes public and **Vulnerability-Lookup 4.0** adds federation.[8]
May 2026	**Vulnerability-Lookup 5.0** adds practical GNA / CVD workflows.[9]
Jun 2026	cpe.gcve.eu launches as collaborative **product and CPE curation** infrastructure.[10]
Aug–Sep 2026	**BCP work expands**: KEV directory, sightings, contribution models, AI provenance and more.[11]
Sep 2026	New producers such as **VULNARCHIVE** show automatic GNA-based allocation in practice. **Vulniverse editor** released.

The project evolved by adding **working layers**, not by waiting for a complete final standard.

[7] https://gcve.eu/
[8] https://db.gcve.eu/
[9] https://www.vulnerability-lookup.org/
[10] https://cpe.gcve.eu/

The running network today

GNA directory[a]

- **46** registered GNAs.
- **40** web resources.
- **7** API endpoints.
- **Public registry** and downloadable JSON.

Source: `https://gcve.eu/gna/`

[a] https://gcve.eu/gna/

Vulnerability-Lookup[a]

- **2.5M+** vulnerabilities.
- **85** sources.
- **Open-source**, AGPLv3.
- **GCVE-native** publication and correlation.
- **Used by many organisations** such as CSIRTs, EUVD.

Source: `https://db.gcve.eu/about`

[a] https://db.gcve.eu/about

GCVE is already inspectable as **data, software, services** and independent participants.

Best Current Practices: the backbone[12]

BCP	Purpose	Role
BCP-01	Signature verification of the GNA directory	trust bootstrap
BCP-02	Practical vulnerability handling and disclosure	CVD guidance
BCP-03	Decentralised publication standard	publishing
BCP-04	Identifier allocation	namespace rules
BCP-05	GCVE vulnerability record and extensions	data model
BCP-07	KEV assertion format and directory	exploitation evidence
BCP-10	CPE / product curation model	product context
BCP-12	Vulnerability sighting model	operational observation

BCPs keep the standards close to **operational practice**: document what works, then make it reusable.

[12] https://gcve.eu/bcp/

Open-source tooling delivered - connected by open formats and public data

Publication and correlation

- **Vulnerability-Lookup**[a]: GNA operations, publication, correlation, sightings.
- **gcve client and registry tooling**[b]: signed directory, machine-readable metadata.
- **gcve-eu-kev**[c]: KEV feed conversion and assertions.

[a] https://www.vulnerability-lookup.org/
[b] https://github.com/gcve-eu
[c] https://github.com/gcve-eu/gcve-eu-kev

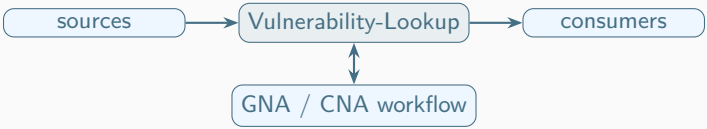
Curation and assistance

- **cpe-editor**[a]: collaborative CPE / PURL curation.
- **patch2vuln**[b]: draft advisory records from Git patches.
- **VulnTrain / VLAI**[c]: open data, models and experimentation.
- **vulniverse**[d]: Vulniverse is a web-based advisory editor.

[a] https://github.com/gcve-eu/cpe-editor
[b] https://github.com/gcve-eu/gcve-lab-patch2vuln
[c] https://github.com/vulnerability-lookup/VulnTrain
[d] https://github.com/vulnerability-lookup/vulniverse

Vulnerability-Lookup became the reference implementation

- Collects and correlates vulnerability information from many sources, **independent of identifier format**.[13]
- Supports **CNA / GNA advisory preparation** with Vulnogram integration.
- Synchronises **comments, sightings and bundles** between instances.
- Implements **GCVE-native publication workflows** and public dumps.[14]



[13] https://www.vulnerability-lookup.org/
[14] https://db.gcve.eu/

CPE.GCVE.EU: fixing the unglamorous problem

- Vulnerability management fails when the **product identity** is wrong.
- Vendors rename products, open-source projects move, aliases multiply, and package identifiers do not always map cleanly to CPE.
- `cpe.gcve.eu`[15] adds collaborative **vendor, product, CPE and PURL curation** with proposals, moderation and API access.

GCVE is not only about **naming vulnerabilities**. It also helps improve the **product context** needed to use vulnerability data correctly.

[15] https://cpe.gcve.eu/

KEV assertions: exploitation without a single oracle

- **Exploitation evidence** is one of the strongest prioritisation signals.
- BCP-07 models **KEV information as attributable assertions** rather than a single universal truth.[16]
- The **KEV directory** makes catalogues discoverable and machine-readable.[17]
- Initial sources include **CISA, CIRCL, ENISA, Shadowserver and Previdian**.

Different observers can publish **different exploitation views**; consumers can compare them instead of inheriting one hidden policy.

[16] https://gcve.eu/bcp/gcve-bcp-07/

[17] https://vulnerability.circl.lu/known-exploited-vulnerabilities-catalog/

AI assistance: useful only when accountable

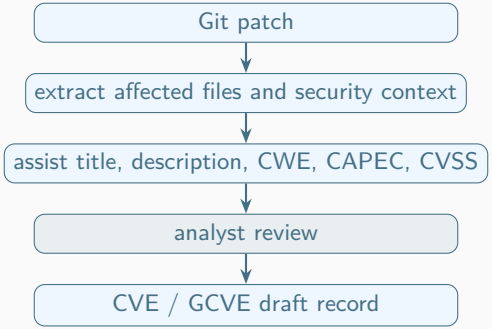
- **AI-assisted code review and triage** increases the amount of vulnerability material to process.
- GCVE treats AI output as **evidence or annotation**, not as an authority.
- BCP-05 extensions support **explicit provenance** for AI-assisted enrichment and classification.[18]
- **Human review remains critical** before operational publication decisions.

> Automation should increase **analyst leverage** without hiding how a conclusion was produced.

[18] https://gcve.eu/bcp/extension/gcve-bcp-05-x-01/

patch2vuln: from a Git patch to a draft record[19]

```
python3 patch2vuln.py \
  --gcve-id gcve-1-2026-20206 \
  --vendor misp --product misp \
  https://github.com/MISP/misp/commit/382188d2f.patch
```



[19] https://github.com/gcve-eu/gcve-lab-patch2vuln

Community growth: the model is being reused

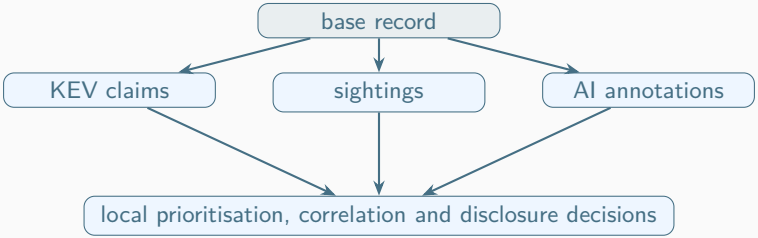
- GNAs now include **CSIRTs, vendors, open-source projects, vulnerability databases** and experimental producers.[20]
- The **signed directory** turns participation into machine-readable infrastructure.[21]
- **VULNARCHIVE / GNA 1988** demonstrates automatic identifier assignment in a federated producer model.[22]
- The **GCVE workshop and VulnOpticon week** show a community moving from concept to shared practice.

A federated vulnerability ecosystem succeeds when **other producers can join** without asking the original operator to run their workflow.

[20] https://gcve.eu/gna/
[21] https://gcve.eu/bcp/gcve-bcp-01/
[22] https://vuln.freearchive.org/

What comes next

The next phase: from records to evidence graphs



The useful object is not one static record; it is a living set of **attributable observations** around a stable identity.

Active workstreams

1. **BCP-11**[23]: community-proposed updates to existing records, without erasing authority boundaries.
2. **BCP-12**[24]: sightings as first-class operational observations.
3. **Embargo-aware extensions**: coordinated publication state without premature disclosure.
4. **Private GNA ecosystems**: identifiers useful inside bounded trust domains.
5. **OSV / CSAF interoperability**: GCVE as a bridge, not another silo.[25]
6. **Local Exploit Hazard**: moving from global severity to local exposure.

[23] https://discourse.ossbase.org/t/gcve-bcp-11-community-proposed-updates-to-existing-cve-records/1110
[24] https://gcve.eu/bcp/gcve-bcp-12/
[25] https://gcve.eu/bcp/gcve-bcp-05/

What we still need to improve

Technical

- Stronger **validation and test suites** for BCPs.
- More **converters** for existing advisory ecosystems.
- Better **product identity**, CPE/PURL mappings and version ranges.
- More **synchronisation patterns** between instances.

Community

- More **independent GNAs** and KEV producers.
- More **review** of proposed BCPs and extensions.
- Clearer **operational guidance** for CSIRTs, PSIRTs and open-source maintainers.
- More examples of **real CVD workflows**.

The next success metric is not only more records; it is more **independent, reusable and trustworthy** production of vulnerability knowledge.

How to take part

If you publish vulnerability information

- Become a **GNA** if you fit the eligibility model.[a]
- Publish a **BCP-03/BCP-05 compatible feed**.[b]
- Add **KEV assertions or sightings** where you have evidence.[c]

[a] https://gcve.eu/gna/
[b] https://gcve.eu/bcp/gcve-bcp-03/
[c] https://gcve.eu/bcp/gcve-bcp-07/

If you consume vulnerability information

- Mirror the data and **verify signatures**.[a]
- Run your own **Vulnerability-Lookup** instance.[b]
- Test the **CPE editor, patch2vuln, VLAI and converters**.[c]

[a] https://gcve.eu/bcp/gcve-bcp-01/
[b] https://github.com/vulnerability-lookup/vulnerability-lookup
[c] https://gcve.eu/software/

GCVE is deliberately open to **specialised use-cases**: tell us where the model does not yet fit your operational reality.

Takeaways

1. **GCVE moved from concept to infrastructure**: directory, GNAs, BCPs, open-source tooling and running services.
2. **Decentralisation is practical**: publication, KEV assertions, sightings and enrichment can be independent but interoperable.
3. **Compatibility matters**: CVE, CSAF and OSV remain part of the ecosystem.[26]
4. **The future is evidence-rich**: records will be surrounded by provenance, observations, corrections and local context.

Rebooting vulnerability tracking means making the ecosystem **more open, more resilient and more useful** to the people who operate it.

[26] https://gcve.eu/bcp/gcve-bcp-05/

References

- GCVE initiative: https://gcve.eu/
- GNA directory: https://gcve.eu/gna/
- Vulnerability-Lookup: https://vulnerability-lookup.org/ and https://db.gcve.eu/
- GCVE BCPs: https://gcve.eu/bcp/
- Open data: https://gcve.eu/opendata/
- Software catalogue: https://gcve.eu/software/
- CPE editor: https://cpe.gcve.eu/
- Contact: info@gcve.eu – Mastodon: @gcve@social.circl.lu

Thank you

Questions?

https://gcve.eu
https://db.gcve.eu