CIRCL
Computer Incident
Response Center
Luxembourg

GCVE.eu

GCVE

A Decentralized Approach to Vulnerability Allocation, Publishing and Management

https://vulnerability-lookup.org – https://gcve.eu/

---

info@gcve.eu - @→ @gcve@social.circl.lu

GCVE Workshop Vulnopticon 2026

CIRCL https://www.circl.lu

TLP:CLEAR

Strategy and Motivation

GCVE strategic intent

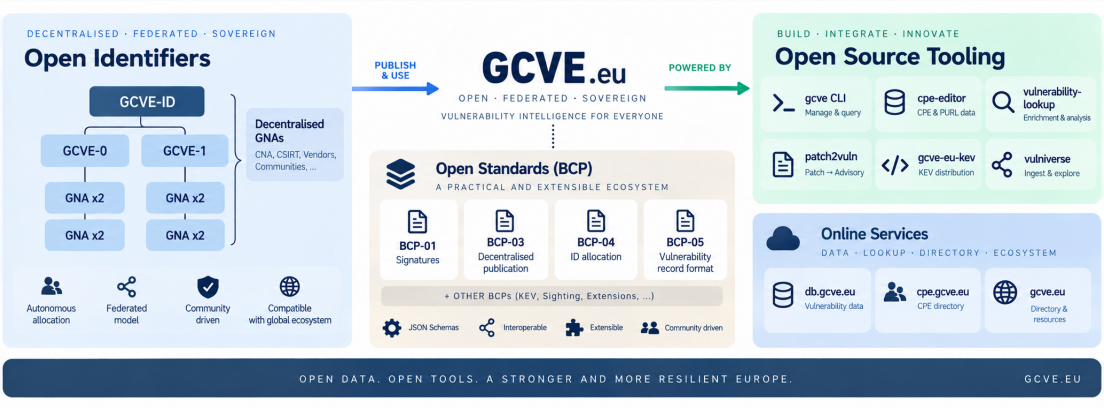
GCVE initiative was officially launched the 16th April 2025[1].

- **Sovereignty**
- **Autonomy**
- **Independence**
- **Fast innovation**

GCVE initative has the strategy to make vulnerability coordination **federated, open, attributable and operational**.

[1] The original idea came from the self-publication service in vulnerability-lookup.

GCVE overview



TLP:CLEAR

Sovereignty: control the naming and publication path

- Vulnerability coordination must not depend on a single operational or political chokepoint.
- Organisations need a way to publish from their own trusted infrastructure.
- **A public identifier should support coordination, not become a publication blocker**.

> Sovereignty means that the source of truth can remain close to the actor responsible for the disclosure.

Autonomy: each GNA keeps its operational reality

- Each GCVE Numbering Authority (GNA)[2] defines its own scope.
- **Each GNA controls its process and publication rhythm**.
- National, sectoral, vendor and open-source workflows can coexist.

Autonomy avoids forcing every disclosure case into one global workflow.

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

Independence: open tooling, reproducible data flows

- Open specifications[3] make the model inspectable and implementable by others.
- Open-source tooling[4] reduces dependency on a single service provider.
- Implementations can run locally, nationally, sectorally or inside an organisation.

Independence is both technical and operational: the process remains reproducible.

[3] https://gcve.eu/bcp/
[4] https://gcve.eu/software/

Fast innovation: standards, but with running code

- Some standards are designed by committee, but the process can be too slow to keep pace with and **support innovation in CVD processes**.
- GCVE uses Best Current Practices[5], public review and running code[6].
- New operational needs require new standards and fast implementation.

> Fast innovation means improving the model while it is already usable.

[5] https://gcve.eu/bcp/
[6] https://db.gcve.eu/

Why now? From dependency to capability

- **Vulnerability disclosure is now a critical operational function**.
- CSIRTs, vendors, manufacturers, open-source projects and researchers need to publish quickly and responsibly.
- Centralised allocation can create delays, ambiguity and single points of failure.

GCVE shifts the model from **permission to publish** toward **accountable self-publication**.

The key question

Who controls the

timeline, **revision process** and **publication endpoint**?

GCVE makes those controls explicit, attributable and reusable.

Format agnostic by design

- GCVE separates the **identifier and publication model** from a specific record syntax.
- A GCVE can be referenced, transported or mapped across existing ecosystems.
- The project favours compatibility over replacement.

GCVE should fit into existing CVD and vulnerability-intelligence pipelines.

Compatibility targets

The GCVE core format is a **standard CVE record**[7] **with additional extensions**. All GCVE extensions can also be used as extensions in other formats.

Existing formats

- CVE Record Format[a]
- CSAF
- OSV

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

GCVE layer

- Identifier allocation[a]
- Publication endpoint[b]
- Extensions via BCPs

[a] https://gcve.eu/bcp/gcve-bcp-04/
[b] https://gcve.eu/bcp/gcve-bcp-03/

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

GCVE in a CVD process: timeline control per publisher

- Reserve or allocate when the case exists operationally.
- Prepare the record while coordination continues.
- Publish when the disclosure process is ready.
- Update later when new evidence, remediation or exploitation data appears.

The publisher controls the timeline instead of waiting for a remote bottleneck.

GCVE in a CVD process: publication and collaboration

- Self-publication: the GNA remains authoritative for its own records.
- Revision-friendly: records can evolve with better evidence.
- Collaboration-friendly: attribution, references[8] and extensions support multiple contributors.
- Faster publication: the public name can appear when it is needed.

CVD moves from **waiting for an identifier** to **publishing attributable vulnerability knowledge**.

[8] https://gcve.eu/bcp/gcve-bcp-05/#relationships-field

Recent initiative, concrete deliveries

Already operational

- GNA namespace
- Signed machine-readable directory
- GNAs publishing in the GCVE ecosystem
- GNAs using identifiers in other ecosystems

Already reusable

- Best Current Practices
- Open-source reference tooling
- Vulnerability-Lookup integration
- Public community review

GCVE is recently established, but it is already more than a proposal.

Delivered capabilities

- Decentralised publication model for GNAs.
- Machine-readable records and discovery.
- Operational extensions: KEV assertions, sightings and provenance.
- Tooling around Vulnerability-Lookup, CPE.GCVE.EU and patch2vuln.

> The initiative already has specifications, infrastructure, software, data flows and a growing community.

From strategy to the technical deep dive

- Identifier allocation and GNA namespaces.
- Directory, signatures and trust.
- Publication through APIs, dumps or advisory formats.
- Interoperability with CVE, CSAF, OSV and vulnerability-intelligence platforms.
- Automation with Vulnerability-Lookup[9], CPE.GCVE.EU[10], KEV conversion and patch2vuln.

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

Open Identifiers: GCVE

Who defines the identity of a vulnerability?

- An identifier is the name used to coordinate around the same problem.
- Today, many processes depend on a centrally allocated public name.
- Delays or disagreement can leave a vulnerability without a usable public identifier.

Can vulnerability identification be part of an open, decentralised ecosystem?

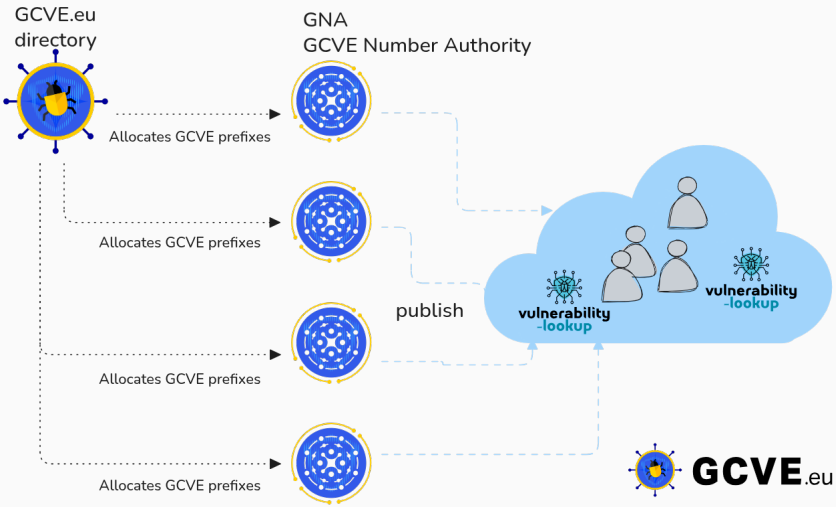
GCVE: the Global CVE Allocation System

- A decentralised allocation system for vulnerability identifiers.
- GNAs allocate identifiers autonomously[11].
- Format: `GCVE-<GNA-ID>-<YEAR>-<UNIQUE-ID>`.
- Example: `GCVE-1-2026-0020`.
- GNA 0 maps the CVE namespace.

GCVE does not replace CVE, CSAF or OSV. It removes a single point of failure in how vulnerabilities get an identifier.

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

Overview


GCVE.eu
directory
GNA
GCVE Number Authority
Allocates GCVE prefixes
Allocates GCVE prefixes
Allocates GCVE prefixes
Allocates GCVE prefixes
publish
vulnerability
-lookup
vulnerability
-lookup
GCVE.eu

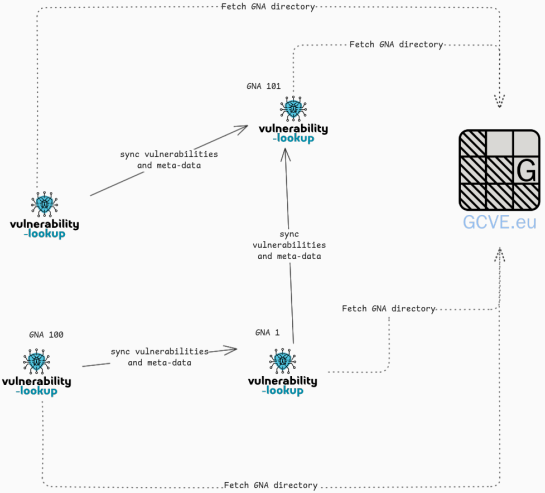
Principles: disagreement is a feature

- **Each GNA decides what is in scope and what is published.**
- Records are attributed to their source.
- **Cross-references[12] make relationships explicit.[13]**
- Consumers decide which GNAs they trust.

> Centralised systems resolve disagreement by authority. Federated systems resolve it by attribution and transparency.

[12] https://gcve.eu/bcp/gcve-bcp-05/#relationships-field
[13] https://vulnerability.circl.lu/vuln/GCVE-1-2025-0032

A distributed network of GNAs



TLP:CLEAR

Who is publishing already?

- 46 GNAs in the directory as of September 2026.
- Existing participants include CSIRTs, vendors, open-source projects, researchers and vulnerability databases.
- Seven new GNAs joined during summer 2026 alone.
- Some automatic GNAs were added such as 1988[14].

The network is still recent, but it is already diverse.

https://gcve.eu/gna/

[14] https://vuln.freearchive.org/

Who can become a GNA?

- Existing CNA.
- CSIRT/CERT listed on FIRST.org, TF-CSIRT or the EU CSIRTs Network.
- **Vendor**[15] **regularly disclosing vulnerabilities** in its own products.
- Actor with a public disclosure policy and an accessible GCVE-BCP-05 feed.

[15] Including open-source organisations or developers

What a GNA gets

- Fast onboarding once eligible.
- Its own namespace.
- **Ability to publish immediately**.
- Ability to apply identifiers to historical advisories or specific automation workflow[16].
- Incremental adoption of BCPs.

[16] GNA 1988 example `https://vuln.freearchive.org/`

What a GNA gives up

- The comfort of someone else deciding.
- Anonymity: records are attributed[17].
- Hidden disputes: disagreement becomes visible and reviewable[18].
- The excuse: “the CVE is not out yet”.

Sovereignty comes with accountability.

[17] A GNA could still use the GNA prefix to make private publishing.
[18] Security researchers can directly act as publisher.

Best Current Practices: foundations

ID	Title	Status
BCP-01	Signature Verification of the Directory File	Published
BCP-02	Practical Guide to Vulnerability Handling and Disclosure	Published
BCP-03	Decentralized Publication Standard	Published
BCP-04	Recommendations and Best Practices for ID Allocation	Published
BCP-05	GCVE Vulnerability Format	Published
BCP-06	Requirements and Evaluation Criteria for GNAs	Draft

Public review: `https://gcve.eu/bcp/` – `https://discourse.ossbase.org/c/gcve/14`

Best Current Practices: operational extensions

ID	Title	Status
BCP-07	Known Exploited Vulnerability – KEV Assertion Format	Published
BCP-08	GCVE GNA Directory File	Draft
BCP-09	Scope of a GCVE Record	Draft
BCP-10	Improved Common Platform Enumeration for GCVE	Draft
BCP-11	Community-Proposed Updates to Existing CVE Records	Draft
BCP-12	Sighting Format	Draft

Extensions: BCP-05-X-01 (AI-assisted annotation provenance), BCP-05-X-02 (patch-to-vulnerability provenance).

Thank you for your attention

- Issues, new sources of advisories or ideas:
  `https://github.com/vulnerability-lookup/vulnerability-lookup`
- Support and questions: info@circl.lu
- Become a GNA: gna@gcve.eu
- GCVE **@gcve@social.circl.lu**