



GCVE.eu



GNA
GCVE.eu

GCVE: Global CVE Allocation System

GCVE Backstage: BCPs, Tooling, and Hackathon Opportunities

 <https://www.gcve.eu/>

Alexandre Dulaunoy - alexandre.dulaunoy@circl.lu

April 14 2026

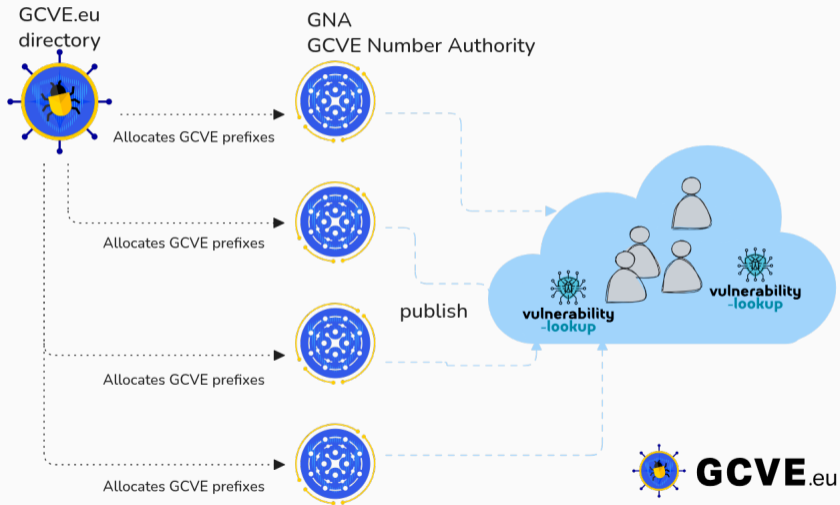
CIRCL <https://www.circl.lu>

- CIRCL has developed several open-source tools, including MISP and Vulnerability-Lookup¹, a project designed to manage vulnerabilities—from data collection to publication.
- We identified the need for a **simpler, more autonomous process for allocating vulnerability identifiers**.
- While the existing CNA process (part of the CVE Program) provides structure and consistency, it can be challenging for some publishers due to its procedural requirements.
- A certain level of resilience is essential, independently of geopolitical challenges.

¹<https://vulnerability-lookup.org>

- The primary role of GCVE is to provide **globally unique identifiers** to GCVE Numbering Authorities (GNAs).
- **GNAs operate autonomously**, with full control over how they assign and manage identifiers.
- **GCVE publishes Best Current Practices (BCPs)** on directory management, Coordinated Vulnerability Disclosure (CVD), and publication protocols.
- GCVE maintains and publishes the **official directory of all GNAs**, including their publication endpoints.

GCVE.eu - overview



- You are an existing CNA recognized by the CVE Program.
- You are not a CNA, but **meet at least one of the following conditions**²:
 - You are a registered CSIRT or CERT listed on FIRST.org, part of the EU CSIRTs Network, or a member of TF-CSIRT.
 - You are a software, hardware, or service provider that regularly discloses vulnerabilities affecting your own products or services, and you have an official CPE vendor name assigned.
 - You have a public vulnerability disclosure policy and maintain a GCVE-BCP-05 publicly accessible source for newly disclosed vulnerabilities.

²<https://gcve.eu/about/#eligibility-and-process-to-obtain-a-gna-id>

- **Fast, straightforward onboarding:** as soon as the eligibility criteria are met, registration is quick and simple.
- **Flexible identifier usage:** you may publish new CVE entries immediately and apply your assigned prefix to both current and historical identifiers.
- **Autonomy over publication:** each GNA determines for itself what constitutes a vulnerability and what information is made public.
- **Incremental adoption of BCPs:** additional GCVE Best Current Practices can be adopted over time; implementing every BCP is encouraged but not mandatory.

Published Best Current Practices (BCPs)

ID	Title	Status	Ver.	Published
GCVE-BCP-01	Signature Verification of the Directory File	PUB	1.1	25 Apr 2025
GCVE-BCP-02	Practical Guide to Vulnerability Handling and Disclosure	PUB	1.5	25 Jan 2026
GCVE-BCP-03	Decentralized Publication Standard	PUB	1.0	10 Jun 2025
GCVE-BCP-04	Recommendations and Best Practices for ID Allocation	PUB	1.3	02 Oct 2025
GCVE-BCP-05	GCVE Vulnerability Format (Updated CVE Record Format)	PUB	1.6	02 Jan 2026
GCVE-BCP-07	Known Exploited Vulnerability - KEV Assertion Format	PUB	1.9	27 Jan 2026

Draft and public documents are always open for public review.

<https://gcve.eu/bcp>

<https://vulnerability-lookup.org> is the reference GCVE implementation

TLP:CLEAR

Best Current Practices (BCPs) — Pre-Draft

ID	Title	Status	Ver.	Discussed
GCVE-BCP-06	Requirements and Evaluation Criteria for GCVE Numbering Authorities	PRE-DRAFT	–	Ongoing
GCVE-BCP-08	GCVE GNA Directory File (Structure and Semantics)	PRE-DRAFT	–	Ongoing
GCVE-BCP-09	GCVE-BCP-09: Scope of a GCVE Record	PRE-DRAFT	–	Ongoing
GCVE-BCP-10	GCVE-BCP-10 : Improved Common Platform Enumeration for GCVE	PRE-DRAFT	–	Ongoing

Pre-draft documents are discussed publicly before formal drafting begins.

<https://discourse.ossbase.org/c/gcve/14>

- GCVE reserves a set of GNA IDs for existing programs such as GHSA, the CVE Program, and EUVD.
- This approach **ensures compatibility and interoperability with established systems.**
- GCVE acts as a complementary framework that **enables autonomous publication and identifier assignment.**
- GCVE can be viewed as a functional equivalent to IANA for prefix allocation in the vulnerability coordination space.

Hackathon Opportunity: Build on the GCVE Dataset

- GCVE is not only a specification and an allocation model: it also comes with an **existing public dataset of vulnerabilities** available at:
 - JSON dumps - <https://vulnerability.circl.lu/dumps/>
 - API - <https://db.gcve.eu/api/>
- During the hackathon, you can reuse these dumps to quickly prototype:
 - search and correlation tools across multiple vulnerability sources,
 - visualisations, dashboards, or trend analysis,
 - data quality checks, deduplication, and enrichment pipelines,
 - tooling for sightings, KEV tracking, or bundle generation,
 - integrations with your own asset inventory, SBOM, or alerting workflows.
- **No need to start from scratch:** the data is already there, ready to be explored, transformed, and integrated into new ideas.

Hackathon Opportunity: Better Product & Vendor References in GCVE

- **GCVE-BCP-10** aims to improve how products and vendors are identified and normalized in vulnerability records.
- During the hackathon, we will work on a **cpe-editor**³ prototype to:
 - review and correct CPE entries,
 - normalize vendor/product names,
 - reduce duplicates and ambiguous references.
- This is also an opportunity to explore complements to CPE, such as:
 - purl,
 - SWID,
 - SPDX / CycloneDX identifiers,
 - package registries and upstream repositories.
- Goal: more accurate, maintainable, and practical software references in GCVE.

³<https://github.com/adulau/cpe-editor>

Hackathon Ideas Around GCVE

- Build practical tools around the GCVE ecosystem: **allocation workflows, validation, decentralized publishing, synchronization, and trust.**
- Explore operational use cases such as history tracking, enrichment, deduplication, search, sightings, and KEV-driven workflows.
- Improve product and vendor references in GCVE, including work on the **cpe-editor** prototype and alternative software identifiers.
- Reuse the existing public vulnerability dataset to prototype dashboards, integrations, correlation engines, or analysis tools.
- Experiment with new ideas that make GCVE **easier to publish**, consume, verify, and operate in practice.

- GCVE is an experiment in making vulnerability identification and publication more **decentralized, practical, and open**.
- Beyond the numbering model, GCVE is also about building an ecosystem: shared data, synchronization, better software references, and interoperable tooling.
- The hackathon is an opportunity to turn these ideas into concrete prototypes, from data reuse and enrichment to validation, search, and **cpe-editor**.
- The goal is simple: make vulnerability information easier to publish, improve, consume, and operate at scale.
- **If these challenges sound interesting, join us and build with GCVE.**

Thank You for Your Attention

- For questions, want to join the initiative or become a GNA, contact: info@gcve.eu
- Want to experiment with GCVE, Vulnerability-Lookup, or new GNA workflows? **Come talk to us during the hackathon.**