GCVE: Global CVE Allocation System

Enhancing Flexibility, Scalability, Autonomy, and Resilience in Vulnerability Identification

🏠 https://www.gcve.eu/

Alexandre Dulaunoy - alexandre.dulaunoy@circl.lu

November 25, 2025 - Distro Security Team WG

CIRCL https://www.circl.lu

TLP:CLEAR

GCVE.eu - History

- CIRCL has developed several open-source tools, including MISP and Vulnerability-Lookup[1], 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.

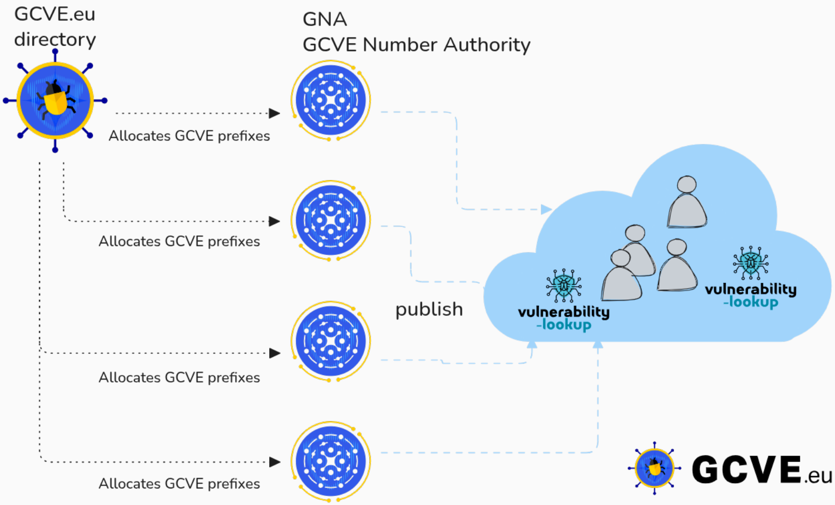
[1] https://vulnerability-lookup.org - https://vulnerability.circl.lu/

TLP:CLEAR

GCVE.eu - Role

- 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



GCVE.eu - Who Can Be a GNA?

- 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 publicly accessible source for newly disclosed vulnerabilities.

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

TLP:CLEAR

GCVE.eu — Benefits of Becoming a GNA

- **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.

TLP:CLEAR

GCVE.eu - Best Current Practices (BCPs)

- **GCVE-BCP-01**[3] — *Signature Verification of the Directory File*
  Status: PUBLISHED (Public Review) **Version:** 1.1
  Published: 25 April 2025
- **GCVE-BCP-02** — *Practical Guide to Vulnerability Handling and Disclosure*
  Status: DRAFT (Public Review) **Version:** 1.2
  Published: 28 July 2025
- **GCVE-BCP-03** — *Decentralized Publication Standard*
  Status: DRAFT (Public Review) **Version:** 1.0
  Published: 10 June 2025
- **GCVE-BCP-04** — *Recommendations and Best Practices for ID Allocation*
  Status: DRAFT (Public Review) **Version:** 1.2
  Published: 2 October 2025

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

TLP:CLEAR

GCVE-BCP-01 - Signature Verification of the Directory File

- This BCP ensures that consumers of the GCVE directory file[4] can cryptographically verify its authenticity and integrity before parsing or trusting its contents.
- A Python client and library for the Global CVE Allocation System[5] is available and includes an integrity validator for the GCVE directory JSON.
- Tools that rely on the GCVE directory **SHOULD** automate this validation and **MUST** raise an alert or abort the workflow if the signature check fails.

[4] https://gcve.eu/dist/gcve.json

[5] https://github.com/gcve-eu/gcve

GCVE-BCP-02 — Practical Guide to Vulnerability Handling and Disclosure

- This BCP[6] provides actionable recommendations for software developers, open-source project maintainers, and organizations to manage vulnerability reports from discovery through resolution and coordinated public disclosure. The guidance is organized around the key stages of a vulnerability's life-cycle: preparation, receipt, triage, investigation, remediation, and communication.
- The document is aimed at GNA, which requires a public disclosure guide with concrete recommendations.
- GCVE recommends that GNA **SHOULD** adopt the practices described in this guide.

[6] https://gcve.eu/bcp/gcve-bcp-02/

TLP:CLEAR

GCVE-BCP-03 - Decentralized Publication Standard

- The decentralized model standard[7] is **based on the principle that each GNA has full control over its own publication process**. The GCVE directory then provides a way to discover the entry points for collecting vulnerability information from your trusted set of GNAs, allowing users to decide whom to trust and from whom to pull vulnerability information.
- The transport mechanism used to gather vulnerability information relies on HTTP, with two modes of access via a single URL.
- The URL is referenced in the GCVE directory under the `gcve_pull_api` field.

[7] https://gcve.eu/bcp/gcve-bcp-03/

GCVE-BCP-03 - API End Point

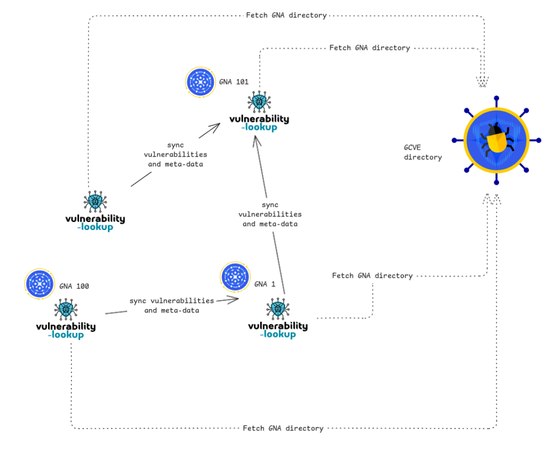
- The API endpoint is defined in the field `gcve_pull_api`, which must support at least the following API endpoints:
  - `/api/vulnerability/recent/` – Retrieves vulnerabilities reported after a specified date, with optional filters for source and number of results.
  - `/api/vulnerability/last/` – Retrieves the latest vulnerabilities, with optional filters for source and number of results.
- GCVE-BCP-03 does not enforce a specific JSON format for vulnerability publication.
- However, the recommended format—also used in the reference implementation[8]—is the CVE Record Format[9] extended in the future GCVE-BCP-05[10].

[8] https://www.vulnerability-lookup.org/

[9] https://github.com/CVEProject/cve-schema/blob/main/schema/CVE_Record_Format.json

[10] https://discourse.ossbase.org/t/gcve-bcp-05-drafting-best-practices-for-the-container-format-modified-cve-record-format/121

GCVE-BCP-03 — Decentralized Publication Standard Overview



TLP:CLEAR

GCVE-BCP-04: Scope & Purpose

Goal. Provide guidance to GNAs for allocating **consistent, valid and interoperable** GCVE identifiers.

What BCP-04 defines

- Canonical and alternative GCVE ID formats
- Length, character set and validation rules
- Allocation principles ensuring uniqueness and clarity

Design Objectives

- Human-readable identifiers
- Compatibility with existing vulnerability ecosystems
- Freedom for GNAs, without a central authority blocking publication

Source: GCVE-BCP-04 — `https://gcve.eu/bcp/gcve-bcp-04/`

TLP:CLEAR

GCVE-BCP-04: Identifier Formats

Canonical Format (recommended)

- `GCVE-<GNA-ID>-<YEAR>-<UNIQUE-ID>`

Alternative Format (allowed)

- `GCVE-<GNA-ID>-<GNA-VALUE>`
- Printable 7-bit characters only (no whitespace/control chars)

Length

- Maximum: **255 characters** (prefer shorter for tooling compatibility)

Examples

- `GCVE-0-2024-13987`
- `GCVE-65535-GHSA-jc7w-c686-c4v9` (test GNA example)

TLP:CLEAR

GCVE-BCP-04: Validation & Allocation Principles

Validation

- Validation rules and regex are defined in BCP-04 for format and length compliance.
- Ensures identifiers remain both **machine-parseable** and **human-readable**.

Allocation Principles

- IDs must be **unique** within each GNA
- Multiple IDs across GNA may describe the **same vulnerability**
- Cross-reference other GCVE IDs and external systems
- IDs may cover: new vulns, metadata, patches or variants

Consistent formatting = easier federation, lookup and automation.

TLP:CLEAR

GCVE.eu – Comparison with Other Initiatives

- 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.

Conclusion

- GCVE is an open program, GNAs can easily join, and the BCP process is active and open to contributions from the community.
- The publication standard is implemented as a reference in the open-source *vulnerability-lookup*[11] software, but it can be easily integrated into other tools or services.
- Existing **GNAs are already publishing autonomously**, and anyone can freely choose which GNA to retrieve information from.

[11] `https://vulnerability-lookup.org`

Thank You for Your Attention

- For questions, want to join the initiative or become a GNA, contact: `info@gcve.eu`

Co-funded by
the European Union