CIRCL
Computer Incident
Response Center
Luxembourg

GCVE.eu

Advancing Vulnerability Tracking and Disclosure Through an Open and Distributed Platform

Unlock Your Brain Harden Your System 2025

https://www.vulnerability-lookup.org

Alexandre Dulaunoy - alexandre.dulaunoy@circl.lu Cédric Bonhomme - cedric.bonhomme@circl.lu

November 8, 2025

CIRCL https://www.circl.lu 

TLP:CLEAR

Origin of the project

Who is behind Vulnerability-Lookup?

Vulnerability-Lookup[1] is an Open Source project led by **CIRCL**.
It is co-funded by **CIRCL** and the **European Union**[2].
Used by many organisations including CSIRTs and ENISA (EUVD).
A reference implementation to **GCVE** standards.

vulnerability
-lookup

[1] https://www.vulnerability-lookup.org
[2] https://github.com/ngsoti

Origin

- `cve-search`[3] is an open-source tool initially developed in late 2012, focusing on maintaining a **local** CVE database.
- `cve-search` is widely used as an **internal** tool.
- The design and scalability of cve-search are limited. Our operational public instance at https://cve.circl.lu has reached a hard limit of 20,000 queries per second.
- Vulnerability sources have **diversified**, and the **NVD CVE is no longer the sole source** of vulnerability information.

[3] `https://github.com/cve-search/cve-search`

Initial Challenges

- **Volume of data:** Handling a substantial dataset and heavy network traffic, currently over 1,755,144 security advisories and more than 150,000 sightings[4].
- **Flexibility:** Balancing ongoing development with legacy issues while designing a future-proof architecture. It's complex and yes, sometimes chaotic[5].
- **Robustness:** Validating data even when external entities don't comply with their own JSON schemas. It's not always pretty.
- **Fast lookup:** Rapidly correlating identifiers across **diverse sources**, including unpublished advisories.

[4] The first sighting on Exploit-DB dates back 26 years.
[5] We enjoy challenges, especially when they lead to practical solutions.

Ongoing Challenges and Development

- **CPE fragmentation:**[6] Tackling the fragmentation of CPEs (e.g., `cpe:/a:oracle:java` vs. `cpe:/a:sun:java`) by introducing *Organizations* as unified containers.
- **CVD process:** Building an open-source tool that fully supports the Coordinated Vulnerability Disclosure (CVD) process.[7]
- **Vulnerability numbering:** Enabling a new distributed approach through the Global CVE Allocation System.[8]
- **Scoring vulnerabilities:** Aggregating a large volume of observations from diverse advisory types to improve vulnerability scoring.

[6] Well, another mess to clean up!
[7] Aligned with NIS 2 and the Cyber Resilience Act.
[8] `https://gcve.eu`

It's a lot of sources!

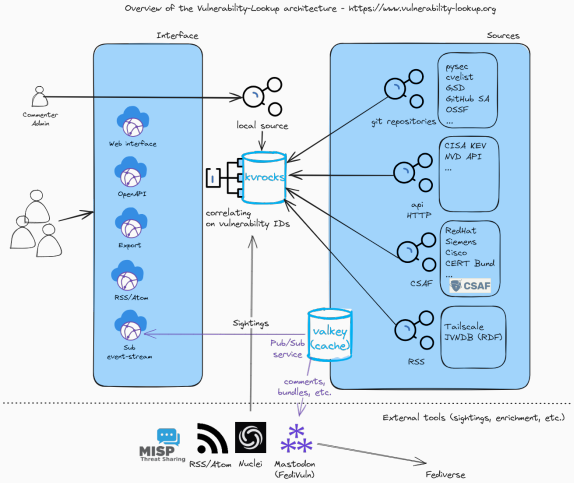
- **CVE Program** Git
- **NIST NVD CVE** API 2.0
- **Fraunhofer FKIE CVE** Git
- **GitHub Advisory Database** Git
- **Python Advisory Database** Git
- **Cloud Security Alliance - GSD** Git
- **VARIoT** API
- **GCVE.eu all GNA sources** API
- **CSAF 2.0** (HTTP CSAF)
  CERT-Bund, Cisco, Siemens, ABB, Red Hat, Suse, OpenSuse, Microsoft, NCSC-NL, CISA, etc.
- **Japan - JVN DB** HTTP
- **China - CNVD** HTTP
- **CERT-FR** HTTP
- **Tailscale** RSS
- **CISA KEV, EU KEV** HTTP
- **CWE, CAPEC, MITRE EMB3D** HTTP

Open Data Initiative: Regular JSON dumps published[9].

[9] https://vulnerability.circl.lu/dumps/

Design and Implementation

Vulnerability-Lookup High-Level Architecture



TLP:CLEAR

Extended API

```
$ curl -s https://vulnerability.circl.lu/api/vulnerability/last/csaf_redhat/10 | jq .[2].document.title
"Red Hat Security Advisory: Red Hat Ceph Storage 6.1 security and bug fix update"

$ curl -s https://vulnerability.circl.lu/api/vulnerability/last/csaf_redhat/10 | jq .[2].vulnerabilities[0].cve
"CVE-2021-4231"
```

- **Documented API** (OpenAPI): https://vulnerability.circl.lu/api
- Pagination and filtering by source
- CPE search by vendor and product name
- **Many endpoints available via RSS and Atom**[10]

[10] https://www.vulnerability-lookup.org/documentation/feeds.html

Empowering the Community

Crowd-Sourced Threat Intelligence

- **Bundles:** Group similar vulnerabilities and aggregate sightings for easier tracking.
- **Comments:** Additional context such as PoCs, remediations, related insights.
- **Tags:** Use the MISP Vulnerability Taxonomy to annotate comments[11]. Example:

```
vulnerability:information=remediation
```

- **Sightings:** Report real-world observations of vulnerabilities, including metadata like timestamps and sources.


```
{
  "uuid": "f9ec8b2c-2ceb-4c05-b052-264b51c6a3ee", "vulnerability_lookup_origin": "1a89b78e-f703-45f3-bb86-59eb712668bd",
  "author": "9f56dd64-161d-43a6-b9c3-555944290a09", "creation_timestamp": "2025-04-17T19:14:32.000000Z",
  "vulnerability": "CVE-2025-32433",
  "type": "exploited",
  "source": "https://gist.github.com/numanturle/b7333fb02a4ee3618995babc9b62c507"
}
```


[11] https://www.misp-project.org/taxonomies.html#_vulnerability_3

Types of Sightings

Type	Description	Negative/Opposite
`seen`	The vulnerability was mentioned, discussed, or observed by the user.	No
`confirmed`	The vulnerability has been validated from an analyst's perspective.	Yes
`published-proof-of-concept`	A public proof of concept is available for this vulnerability.	No
`exploited`	The vulnerability was observed as exploited by the user who reported the sighting.	Yes
`patched`	The vulnerability was observed as successfully patched by the user who reported the sighting.	Yes

Table 1: Types of vulnerability sightings

Automated Sightings: Tools and Sources

Automatically gathering crowd-sourced intelligence without requiring direct user contributions to our platform.

- **Social Platforms:** Fediverse, Bluesky
- **Threat Intelligence Tools:** MISP, Nuclei
- **Content Feeds:** RSS/Atom, curated web pages, GitHub Gist
- **Specialized Projects:** ShadowSight, ExploitDBSighting, Metasploit
- **Community Contributions:** Passive signals and indirect data enrichment

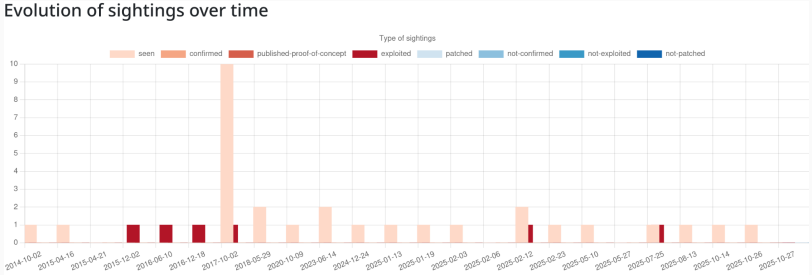
Scoring Vulnerabilities

Sightings Detection Rate and Types of Sightings

- A high rate of sightings (type *seen*) often correlates with high or critical severity vulnerabilities[12].
- Early sightings of type *exploited* (e.g., proof-of-concept code) or *confirmed* (e.g., detection templates for tools like Nuclei) can signal emerging threats.
- Sightings can sometimes be detected **before any official advisory is published**.
- Continuous exploitation patterns are frequently observed through sources like The Shadowserver Foundation or MISP.
- Recent work on forecasting sightings evolution[13]

[12] Don't underestimate the hype surrounding some vulnerabilities.
[13] `https://github.com/vulnerability-lookup/TARDISsight`

Evolution of sightings over time

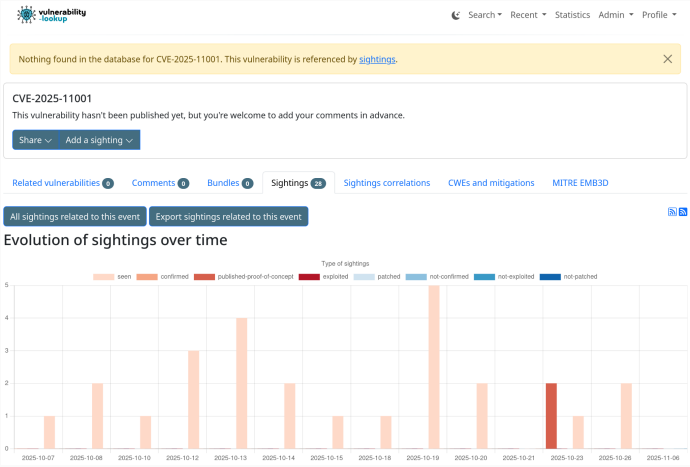


Sightings

Author	Source	Type	Date
automation	https://gist.github.com/meirdev/9456cc133c7718206f32c0d5528671a4 (correlations)	seen	10 days ago
cedric	https://rulezet.org/rule/detail_rule/40653 (correlations)	seen	11 days ago
automation	MISP/a41d8549-5384-5e1a-8c33-bf88e35b5a0a (correlations)	seen	23 days ago
automation	https://gist.github.com/tauzen/e0a07a80095b49f1c46cdc8d09e52264 (correlations)	seen	2 months ago
automation	The Shadowserver (honeypot/exploited-vulnerabilities) - (2025-07-25) (correlations)	exploited	3 months ago
automation	https://gist.github.com/edgarcosta/934eb264e54da84a497ce3f607ba247b (correlations)	seen	5 months ago

https://vulnerability.circl.lu/vuln/CVE-2014-6271#sightings

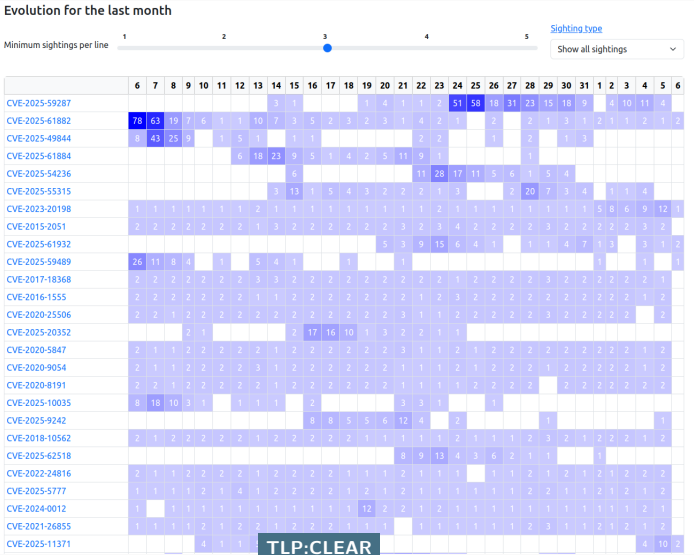
Evolution of sightings over time



https://vulnerability.circl.lu/vuln/CVE-2025-11001#sightings

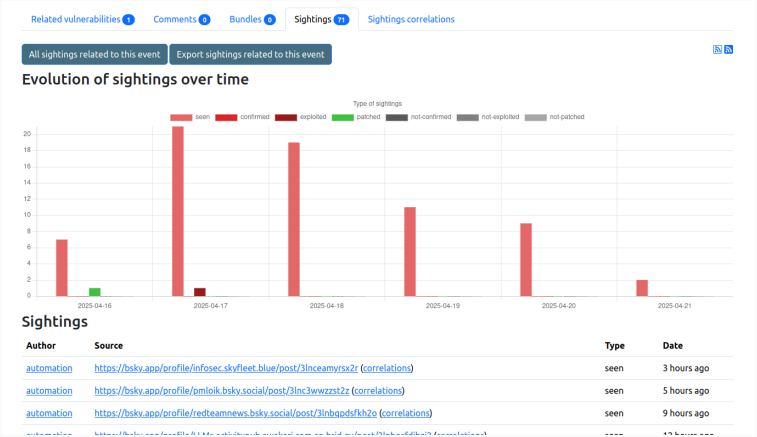
TLP:CLEAR

Tracking CVEs via their sightings



TLP:CLEAR

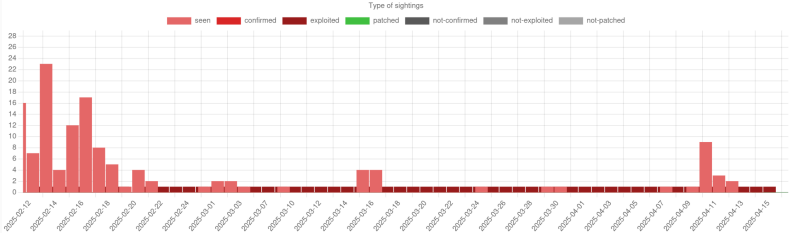
Early PoC (erlang / otp)



https://vulnerability.circl.lu/vuln/CVE-2025-32433#sightings

Continuous Exploitations (Palo Alto Networks / Cloud NGFW)

Evolution of sightings over time



Sightings

Author	Source	Type	Date
automation	The Shadowserver (honeypot/exploited-vulnerabilities) - (2025-04-16) (correlations)	exploited	1 day ago
automation	https://bsky.app/profile/christopherkunz.bsky.social/post/3lmu2zatyx22z (correlations)	seen	2 days ago
automation	https://chaos.social/users/christopherkunz/statuses/114340622271163262 (correlations)	seen	2 days ago
automation	The Shadowserver (honeypot/exploited-vulnerabilities) - (2025-04-15) (correlations)	exploited	2 days ago

https://vulnerability.circl.lu/vuln/CVE-2025-0108#sightings

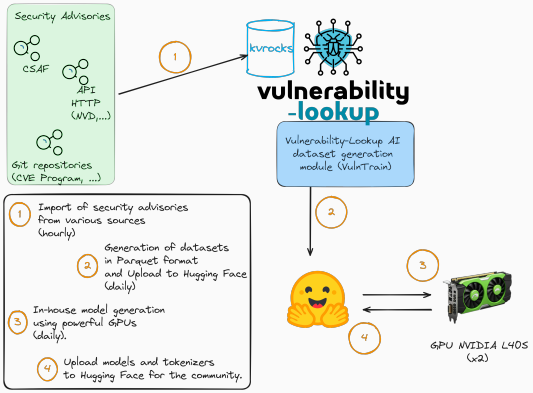
- **Speedify VPN (macOS):** https://vulnerability.circl.lu/vuln/CVE-2025-25364#sightings
  - Low visibility, no EPSS score, few sightings

Sightings

Author	Source	Type	Date
automation	https://infosec.exchange/users/dragonjar/statuses/114364291565132421 (correlations)	seen	1 day ago
automation	https://bsky.app/profile/r-netsec.bsky.social/post/3ln4hb7anxx2q (correlations)	seen	2 days ago
automation	https://bsky.app/profile/r-netsec-bot.bsky.social/post/3ln4arcbktd2z (correlations)	seen	2 days ago
automation	https://infosec.exchange/users/threatcodex/statuses/114217935883108579 (correlations)	seen	27 days ago

Toward Practical AI Applications

Completing Missing Data with AI



- Some vulnerabilities are published without CVSS score.
- **Predicts severity from the vulnerability description** before an official score is available.
- Available as a standalone model or via the CIRCL public instance.
- To address this, we developed **VLAI Severity**[a], a model trained on the Vulnerability-Lookup dataset.
- Open Source Datasets and Trainers[b]

[a] https://arxiv.org/abs/2507.03607
[b] https://github.com/vulnerability-lookup/VulnTrain

Current datasets

Dataset	Size (rows)	Generation Time	Features
vulnerability-scores[14]	652,590	10m45s	Descriptions (en), CVSS, CPE
vulnerability-CNVD[15]	124,099	1m35s	Descriptions (cn), CVSS
vulnerability-cwe-patch[16]	15,836 (18,435 patches)	60m	Descriptions (en), CWE, patches (commit id + url + full diff)

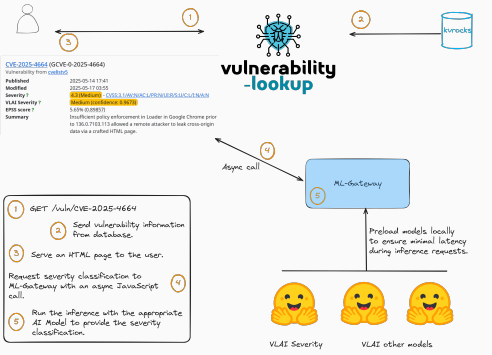
[14] https://huggingface.co/datasets/CIRCL/vulnerability-scores
[15] https://huggingface.co/datasets/CIRCL/Vulnerability-CNVD
[16] https://huggingface.co/datasets/CIRCL/vulnerability-cwe-patch

Current models

Model	Size	Epochs	Accuracy	Training Time
Severity classification[17]	0.1B params	5	0.8240	6.72h
Severity classification (CNVD)[18]	0.1B params	5	0.7817	65.989m
CWE guessing[19]	0.1B params	36-40	0.7464	43m

[17] https://huggingface.co/CIRCL/vulnerability-severity-classification-roberta-base
[18] https://huggingface.co/CIRCL/vulnerability-severity-classification-chinese-macbert-base
[19] https://huggingface.co/CIRCL/cwe-parent-vulnerability-classification-roberta-base

Integration for inference



The case of missing severity information in the advisory.

- Optional integration[a]
- No dependencies with Vulnerability-Lookup
- Models are pulled from Hugging Face and preloaded locally
- Documented API (OpenAPI) to trigger the inferences

[a] https://github.com/vulnerability-lookup/ML-Gateway

Lookup is Cool, but Publishing is Even Cooler

GCVE.eu - Role

- The primary role of GCVE[20] 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.

[20] `https://gcve.eu`

GCVE.eu - Who Can Be a GNA?

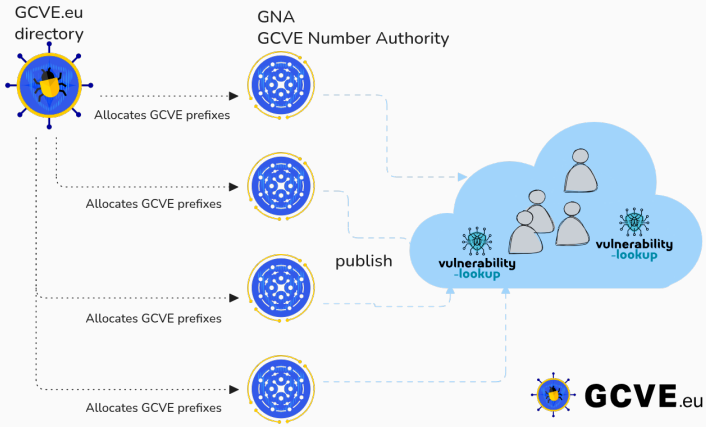
- You are an existing CNA recognized by the CVE Program.
- You are not a CNA, but **meet at least one of the following conditions**[21]:
  - You are a registered CSIRT or CERT listed on FIRST.org, part of the EU CSIRTs Network, or a member of TF-CSIRT.
  - You are a software, hardware, or service provider 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.

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

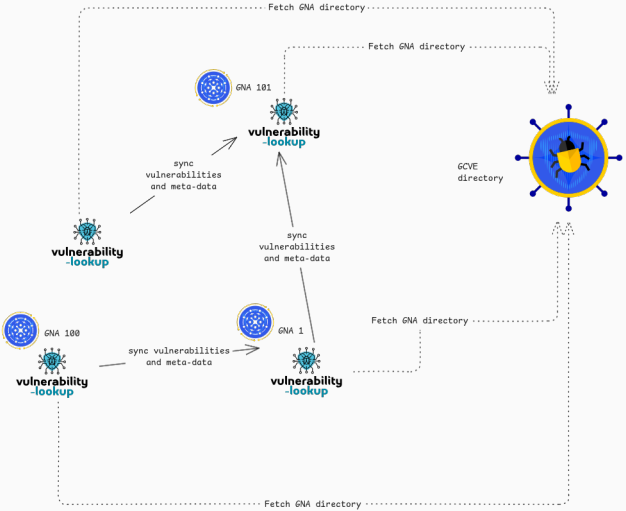
GCVE.eu – Comparison with Other Initiatives

- 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.

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

Decentralized Publication Standard



TLP:CLEAR

Closing

Future Development

- Deeper analysis of the content and context of sightings, including **source reliability assessment**.
- Integration of **forecasting models** based on sightings.
- Full-text search capabilities across all integrated sources.
- **Improved notification capabilities** for newly observed vulnerabilities via webhooks.
- and more:
  `https://github.com/vulnerability-lookup/vulnerability-lookup/issues`

The project is evolving rapidly — feedback and feature suggestions are always welcome!

References

https://www.vulnerability-lookup.org

https://vulnerability.circl.lu

https://github.com/vulnerability-lookup/vulnerability-lookup

https://huggingface.co/CIRCL