



CIRCL
Computer Incident
Response Center
Luxembourg



GCVE.eu

Vulnerability-Lookup: Beyond CVEs

SIG-ISM Meeting - 10th Anniversary 2025 - Madrid, Spain

 <https://www.vulnerability-lookup.org>

Cédric Bonhomme - cedric.bonhomme@circl.lu - <https://www.linkedin.com/in/cedricbonhomme>

October 8, 2025

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

1. Origin of the project
2. Design and Implementation
3. Empowering the Community
4. Scoring Vulnerabilities
5. Toward Practical AI Applications
6. Publishing security advisories

Origin of the project

Who is behind Vulnerability-Lookup?



Vulnerability-Lookup¹ 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://www.restena.lu/en/project/ngsoti>

Origin of Vulnerability-Lookup

- `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 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 1,732,364 security advisories and more than 140,000 sightings⁴.
- **Flexibility:** Balancing ongoing development with legacy issues while designing a future-proof architecture. It's complex and yes, sometimes chaotic⁵.
- **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- **Fast lookup:** Rapidly correlating identifiers across **diverse sources**, including unpublished advisories.

⁴The first sighting on Exploit-DB dates back 26 years.

⁵We 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.

⁶Well, another mess to clean up!

⁷Aligned with NIS 2 and the Cyber Resilience Act.

⁸<https://gcve.eu>

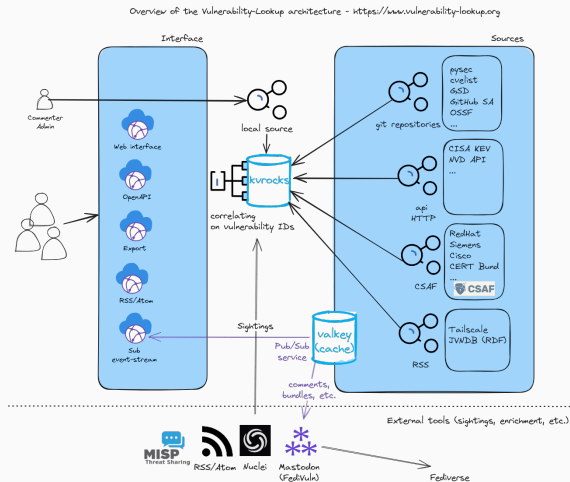
Current sources in Vulnerability-Lookup

- **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** API
- **CSAF 2.0 (HTTP CSAF)**
CERT-Bund, Cisco, Siemens, Red Hat, Suse, OpenSuse, Microsoft, NCSC-NL, CISA, etc.
- **Japan - JVN DB** HTTP
- **China - CNVD** HTTP
- **CERT-FR** HTTP
- **Tailscale** RSS
- **CISA KEV** HTTP
- **EU KEV** HTTP
- **Growing...**

Design and Implementation

Vulnerability-Lookup High-Level Architecture

- Collects and aggregates vulnerability data.
- Preserves data integrity (never alters the original content).
- Harmonizes data using kvrocks.
- Correlates information across multiple sources (CVE, PySec, etc.).
- Provides both APIs and a Web interface.
- Supports advanced queries and filtering.



```
$ curl -s 'https://vulnerability.circl.lu/api/vulnerability/?per_page=10&page=1&source=csaf_siemens' |  
  jq .[2].document.title  
"SSA-722410: Multiple Vulnerabilities in User Management Component (UMC)"  
  
$ curl -s 'https://vulnerability.circl.lu/api/vulnerability/?per_page=10&page=1&source=csaf_siemens' |  
  jq .[2].vulnerabilities[0].cve  
"CVE-2025-40795"
```

- **Documented API** (OpenAPI): <https://vulnerability.circl.lu/api>
- Pagination and filtering by source
- Search by vendor and product name
- **Many endpoints available via RSS and Atom⁹**

⁹<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 comments¹⁰. 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/b7333fb02a4ee3618995bab9b62c507"  
}
```

¹⁰https://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.	-
confirmed	The vulnerability has been verified by an analyst.	X
exploited	The vulnerability was actively exploited and observed by the user reporting the sighting.	X
patched	The vulnerability was successfully mitigated or patched by the user reporting the sighting.	X

Table 1: Types of vulnerability sightings

Automated Sightings: Tools and Sources

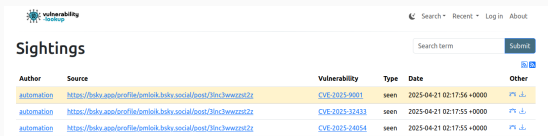
Automatically gathering crowd-sourced intelligence without requiring direct user contributions to our platform.

- **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 vulnerabilities¹¹.
- 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**.



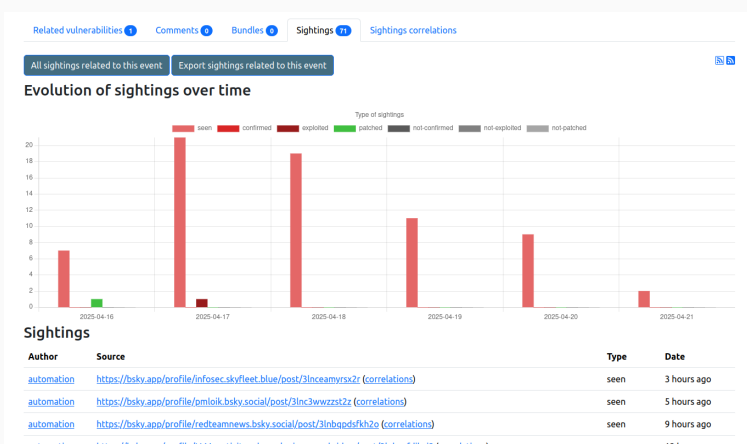
The screenshot shows the 'Vulnerability Sighting' website. At the top, there's a navigation bar with 'Search', 'Recent', 'Log in', and 'About'. Below this is a search bar with a 'Submit' button. The main heading is 'Sightings'. Below the heading is a table with columns: Author, Source, Vulnerability, Type, Date, and Other. The table contains three rows of data, all with 'automation' as the author and 'https://bsky.app/profile/omisoik.bsky.social/post/3lnc3wvzczst2z' as the source. The vulnerabilities listed are CVE-2025-9001, CVE-2025-32433, and CVE-2025-24054. All three are of type 'seen' and dated '2025-04-21 02:17:56 +0000', '2025-04-21 02:17:55 +0000', and '2025-04-21 02:17:55 +0000' respectively. Each row has a link icon in the 'Other' column.

Author	Source	Vulnerability	Type	Date	Other
automation	https://bsky.app/profile/omisoik.bsky.social/post/3lnc3wvzczst2z	CVE-2025-9001	seen	2025-04-21 02:17:56 +0000	🔗
automation	https://bsky.app/profile/omisoik.bsky.social/post/3lnc3wvzczst2z	CVE-2025-32433	seen	2025-04-21 02:17:55 +0000	🔗
automation	https://bsky.app/profile/omisoik.bsky.social/post/3lnc3wvzczst2z	CVE-2025-24054	seen	2025-04-21 02:17:55 +0000	🔗

- Continuous exploitation patterns are frequently observed through sources like The Shadowserver Foundation or MISP.

¹¹Don't underestimate the hype surrounding some vulnerabilities.

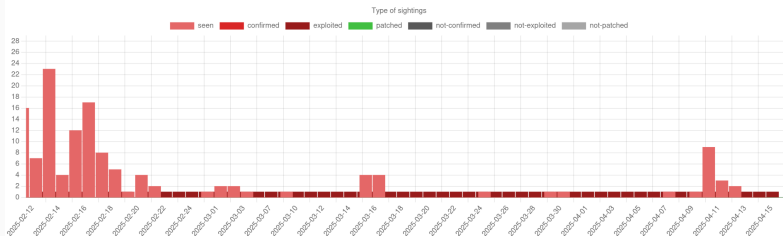
Early PoC (erlang / otp)



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

Continuous Exploitations (Palo Alto Networks / Cloud NGFW)

Evolution of sightings over time



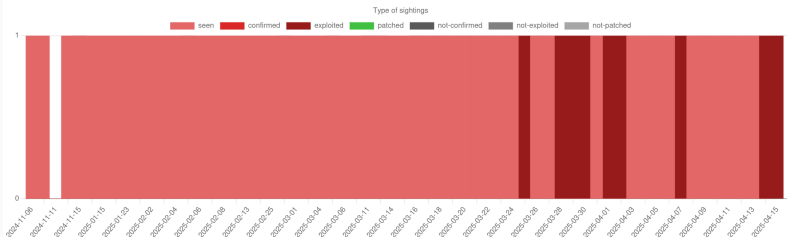
Sightings

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>

Continuous Exploitations (D-Link / DNS-320)

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	The Shadowserver (honeypot/common-vulnerabilities) - (2025-04-16) (correlations)	seen	1 day ago
automation	The Shadowserver (honeypot/common-vulnerabilities) - (2025-04-15) (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-2024-10914#sightings>

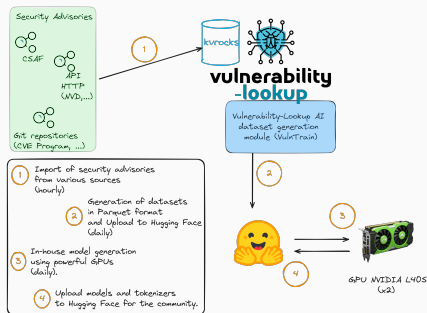
Tracking the Exploitability of Vulnerabilities Prior to Public Disclosure

- **Google / Android:** <https://vulnerability.circl.lu/vuln/CVE-2024-43093#sightings>
- **Speedify VPN (macOS):** <https://vulnerability.circl.lu/vuln/CVE-2025-25364#sightings>
 - Low visibility, no EPSS score, few sightings



Toward Practical AI Applications

Completing Missing Data with AI



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

^a<https://www.vulnerability-lookup.org/user-manual/ai/>

^b<https://github.com/vulnerability-lookup/VulnTrain>

Model	Size	Epochs	Accuracy	Training Time
Severity classification ¹²	125M params	5	0.8289	6.72h
Severity classification (CNVD) ¹³	102M params	5	0.7817	65.989m
CWE guessing ¹⁴	125M params	36-40	0.875	30m

¹²<https://huggingface.co/CIRCL/vulnerability-severity-classification-roberta-base>

¹³<https://huggingface.co/CIRCL/vulnerability-severity-classification-chinese-macbert-base>

¹⁴<https://huggingface.co/CIRCL/cwe-parent-vulnerability-classification-roberta-base>

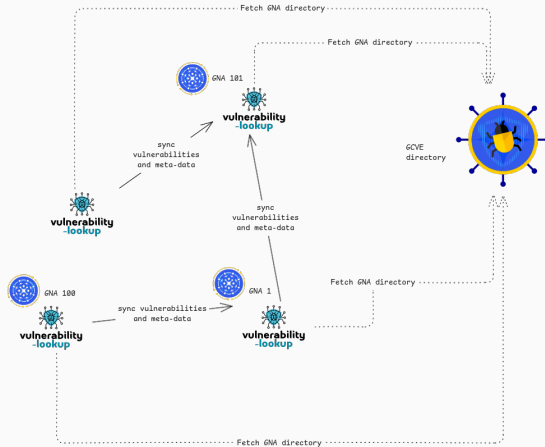
Publishing security advisories

- The primary role of GCVE¹⁵ 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.
- Vulnogram integration¹⁶

¹⁵<https://gcve.eu>

¹⁶<https://github.com/Vulnogram/Vulnogram>

Decentralized Publication Standard



Closing

Future Development

- Deeper analysis of the content and context of sightings, including **source reliability assessment**.
- Integration of scoring models, with testing planned on our dataset to enhance reproducibility.
- **Improved notification capabilities** for newly observed vulnerabilities via webhooks.
- Full-text search capabilities across all integrated sources.



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>