

Scoring vulnerabilities by leveraging activity data from the Fediverse

2025 Cyber Threat Intelligence Conference FIRSTCTI25 - Berlin, Germany

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

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

April 22, 2025

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

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).



vulnerability
-lookup

¹<https://www.vulnerability-lookup.org>

²<https://github.com/ngsoti>

- `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 1,360,500 security advisories and more than 70,000 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- **Fast lookup:** Rapidly correlating identifiers across **diverse sources**, including unpublished advisories.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

- **CISA Known Exploited Vulnerability** (HTTP)
- **NIST NVD CVE** (API 2.0)
- **CVEProject - cvelist** (Git submodule)
- **Fraunhofer FKIE** (Git submodule)
- **Cloud Security Alliance - GSD** (Git submodule)
- **GitHub Advisory DB** (Git submodule)
- **PySec Advisory DB** (Git submodule)
- **CSAF 2.0** (HTTP CSAF)
CERT-Bund, Cisco, Siemens, Red Hat, Microsoft, NCSC-NL, CISA, etc.
- **VARIoT** (API)
- **Japan - JVN DB** (HTTP)
- **Tailscale** (RSS)
- **GCVE.eu source references**
- **Growing...**

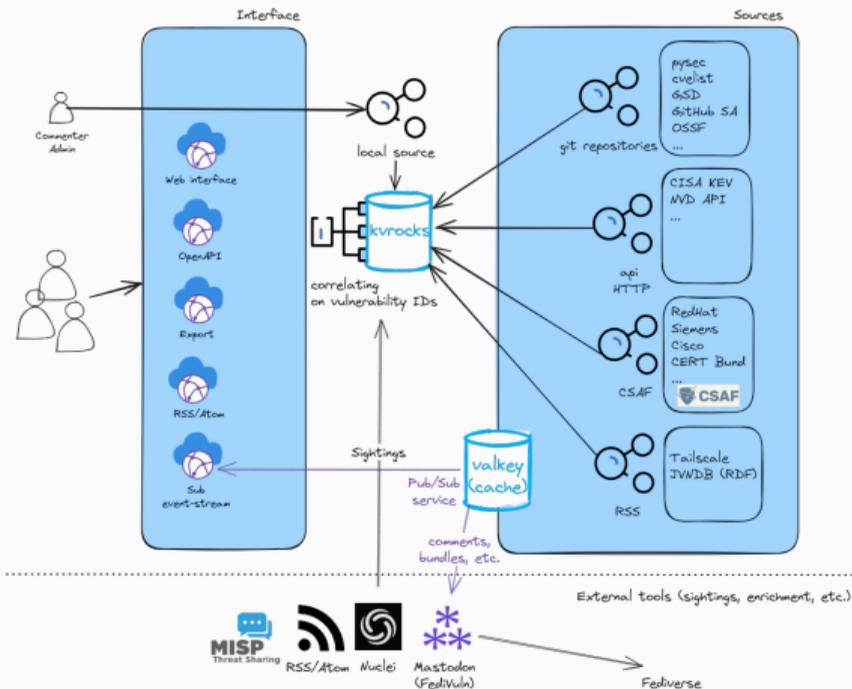
Open Data Initiative: Regular JSON dumps published⁹.

⁹<https://vulnerability.circl.lu/dumps/>

Design and Implementation

Vulnerability-Lookup High-Level Architecture

Overview of the Vulnerability-Lookup architecture - <https://www.vulnerability-lookup.org>



```
$ 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 Atom¹⁰

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 comments¹¹. 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"  
}
```

¹¹https://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

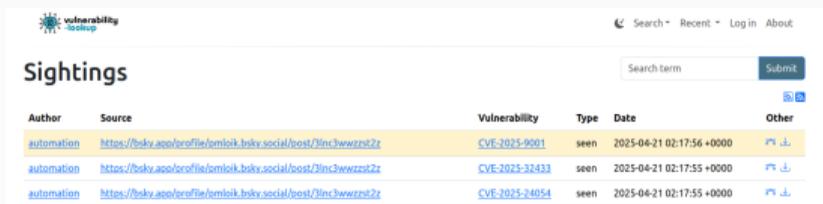
Automatically gathering crowd-sourced intelligence without requiring direct user contributions to our platform.

- **Social Platforms:** Fediverse, Bluesky
- **Threat Intelligence Tools:** MISP, Nuclei
- **Content Feeds:** RSS/Atom, curated web pages, GitHub Gist
- **Specialized Projects:** ShadowSight, ExploitDBSighting
- **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 vulnerabilities¹².
- 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 'Sightings' page on the Vulnerability Database website. It features a search bar with the text 'Search term' and a 'Submit' button. Below the search bar is a table with columns for Author, Source, Vulnerability, Type, Date, and Other. The table contains three rows of data, all with the author 'automation' and the source 'https://bky.apo/profile/lemisik.bky.social/post/3inc3wvzst2z'. The vulnerabilities listed are CVE-2025-9901, CVE-2025-32433, and CVE-2025-24054, all of which were 'seen' on 2025-04-21.

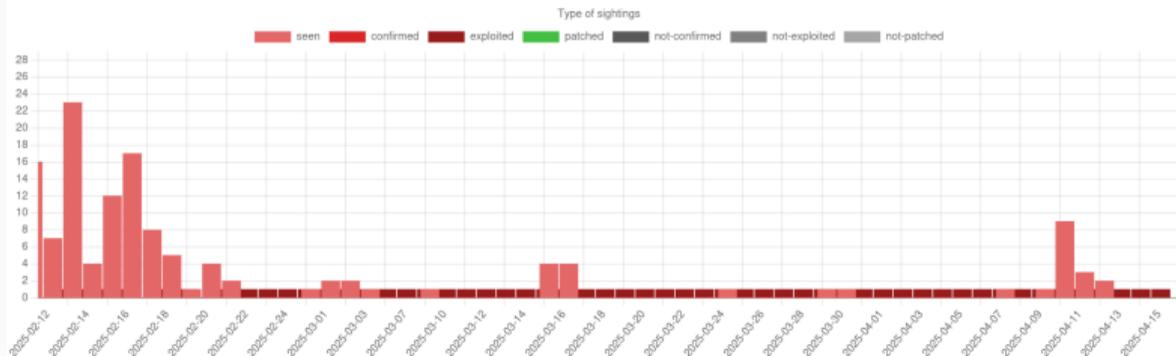
Author	Source	Vulnerability	Type	Date	Other
automation	https://bky.apo/profile/lemisik.bky.social/post/3inc3wvzst2z	CVE-2025-9901	seen	2025-04-21 02:17:56 +0000	🔗 ↓
automation	https://bky.apo/profile/lemisik.bky.social/post/3inc3wvzst2z	CVE-2025-32433	seen	2025-04-21 02:17:55 +0000	🔗 ↓
automation	https://bky.apo/profile/lemisik.bky.social/post/3inc3wvzst2z	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.

¹²Don't underestimate the hype surrounding some vulnerabilities.

Continuous Exploitations (Palo Alto Networks / Cloud NGFW)

Evolution of sightings over time



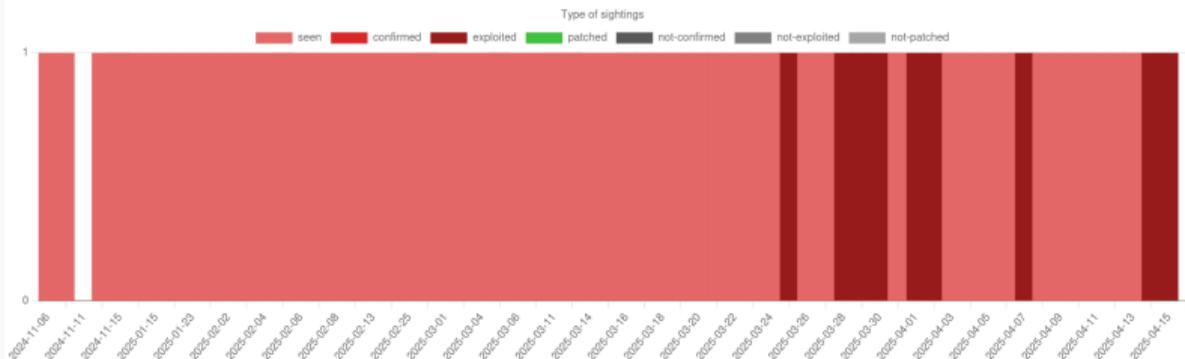
Sightings

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>

Last Month's Most Sighted Vulnerabilities

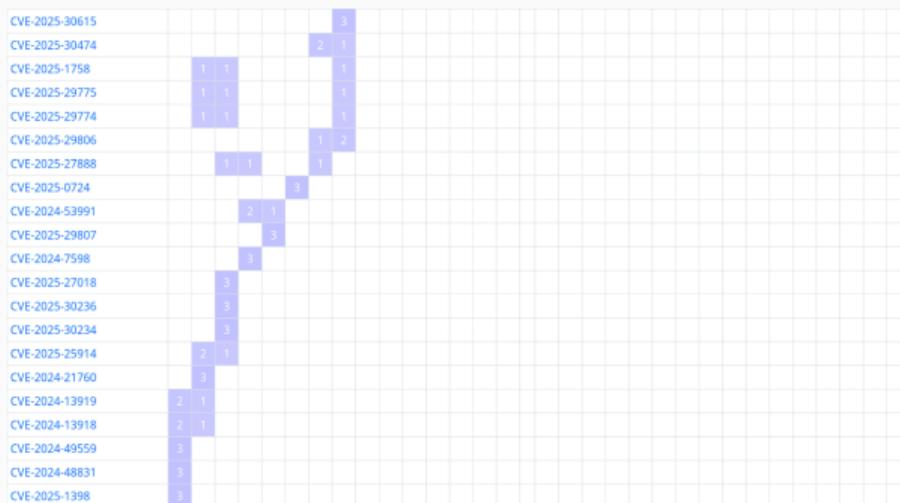
	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	
CVE-2025-29927					3	11	54	42	20	15	7	10	1	3	1	1	4	4	1	2	1		2	1					1	1			
CVE-2025-22457																		39	38	11	12	16	8	6	5	13	3	4	3	4		14	
CVE-2025-24813	13	15	12	13	8	3	2	11	2	1		1	1	3	5	7	7	4		2	1		1	2			1						
CVE-2025-1974							5	24	11	25	7	8	1	5	6	2	7								1								
CVE-2025-2825									2	10	7	2	2	11	9	12	7	2	2	2	2	3	6		5	3	1		1	3			
CVE-2025-29824																							12	29	11	4	2	1	4	2	3	14	
CVE-2025-2783								1	27	15	12	8	7	2		1	1	1															
CVE-2025-30066	12	15	14	3	4	2	1	6	2	1	1				2								1		1								
CVE-2025-24200															3	3	4	3	1	1		3	1		12	30							
CVE-2017-18368	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2		
CVE-2015-2051	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2		
CVE-2025-30406																		1	2					2	3	6	2	2		8	14	3	14
CVE-2025-0108	1	5	5	1	1	1	1	1	1	1	2	1	1	1	1	1	3	1	1	1	1	1	1	1	2	1	2	3	11	3			

- **CVE-2025-22457:** Ivanti / Connect Secure — Severity: 10.0 (Critical)
- **CVE-2025-29927:** Vercel / Next.js — Severity: 9.1 (Critical)

Vulnerability	Product	Sighting count	EPSS	Severity
CVE-2025-29927	next.js	167	89.24% (0.99521)	9.1
CVE-2025-24813	Apache Tomcat	128	93.55% (0.99827)	9.2
CVE-2024-4577	PHP	190	94.38% (0.99961)	9.8
CVE-2025-0282	Connect Secure	243	90.87% (0.99618)	9.0
CVE-2024-55591	FortiOS	126	92.79% (0.99756)	9.8
CVE-2024-10914	D-Link DNS-320	81	93.73% (0.9985)	9.2
CVE-2020-21650	Myucms	57	2.48% (0.83998)	9.1

Table 2: Top vulnerabilities from our April 2025 report, based on sightings and scoring data.

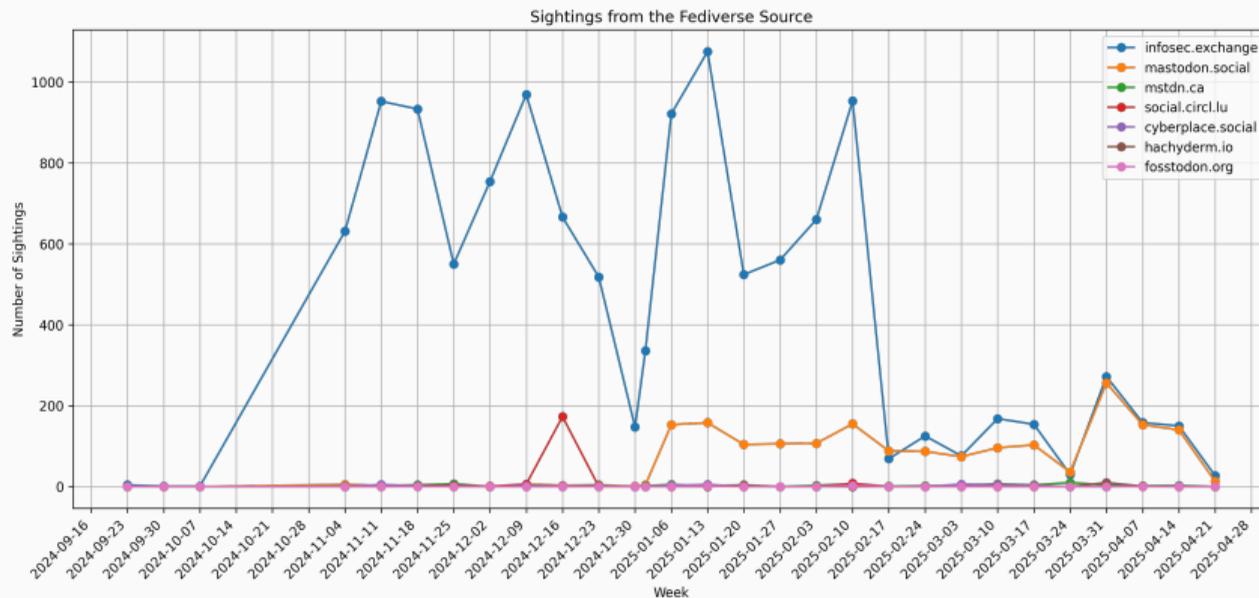
Least Sighted Vulnerabilities in the Last Month



These vulnerabilities typically have low EPSS scores and are often rated as low or medium severity based on CVSS.

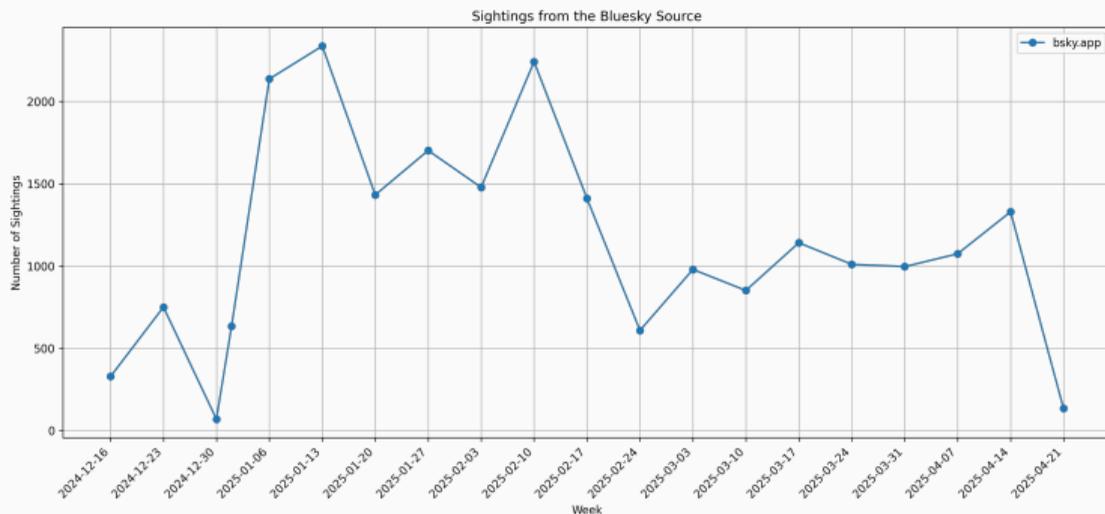
This trend is likely influenced by the fact that EPSS also incorporates data from publicly available web sources.

Evolution of Sightings from the Fediverse



Is there a geopolitical influence on social network activity?

Evolution of Sightings from Bluesky

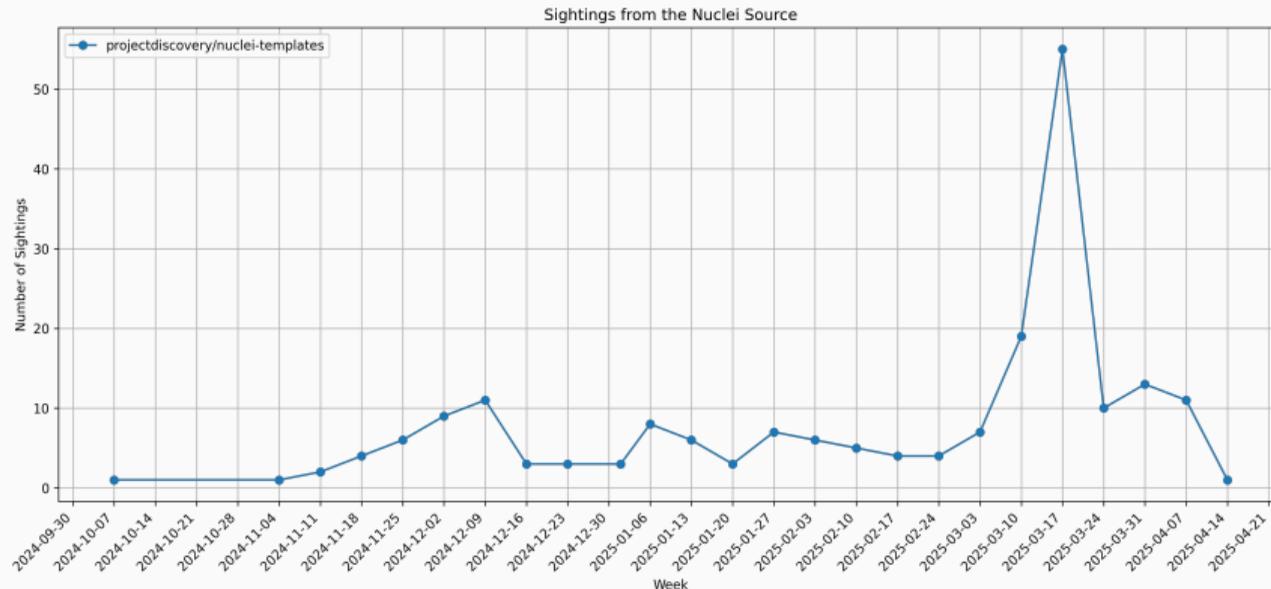


We observed the deletion of hundreds of posts.¹³
Several accounts were also closed in mid-February.¹⁴

¹³<https://vulnerability.circl.lu/sightings/?query=screaminggoat>

¹⁴<https://cyberplace.social/@GossiTheDog/114275910650393298>

Evolution of Sightings from Nuclei



Typical timeline of a high-severity vulnerability:
<https://vulnerability.circl.lu/vuln/CVE-2025-29927#sightings>

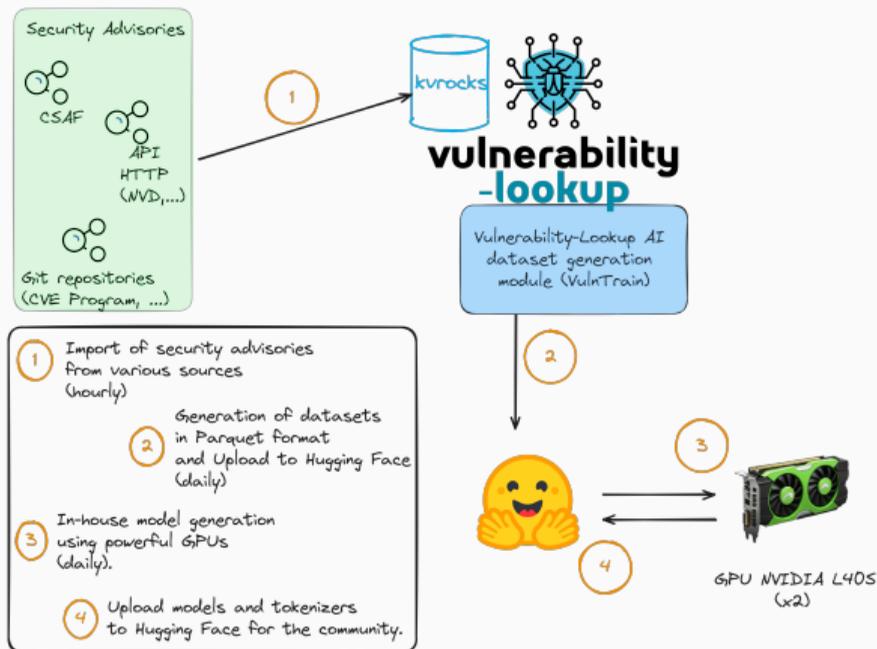
Tracking the Exploitability of Vulnerabilities Prior to Public Disclosure

- **Google / Android:** <https://vulnerability.circl.lu/vuln/CVE-2024-43093#sightings>
- **Speedify VPN (macOS):** <https://vulnerability.circl.lu/vuln/CVE-2025-25364#sightings>
- **SourceCodester:** <https://vulnerability.circl.lu/vuln/CVE-2025-3821#sightings>
 - Low visibility, no EPSS score, few sightings



Closing

NLP, LLMs: What We're Testing and Where We're Headed



- Predicting CPE names using a novel approach (beyond CPE Guesser)
- Automated threat intelligence tagging using ATT&CK mappings
- Vulnerability type classification via CWE mappings
- Ongoing experimentation and refinement

<https://huggingface.co/CIRCL>

Future Development

- Deeper analysis of the content and context surrounding sightings.
- Allocation of vulnerability identifiers aligned with the GCVE system.
- Full-text search capabilities across all sources.
- Integration of scoring models such as EPSS and Vuln4Cast¹⁵, with plans to test them on our dataset to improve reproducibility.
- Synchronization between multiple Vulnerability-Lookup instances.



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

¹⁵<https://github.com/FIRSTdotorg/Vuln4Cast>

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

 <https://vulnerability.circl.lu>

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

 <https://social.circl.lu/@circl>

Thank you for your attention

- Issues, new sources of advisories or ideas:
`https://github.com/vulnerability-lookup/vulnerability-lookup`
- For support and questions, contact: `info@circl.lu`