



CIRCL
Computer Incident
Response Center
Luxembourg

When Data Talks, We Let AI Listen

BSides Luxembourg

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

Léa ULUSAN

2025/06/19

CIRCL

- **Challenges:** Working with messy, real-world vulnerability data
- **AI in action:** Structuring, scoring, and making sense of it
- **What's next:** Lessons learned and future directions

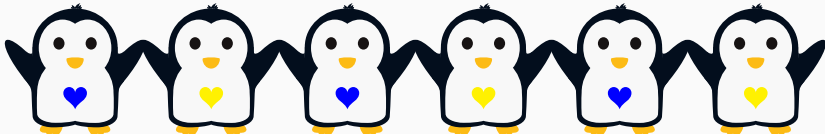
Who is behind Vulnerability Lookup?



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).



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

²<https://github.com/ngsoti>

Origin and Challenges we aim to address

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.

Challenges:

- The design and scalability of `cve-search` are limited. Our operational public instance previously at `cve.circl.lu` is reaching 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>

Making vulnerability data actionable

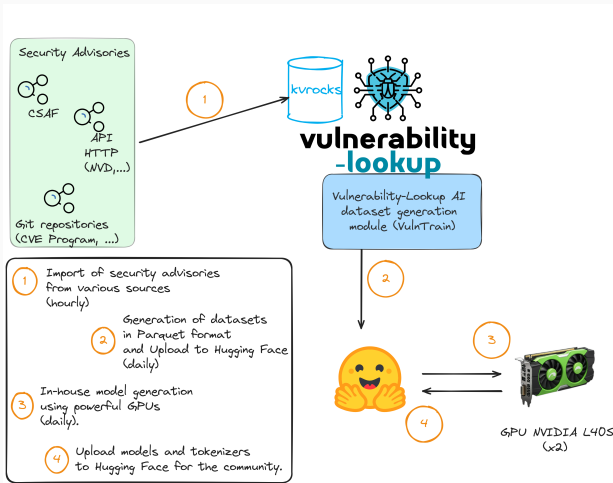
- **Collaborative features:**
 - Tags, bundles, and comments
 - Sightings (real-world observations)
- **But:** Many vulnerabilities have no CVSS score
- **Goal:** Predict severity based only on the description



A constantly updated dataset

- Over 1 million correlated vulnerability records
- Extracted from CIRCL's internal data pipeline
- Includes:
 - CVE ID, description, CVSS score
 - Tags, CPEs, CWEs, timestamps
- Published on Hugging Face: <https://huggingface.co/datasets/CIRCL/vulnerability-scores>

Ready for production:

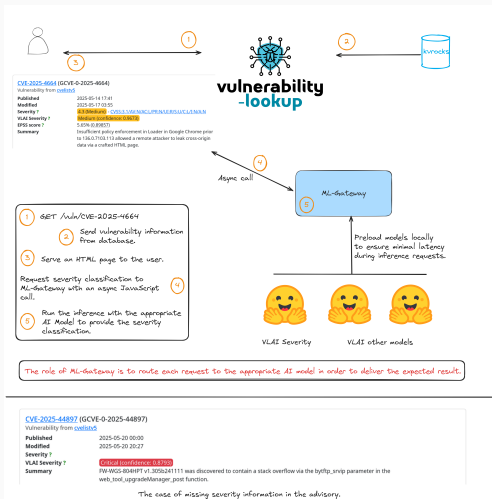


Severity prediction with RoBERTa

- Fine-tuned RoBERTa model
- Input: CVE text description
- Output: Severity level (Low, Medium, High, Critical)
- Achieves over 90% accuracy on recent CVEs
- Example: CVE-2025-44897 → **Critical** (98% confidence)

CVE-2025-44897 (GCVE-0-2025-44897)	
Vulnerability from cvelistv5	
Published	2025-05-20 00:00
Modified	2025-05-21 13:33
Severity ?	9.8 (Critical) - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
VLAI Severity ?	Critical (confidence: 0.9758)
EPSS score ?	0.05% (0.16593)
Summary	FW-WGS-804HPT v1.305b241111 was discovered to contain a stack overflow via the byftftp_srvip parameter in the web_tool_upgradeManager_post function.
References	URL Tags

Putting Our Models to Work



What's next?

- CWE Guesser: Predict the vulnerability type from the description
- Analyze Git commit messages to identify how vulnerabilities are fixed
 - Detect patterns in patches and commits
 - Link vuln types to their fixing strategies
- CVE-to-CPE inference: Guess impacted products
- Map to MITRE ATT&CK tactics to improve context
- Help prioritize patching based on risk and impact
- Open to community contributions!

Closing

Future development





- We're just getting started with AI!
- Our goal: Make vulnerability data truly actionable and open.
- We believe collaboration is key to building smarter, more scalable tools.



This is only the beginning — we welcome your feedback, ideas, and contributions to shape the future of vulnerability intelligence together !

Thank you for your attention !

- **References**

-  <https://vulnerability.circl.lu>
-  <https://www.vulnerability-lookup.org>
-  <https://social.circl.lu/@circl>
-  <https://www.circl.lu/pub/ai-strategy/>

- **Issues or contributions**

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

- **Contact us**

info@circl.lu

- **Contact me !**

lea.ulusan@edu.ece.fr