CIRCL
Computer Incident
Response Center
Luxembourg

VLAI: A RoBERTa-Based Model for Automated Vulnerability Severity Classification

CyberDay.lu - Belval, Luxembourg

https://arxiv.org/abs/2507.03607

Cédric Bonhomme - cedric.bonhomme@circl.lu

October 9, 2025

CIRCL https://www.circl.lu

Contents

Origin of Vulnerability-Lookup

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://www.restena.lu/en/project/ngsoti

What is Vulnerability-Lookup?

- A unified place to **search**, **triage**, and **track** software and product vulnerabilities from different sources.
- Brings together vulnerability information, correlation of identifiers (e.g., CVE, GHSA, OSV), references, timelines, and risk signals in one view.
- Designed for **CSIRTs**, **SOCs**, **vulnerability managers**, and **developers** in mind.
- **Web UI first** with strong **API** and automation options.
- Support a complete **CVD process management**[3] along with the ability to fork vulnerability information[4]. Distributed GNA directory.

[3] CNA Program, GCVE GNA Publication
[4] Implemented before the GNA initiative!

Origin of Vulnerability-Lookup

- `cve-search`[5] 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.

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

Initial Challenges

- **Volume of data:** Handling a substantial dataset and heavy network traffic, currently over 1,731,444 security advisories and more than 140,000 sightings collected in one year [6].
- **Flexibility:** Balancing ongoing development with legacy issues while designing a future-proof architecture. It's complex and yes, sometimes chaotic[7].
- **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.

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

Ongoing Challenges and Development

- **CPE fragmentation:**[8] 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 to support the Coordinated Vulnerability Disclosure process. [9]
- **Vulnerability numbering:** Enabling a new distributed approach through the Global CVE Allocation System.[10]
- **Scoring vulnerabilities:** Aggregating a **large volume** of observations from diverse advisory types to improve vulnerability scoring. Automatic **weighting** of sightings by source or type (e.g., exploited). Automatic **detection of the type** not depending on the source.

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

Where the Data Comes From

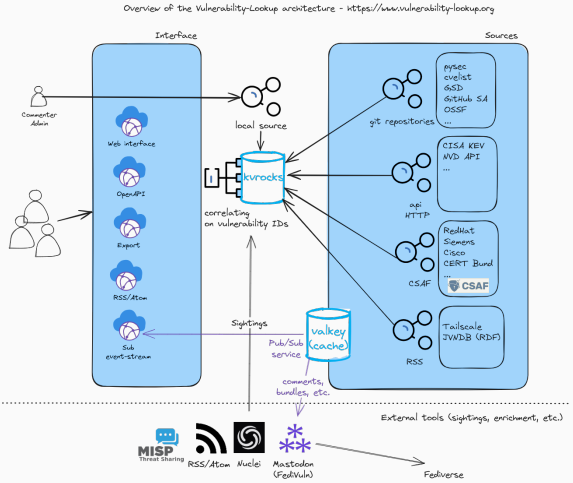
Contents

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** 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...**

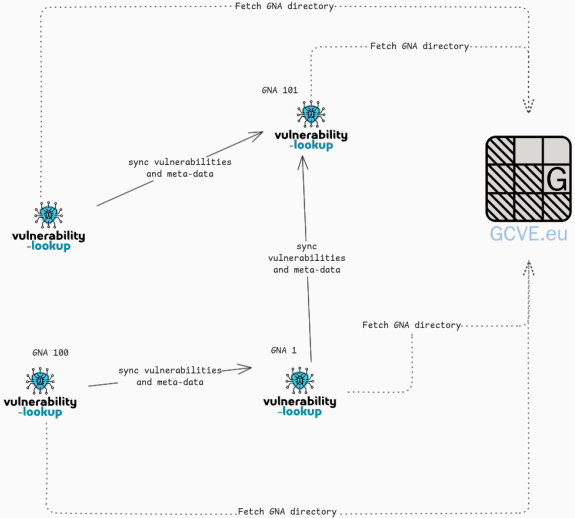
Vulnerability-Lookup High-Level Architecture

- 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.



TLP:CLEAR

A Distributed Network



TLP:CLEAR

From Data to Datasets

Contents

Why We Share Datasets

- **Open Data Initiative**: CIRCL's commitment to making data openly available.
- Consistent open approach applied across all our projects.
- Regularly updated JSON dumps [11] and "AI" datasets [12].
- Public, unauthenticated API access for Vulnerability-Lookup.

[11] https://vulnerability.circl.lu/dumps/
[12] https://huggingface.co/CIRCL/datasets

Building AI Datasets

- Our experience with large datasets is not recent (Passive DNS[13], BGP ranking[14], MISP[15], AIL[16], Lookyloo[17], etc.). And we learned from our past mistakes.
- Turn messy data into structured, actionable insights.
- Link related vulnerabilities via enrichment, correlation, and crawling.
- Support the process with **VulnTrain**[18]: a tool to build AI Datasets and Models.

[13] https://www.circl.lu/services/passive-dns/
[14] https://github.com/D4-project/BGP-Ranking
[15] https://github.com/MISP
[16] https://github.com/ail-project
[17] https://github.com/Lookyloo
[18] https://github.com/vulnerability-lookup/VulnTrain

Current datasets

Dataset	Size (rows)	Generation Time	Features
vulnerability-scores[19]	641,918	10m45s	Descriptions (en), CVSS, CPE
vulnerability-CNVD[20]	123,171	1m31s	Descriptions (cn), CVSS
vulnerability-cwe-patch[21]	883	210m	Descriptions (en), CWE, patches (commit id + url + full diff)

[19] https://huggingface.co/datasets/CIRCL/vulnerability-scores
[20] https://huggingface.co/datasets/CIRCL/Vulnerability-CNVD
[21] https://huggingface.co/datasets/CIRCL/vulnerability-cwe-patch

From Datasets to Models

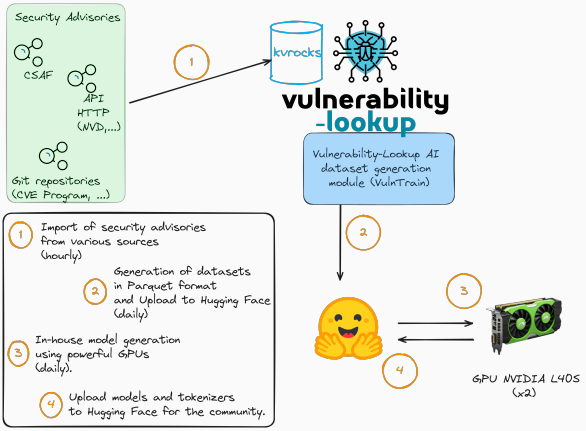
Contents

Why We Are Building AI Models

- CIRCL AI approach[22]: we enhance existing solutions rather than replacing functional systems with NLP/ML/LLM solutions.
- AI-powered **enrichment** of vulnerability descriptions.
- Providing actionable insights to security experts when data is **missing or inaccurate** (e.g., severity, CWE, CPE information).
- We actively participate in collaborative research and development efforts, such as the EU-funded AIPITCH (AI-Powered Innovative Toolkit for Cybersecurity Hubs) project[23]

[22] https://circl.lu/pub/ai-strategy/
[23] https://www.science.nask.pl/en/research-areas/projects/12456

Model generation workflow with VulnTrain



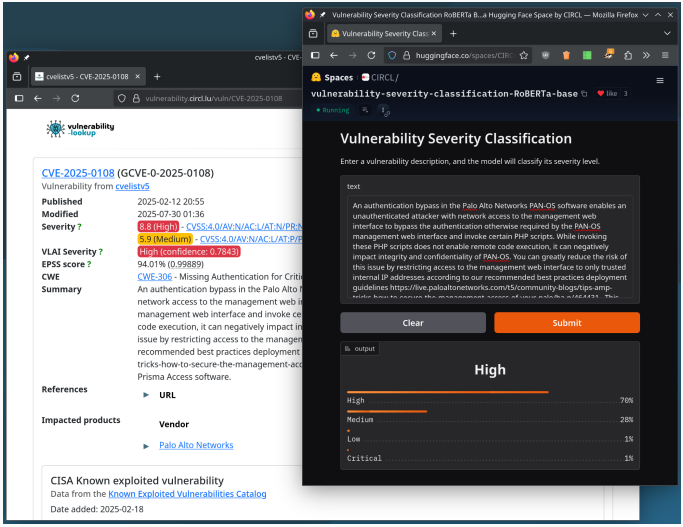
- local training
- models are publicly shared
- regular update

Current Models

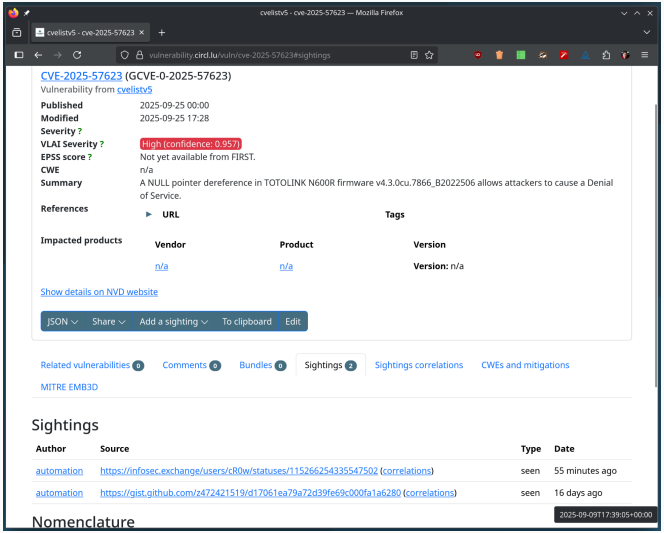
Model	Size	Epochs	Accuracy	Training Time
Severity classification[24]	125M params	5	0.8289	6.72h
Severity classification (CNVD)[25]	102M params	5	0.7817	65.989m
CWE guessing[26]	125M params	36-40	0.875	30m

[24] https://huggingface.co/CIRCL/vulnerability-severity-classification-roberta-base
[25] https://huggingface.co/CIRCL/vulnerability-severity-classification-chinese-macbert-base
[26] https://huggingface.co/CIRCL/cwe-parent-vulnerability-classification-roberta-base

With different CVSS scores

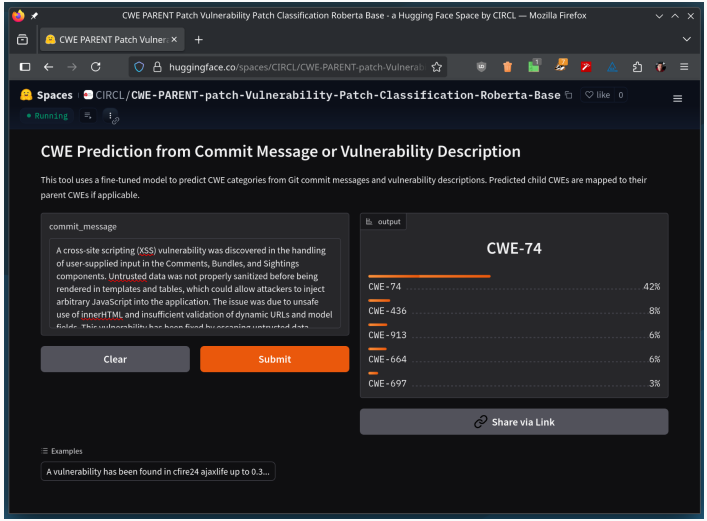


Few information (reserved 17 September 2025 - sightings since 9 September)

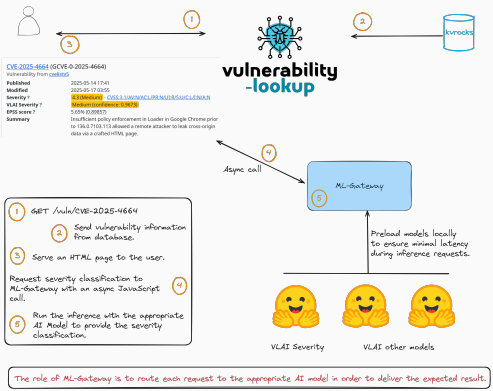


TLP:CLEAR

CWE Guessing (GCVE-1-2025-0004 - CWE 79)



Integration



- Optional integration
- No dependencies with Vulnerability-Lookup
- Models are pulled from Hugging Face and preloaded locally
- Documented API (OpenAPI) to trigger the inferences
- `https://github.com/vulnerability-lookup/ML-Gateway`

Example

```
$ curl -X 'POST' \
  'https://vulnerability.circl.lu/api/vlai/severity-classification' \
  -H 'accept: application/json' \
  -H 'Content-Type: application/json' \
  -d '{
  "description": "An authentication bypass in the API component of Ivanti Endpoint
    Manager Mobile 12.5.0.0 and prior allows attackers to access protected
    resources without proper credentials via the API."
}'
{"severity": "High", "confidence": 0.8225}
```

Demo

Demo.

Closing

Future Development

- Deeper analysis of the content and context surrounding sightings and exploited vulnerabilities.
- Generation of insights based on patches.
- CPE Guessing.
- Allocation of vulnerability identifiers aligned with the GCVE system.
- Full-text search capabilities across all sources.
- Synchronization between multiple Vulnerability-Lookup instances.

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

References

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