Vulnerability Lookup

An open source tool to support CVD processes

CIRCL
Computer Incident
Response Center
Luxembourg

Cédric Bonhomme
TLP:CLEAR

cedric.bonhomme@circl.lu

2024-10-24

Who is behind Vulnerability Lookup?

- Vulnerability Lookup[1], an Open Source project led by **CIRCL**.
- Co-funded by **CIRCL** and the **European Union**.
- Part of the NGSOTI[2] project, dedicated to training the next generation of Security Operations Center (SOC) operators.

[1] https://github.com/cve-search/vulnerability-lookup

[2] https://www.restena.lu/en/project/ngsoti

Origin and Challenges we aim to address

- `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` 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`

Current sources in Vulnerability Lookup

- **CISA Known Exploited Vulnerability** (via HTTP)
- **NIST NVD CVE** (via API 2.0)
- **CVEProject - cvelist** (via git submodule repository)
- **Cloud Security Alliance - GSD Database** (via git submodule repository)
- **GitHub Advisory Database** (via git submodule repository)
- **PySec Advisory Database** (via git submodule repository)
- **CSAF 2.0** (via git submodule repository)
- **VARIoT** (via API)
- **Japan Database - JVN DB** (via HTTP)
- **Tailscale** (via RSS)

Open Data Initiative: Committed to regularly publishing comprehensive JSON dumps of all integrated sources as open data.

Main functionalities of Vulnerability Lookup - v2.0.0

- A fast lookup API to search for vulnerabilities and find correlation.
- Modular system to import **different vulnerability sources**.
- Support of **local source** per instance with custom IDs and JSON schemas (data validation).
- Exploit Prediction Scoring System[4] score from FIRST.
- **CVE Publication as CNA**: Integration of Vulnogram.[5]
- Extensive support for RSS/Atom.

[4] `https://www.first.org/epss`

[5] `https://github.com/Vulnogram/Vulnogram`

Improving threat intelligence

- **Bundles:** Allow to combine similar vulnerabilities.
- **Comments:** Provide additional context (PoC, remediations, etc.).
- **Tags:** Attach tags to comments from the MISP vuln taxonomy[6].

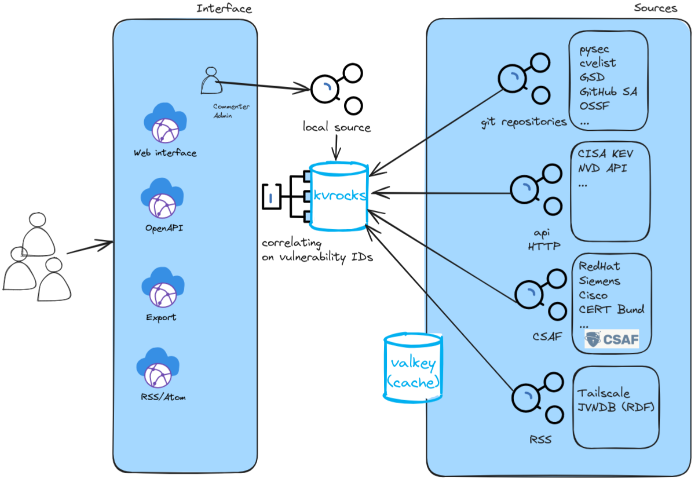
```
vulnerability:information=remediation
```

- **Sightings:** Provide observations on vulnerabilities.

```
{
  "uuid": "99c0bf75-48c6-41ac-a26f-572752dffd27",
  "vulnerability_lookup_origin": "1a89b78e-f703-45f3-bb86-59eb712668bd",
  "author": "8dfa6142-8c6d-4072-953e-71c85404aefb",
  "vulnerability": "CVE-2023-39328",
  "type": "exploited",
  "creation_timestamp": "2024-10-22T16:27:23.729320Z"
}
```

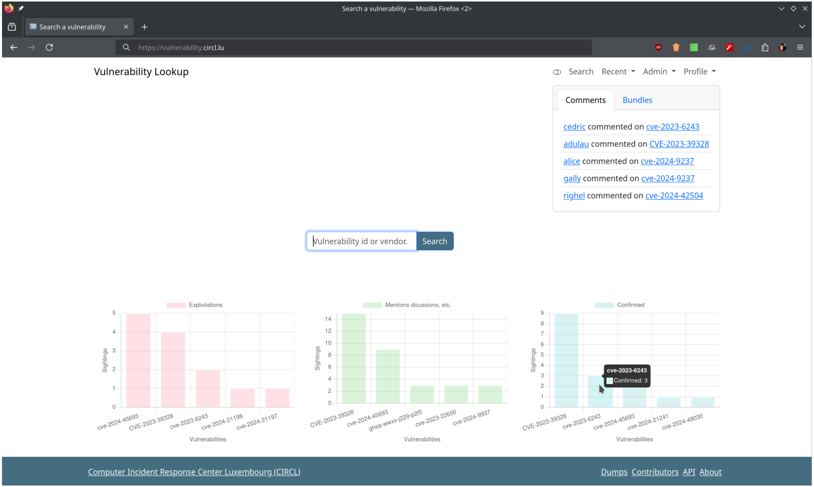
[6] https://www.misp-project.org/taxonomies.html#_vulnerability_3

Vulnerability Lookup high level architecture



Overview of the vulnerability-lookup architecture - https://github.com/cve-search/vulnerability-lookup

Demo



cedric commented on cve-2023-6243

adulau commented on CVE-2023-39328

alice commented on cve-2024-9237

gally commented on cve-2024-9237

righel commented on cve-2024-42504

Future development

- EPSS (or similar models) and Vuln4Cast[7]. We would like to test it with our data set to regenerate the EPSS model.
- Connection with Fediverse / AIL[8] →**Automatic sighting**.
- Synchronization between Vulnerability Lookup instances.
- Full-text search across all sources.

💡 As the project is still in its early stages and evolving rapidly, we are eager to receive feedback and feature suggestions.

[7] `https://github.com/FIRSTdotorg/Vuln4Cast`

[8] `https://www.ail-project.org`

References

- 🏠 https://vulnerability.circl.lu

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

- 📖 https://vulnerability-lookup.readthedocs.io

Thank you for your attention

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