CIRCL
Computer Incident
Response Center
Luxembourg

Correlating security advisories with Vulnerability-Lookup

CSAF Community Days 2024 - Munich, Germany

https://www.vulnerability-lookup.org

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

December 13, 2024

CIRCL https://www.circl.lu

TLP:CLEAR

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**.

[1] https://www.vulnerability-lookup.org

TLP:CLEAR

Origin and Challenges we aim to address

Origin:

- cve-search[2] 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.

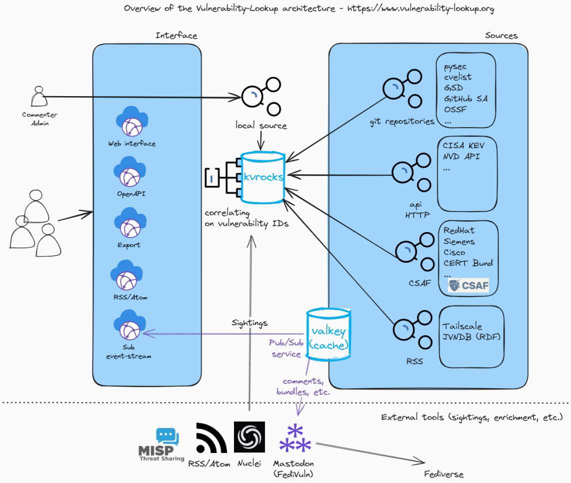
Initial challenges:

- The design and scalability of cve-search are limited. Our operational public instance at https://cve.circl.lu is reaching a hard limit of around 15,000 queries per second.
- Vulnerability sources have **diversified**, and the **NVD CVE is no longer the sole source of vulnerability information**.

[2] https://github.com/cve-search/cve-search

TLP:CLEAR

Vulnerability-Lookup high level architecture

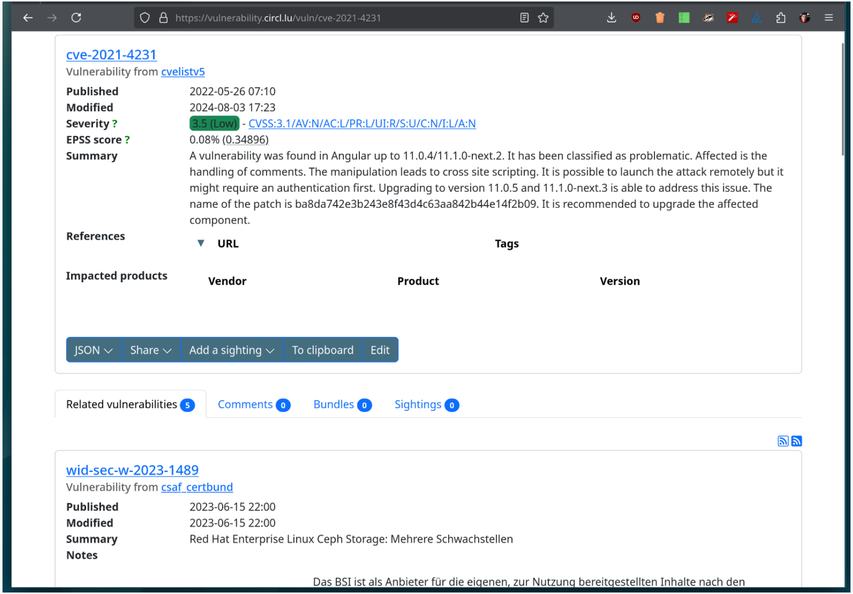


API correlation

```
$ 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/
- paginated and search per sources
- search for CPE with vendor and product name



cve-2021-4231

Vulnerability from cvelistv5

Published 2022-05-26 07:10

Modified 2024-08-03 17:23

Severity ? 3.5 (Low) - CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:N

EPSS score ? 0.08% (0.34896)

Summary A vulnerability was found in Angular up to 11.0.4/11.1.0-next.2. It has been classified as problematic. Affected is the handling of comments. The manipulation leads to cross site scripting. It is possible to launch the attack remotely but it might require an authentication first. Upgrading to version 11.0.5 and 11.1.0-next.3 is able to address this issue. The name of the patch is ba8da742e3b243e8f43d4c63aa842b44e14f2b09. It is recommended to upgrade the affected component.

References

▼ URL	Tags

Impacted products

Vendor	Product	Version

wid-sec-w-2023-1489

Vulnerability from csaf_certbund

Published 2023-06-15 22:00

Modified 2023-06-15 22:00

Summary Red Hat Enterprise Linux Ceph Storage: Mehrere Schwachstellen

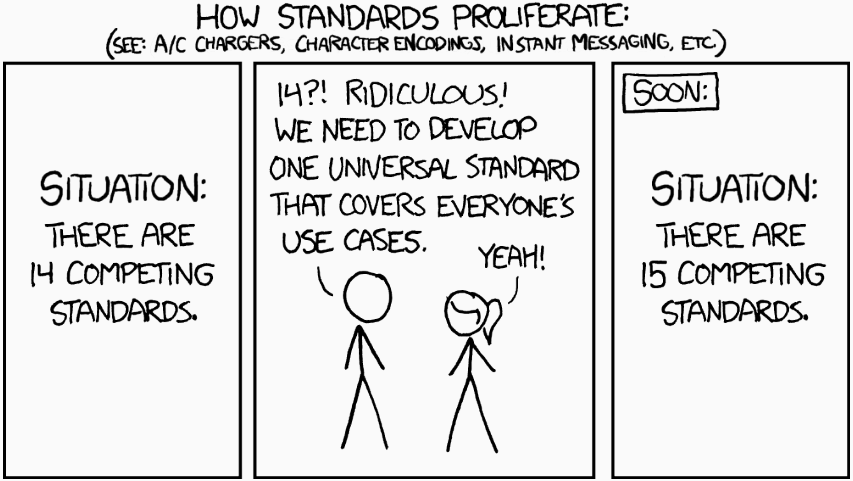
Notes

Das BSI ist als Anbieter für die eigenen, zur Nutzung bereitgestellten Inhalte nach den

Challenges and Considerations

- **Volume of data:** We handle a large volume of data and significant network traffic—currently exceeding 962,000 security advisories.
- **Monitoring of the feeders**: is the feeder process finished or stuck? what is the last update time for a specific source? How to get only new data?
- **Flexibility:** Managing the present while addressing past mistakes and ensuring a future-ready architecture.
- **Robustness:** Validating data, even when entities fail to adhere to their own JSON schema.
- **Fast lookup:** Correlating identifiers from **diverse sources**, even for unpublished advisories.
- **Languages:** Handling internationalization and displaying relevant information.

So much standards


HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

TLP:CLEAR

Inconsistencies in the implementation of standards, errors, etc.

Some recent issues we have encountered:

- Date time, timezone, and response format /gocsaf/csaf#588
- Encoding issues /cve-search/vulnerability-lookup/issues#94
- Interval of update of the feeds ?
- Typographical errors in security advisories or “synonyms” for vendor names.

Standards are good but the implementation is another problem.

Overly strict standards often fail in implementation or are not convenient for users.

TLP:CLEAR

References

https://www.vulnerability-lookup.org

https://vulnerability.circl.lu

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

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

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

TLP:CLEAR