



CIRCL
Computer Incident
Response Center
Luxembourg



GCVE.eu

Beyond CVEs: Mastering the Landscape with Vulnerability-Lookup

from CVE to CVD

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

Alexandre Dulaunoy - Cedric Bonhomme - team@circl.lu

October 23, 2025 - hack.lu 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).

A reference implementation to **GCVE** standards.



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 90,000 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- **Fast lookup:** Rapidly correlating identifiers across **diverse sources**, including unpublished advisories.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 all GNA sources**
- **CWE, CAPEC, MITRE EMB3D or KEV**
- **Growing...**

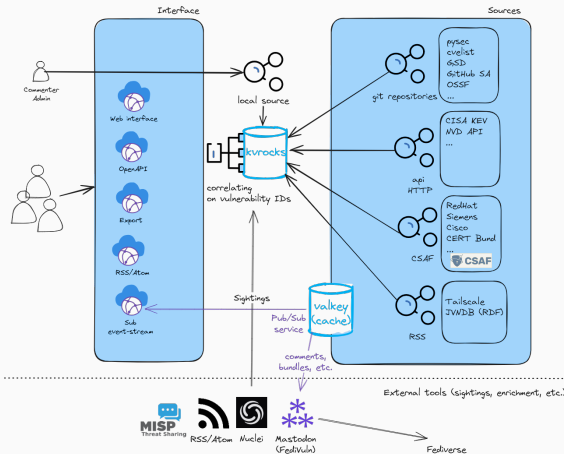
Open Data Initiative: Regular JSON dumps published⁹.

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 Atom**¹⁰

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/b7333fb02a4ee3618995bab9b62c507"  
}
```

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

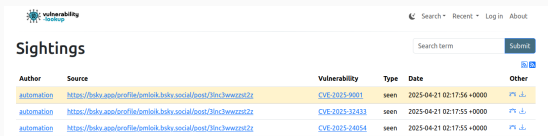
Automatically gathering crowd-sourced intelligence without requiring direct user contributions to our platform.

- **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**.



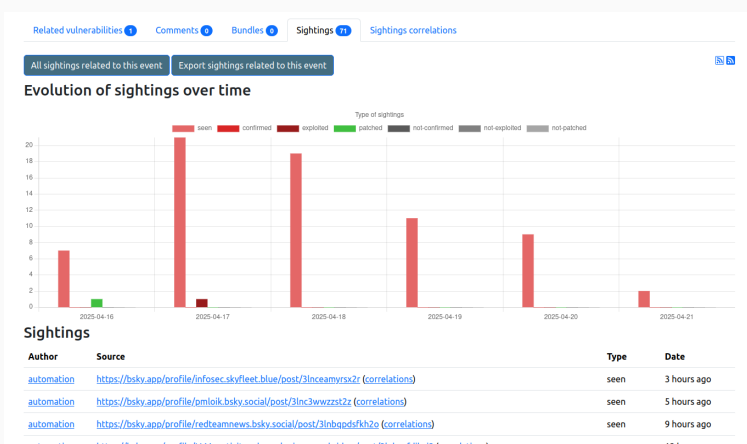
The screenshot shows the 'Vulnerability Sighting' website. At the top, there's a navigation bar with 'Search', 'Recent', 'Log in', and 'About'. Below this is a search bar with a 'Submit' button. The main heading is 'Sightings'. Below the heading is a table with columns: Author, Source, Vulnerability, Type, Date, and Other. The table contains three rows of data, all with 'automation' as the author and 'https://bsky.app/profile/omisoik.bsky.social/post/3lnc3wvzst2z' as the source. The vulnerabilities listed are CVE-2025-9001, CVE-2025-32433, and CVE-2025-24054. All three are of type 'seen' and dated '2025-04-21 02:17:55 +0000'. Each row has a link icon in the 'Other' column.

Author	Source	Vulnerability	Type	Date	Other
automation	https://bsky.app/profile/omisoik.bsky.social/post/3lnc3wvzst2z	CVE-2025-9001	seen	2025-04-21 02:17:55 +0000	🔗
automation	https://bsky.app/profile/omisoik.bsky.social/post/3lnc3wvzst2z	CVE-2025-32433	seen	2025-04-21 02:17:55 +0000	🔗
automation	https://bsky.app/profile/omisoik.bsky.social/post/3lnc3wvzst2z	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.

Early PoC (erlang / otp)

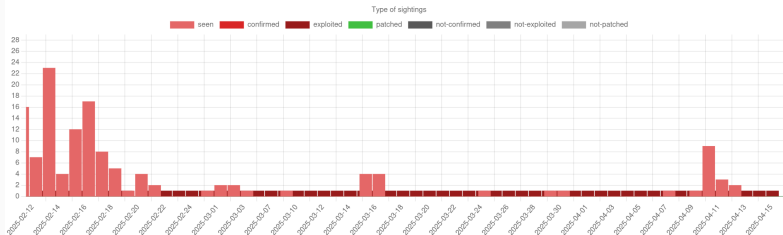


<https://vulnerability.circl.lu/vuln/CVE-2025-32433#sightings>

TLP: CLEAR

Continuous Exploitations (Palo Alto Networks / Cloud NGFW)

Evolution of sightings over time



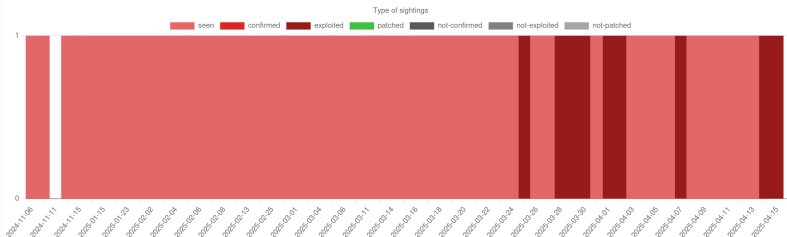
Sightings

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	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		
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		
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		

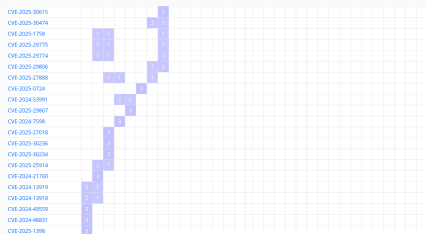
- **CVE-2025-22457:** Ivanti / Connect Secure — Severity: 10.0 (Critical)
- **CVE-2025-29927:** Vercel / Next.js — Severity: 9.1 (Critical)

Other Examples

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



- **Low-sighting outliers offer valuable intel**, even if absent from EPSS or predictive models.
- Particularly relevant in low-noise sources (e.g., MISP, private Telegram channels).
- Often rated low/medium by CVSS and have low EPSS scores.
- Trend highlights EPSS's dependence on public threat intel feeds.

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

Evolution of sightings over time



Sightings

Author	Source	Type	Date
automation	https://infosec.exchange/users/dragonjar/statuses/114364291565132421 (correlations)	seen	1 day ago
automation	https://bsky.app/profile/r-netsec.bsky.social/post/3ln4hb7anxx2g (correlations)	seen	2 days ago
automation	https://bsky.app/profile/r-netsec-bot.bsky.social/post/3ln4arcbktd2z (correlations)	seen	2 days ago
automation	https://infosec.exchange/users/threatcodex/statuses/114217935883108579 (correlations)	seen	27 days ago

Toward Practical AI Applications

From Data to Datasets

1. Origin of the project

2. Design and Implementation

3. Empowering the Community

4. Scoring Vulnerabilities

- **Open Data Initiative:** CIRCL's commitment to making data openly available.
- Consistent open approach applied across all our projects.
- Regularly updated JSON dumps ¹³ and “AI” datasets ¹⁴.
- Public, unauthenticated API access for Vulnerability-Lookup.

¹³<https://vulnerability.circl.lu/dumps/>

¹⁴<https://huggingface.co/CIRCL/datasets>

The Messy Reality of Large Datasets

- Our experience with large datasets is not recent (Passive DNS¹⁵, BGP ranking¹⁶, MISP¹⁷, AIL¹⁸, Lookyloo¹⁹, etc.). And we learned from our past mistakes.
- Adapt to real-world conditions — avoid creating yet another format or standard.
- Deal with missing data, malformed JSON, and conflicting information.
- Tolerate unreliable or unstable remote servers (e.g., some CSAF providers).

¹⁵<https://www.circl.lu/services/passive-dns/>

¹⁶<https://github.com/D4-project/BGP-Ranking>

¹⁷<https://github.com/MISP>

¹⁸<https://github.com/ail-project>

¹⁹<https://github.com/Lookyloo>

- Turn messy data into structured, actionable insights.
- Link related vulnerabilities via enrichment, correlation, and crawling.
- Support the process with **VulnTrain**²⁰.

²⁰<https://github.com/vulnerability-lookup/VulnTrain>

Current datasets

Dataset	Size (rows)	Generation Time	Features
vulnerability-scores ²¹	641,547	10m45s	Descriptions (en), CVSS, CPE
vulnerability-CNVD ²²	122,546	1m31s	Descriptions (cn), CVSS
vulnerability-cwe-patch ²³	883	210m	Descriptions (en), CWE, patches (commit id + url + full diff)

²¹<https://huggingface.co/datasets/CIRCL/vulnerability-scores>

²²<https://huggingface.co/datasets/CIRCL/Vulnerability-CNVD>

²³<https://huggingface.co/datasets/CIRCL/vulnerability-cwe-patch>

From Datasets to Models

1. Origin of the project

2. Design and Implementation

3. Empowering the Community

4. Scoring Vulnerabilities

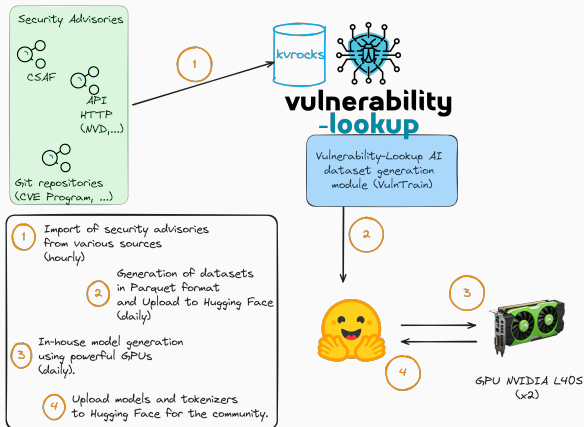
Why We Are Building AI Models

- CIRCL AI approach²⁴: 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) project²⁵

²⁴<https://circl.lu/pub/ai-strategy/>

²⁵<https://www.science.nask.pl/en/research-areas/projects/12456>

Model generation workflow



- local training
- models are publicly shared
- regular update

Model	Size	Epochs	Accuracy	Training Time
Severity classification ²⁶	125M params	5	0.8289	6.72h
Severity classification (CNVD) ²⁷	102M params	5	0.7817	65.989m
CWE guessing ²⁸	125M params	36-40	0.875	30m

²⁶<https://huggingface.co/CIRCL/vulnerability-severity-classification-roberta-base>

²⁷<https://huggingface.co/CIRCL/vulnerability-severity-classification-chinese-macbert-base>

²⁸<https://huggingface.co/CIRCL/cwe-parent-vulnerability-classification-roberta-base>

With different CVSS scores

The image displays two browser windows side-by-side. The left window shows a CVE-2025-0108 entry from cvelistv5, detailing its publication date, severity (8.8 High), and a summary of an authentication bypass in Palo Alto Networks PAN-OS. The right window shows the 'Vulnerability Severity Classification' interface, which takes a vulnerability description as input and outputs a 'High' severity classification with a bar chart showing the distribution of possible outcomes: High (70%), Medium (28%), Low (1%), and Critical (1%).

Left Window (CVE-2025-0108):

- CVE-2025-0108** (GCVE-0-2025-0108)
- Vulnerability from [cvelistv5](#)
- Published:** 2025-02-12 20:55
- Modified:** 2025-07-30 01:36
- Severity ?** **8.8 (High)** - CVSS:4.0/AV:N/AC:L/AT:N/PR:N
- VLA1 Severity ?** **5.9 (Medium)** - CVSS:4.0/AV:N/AC:L/AT:P/PR:N
- EPSS score ?** **High (confidence: 0.7843)**
- CWE** **CWE-306** - Missing Authentication for Critical Function
- Summary** An authentication bypass in the Palo Alto Networks PAN-OS software enables an unauthenticated attacker with network access to the management web interface and invoke certain PHP scripts. While invoking these PHP scripts does not enable remote code execution, it can negatively impact integrity and confidentiality of PAN-OS. You can greatly reduce the risk of this issue by restricting access to the management web interface to only trusted internal IP addresses according to our recommended best practices deployment guidelines <https://live.paloaltonetworks.com/t5/community-blogs/tips-and-tricks-how-to-secure-the-management-access-of-your-prisma-access-software>.
- References**
 - **URL** [CISA Known exploited vulnerability](#)
- Impacted products**
 - Vendor** [Palo Alto Networks](#)
- CISA Known exploited vulnerability**
- Data from the [Known Exploited Vulnerabilities Catalog](#)
- Date added: 2025-02-18

Right Window (Vulnerability Severity Classification):

Enter a vulnerability description, and the model will classify its severity level.

text

An authentication bypass in the Palo Alto Networks PAN-OS software enables an unauthenticated attacker with network access to the management web interface to bypass the authentication otherwise required by the PAN-OS management web interface and invoke certain PHP scripts. While invoking these PHP scripts does not enable remote code execution, it can negatively impact integrity and confidentiality of PAN-OS. You can greatly reduce the risk of this issue by restricting access to the management web interface to only trusted internal IP addresses according to our recommended best practices deployment guidelines <https://live.paloaltonetworks.com/t5/community-blogs/tips-and-tricks-how-to-secure-the-management-access-of-your-prisma-access-software>. This

Clear Submit

output

High

Severity	Percentage
High	70%
Medium	28%
Low	1%
Critical	1%

Vulnerability in Vulnerability-Lookup — published 25 September 2025

The screenshot displays the 'vulnerability lookup' web application. The left sidebar shows a list of vulnerabilities, with 'CVE-2025-60249 (GCVE-0-2025-60249)' selected. The main content area shows the details for this vulnerability, including its publication date (2025-09-25 14:10), severity (6.4 (Medium)), and CWE (CWE-79 - Improper Neutralization of Scripting). The summary describes a cross-site scripting (XSS) vulnerability in the handling of user-supplied input in the Comments, Bundles, and Sightings components. The references section lists the URL 'vulnerability-lookup' and the product 'vulnerability-lookup'. The impacted products section shows the vendor 'CIRCL' and the product 'vulnerability-lookup'.

GCVE-1-2025-0004
Vulnerability from [gna.1](#)

Published 2025-09-25 14:10
Modified 2025-09-25 14:10
Severity 10.0 (Critical) - [CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/HA:H/SC:H/SI:MSA/H](#)
VLA1 Severity Medium (confidence: 0.8514)
EPSS score Not yet available from FIRST.
CWE [CWE-79](#) - Improper Neutralization of Scripting

Summary
A cross-site scripting (XSS) vulnerability was discovered in the handling of user-supplied input in the Comments, Bundles, and Sightings components. Untrusted data was not properly sanitized before being rendered in templates and tables, which could allow attackers to inject arbitrary JavaScript into the application. The issue was due to unsafe use of innerHTML and insufficient validation of dynamic URLs and model fields. This vulnerability has been fixed by escaping untrusted data, replacing innerHTML assignments with safer DOM methods, encoding URLs with encodeURIComponent, and improving input validation in the affected models.

References
[URL](#)

Impacted products

Vendor	Product	Version
CIRCL	vulnerability-lookup	Version: View

[JSON](#) [Share](#) [Add a sighting](#) [To clipboard](#) [Edit](#) [Delete](#)

Patched in Cambridge at Vuln4Cast 2025 in the afternoon.

<https://github.com/vulnerability-lookup/vulnerability-lookup/commit/afa12347f1461d9481eba75ac19897e80a9c7434>

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

cve-2025-57623

vulnerability.circl.lu/vuln/cve-2025-57623#sightings

CVE-2025-57623 (GCVE-0-2025-57623)

Vulnerability from [cvelistv5](#)

Published 2025-09-25 00:00
Modified 2025-09-25 17:28
Severity ?
VLAI Severity ? High (confidence: 0.957)
EPSS score ? Not yet available from FIRST.
CWE n/a
Summary A NULL pointer dereference in TOTOLINK N600R firmware v4.3.0cu.7866_B2022506 allows attackers to cause a Denial of Service.

References
▶ **URL**

Tags

Impacted products

Vendor	Product	Version
n/a	n/a	Version: n/a

[Show details on NVD website](#)

JSON ▼

Share ▼

Add a sighting ▼

To clipboard

Edit

[Related vulnerabilities](#) 0 [Comments](#) 0 [Bundles](#) 0 [Sightings](#) 2 [Sightings correlations](#) [CWEs and mitigations](#)

[MITRE EMB3D](#)

Sightings

Author	Source	Type	Date
automation	https://infosec.exchange/users/cR0w/statuses/115266254335547502 (correlations)	seen	55 minutes ago
automation	https://gist.github.com/z472421519/d17061ea79a72d39fe69c000fa1a6280 (correlations)	seen	16 days ago

Nomenclature 2025-09-09T17:39:05+00:00

TLP:CLEAR

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

CWE PARENT Patch Vulnerability Patch Classification Roberta Base - a Hugging Face Space by CIRCL — Mozilla Firefox

CWE PARENT Patch Vulner: x +

huggingface.co/spaces/CIRCL/CWE-PARENT-patch-Vulnerab

Spaces CIRCL/CWE-PARENT-patch-Vulnerability-Patch-Classification-Roberta-Base like 0

Running

CWE Prediction from Commit Message or Vulnerability Description

This tool uses a fine-tuned model to predict CWE categories from Git commit messages and vulnerability descriptions. Predicted child CWEs are mapped to their parent CWEs if applicable.

commit_message

A cross-site scripting (XSS) vulnerability was discovered in the handling of user-supplied input in the Comments, Bundles, and Sightings components. Untrusted data was not properly sanitized before being rendered in templates and tables, which could allow attackers to inject arbitrary JavaScript into the application. The issue was due to unsafe use of `innerHTML` and insufficient validation of dynamic URLs and model fields. This vulnerability has been found by scanning untrusted data.

Clear Submit

output

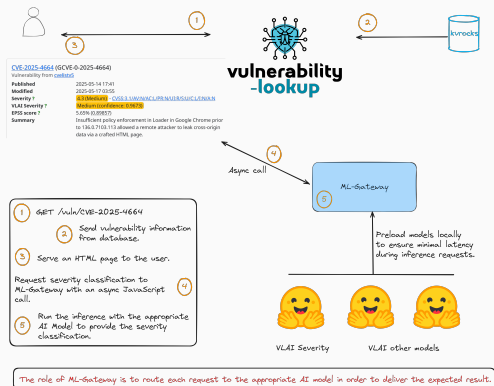
CWE-74

CWE-74	42%
CWE-436	8%
CWE-913	6%
CWE-664	6%
CWE-697	3%

Share via Link

Examples

A vulnerability has been found in cfire24 ajaxlife up to 0.3...



- 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>

CVE-2025-44897 (CVE-0-2025-44897)
Vulnerability from [cveids](#)
Published 2025-05-20 00:00
Modified 2025-05-20 20:27
Severity ?
VLLM Severity ?
Summary **Critical confidence: 0.8793**
FW-WGS-804HPT v1.305b241111 was discovered to contain a stack overflow via the byhttp_snip parameter in the web_tool_upgradeManager_post function.

The case of missing severity information in the advisory.

Example

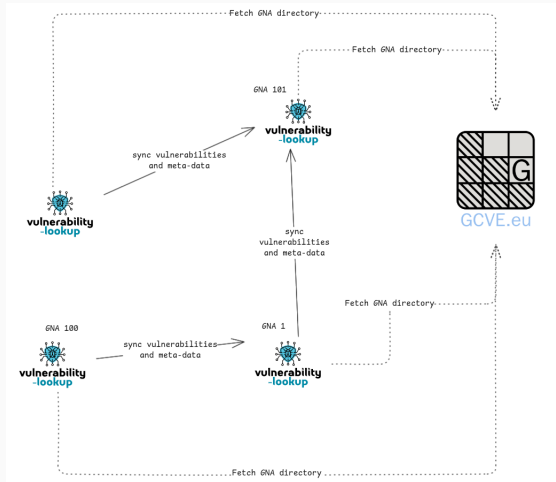
```
$ curl -X 'POST' \  
  'https://vulnerability.circl.lu/api/vlai/severity-classification' \  
  -H 'accept: application/json' \  
  -H 'Content-Type: application/json' \  
  -d '{  
    "description": "An authentication bypass in the API component of Ivanti Endpoint  
      Manager Mobile 12.5.0.0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

**Lookup and AI are Cool, but
Publishing is Even Cooler**

- The primary role of GCVE²⁹ is to provide **globally unique identifiers** to GCVE Numbering Authorities (GNAs).
- **GNAs operate autonomously**, with full control over how they assign and manage identifiers.
- **GCVE publishes Best Current Practices (BCPs)** on directory management, Coordinated Vulnerability Disclosure (CVD), and publication protocols.
- GCVE maintains and publishes the **official directory of all GNAs**, including their publication endpoints.

²⁹<https://gcve.eu/>

Decentralized Publication Standard



Closing

Future Development

- Deeper analysis of the content and context of sightings, including **source reliability assessment**.
- Full-text search capabilities across all integrated sources.
- Integration of scoring models such as Vuln4Cast³⁰, with testing planned on our dataset to enhance reproducibility.
- **Improved notification capabilities** for newly observed vulnerabilities via webhooks.



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

³⁰<https://github.com/FIRSTdotorg/Vuln4Cast>

References

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

📄 CIRCL public instance <https://vulnerability.circl.lu>

🔗 Source code <https://github.com/vulnerability-lookup/vulnerability-lookup>

📁 Dataset, AI Model Training, Models
<https://github.com/vulnerability-lookup/VulnTrain>