Vulnerability Lookup

An open source tool to support CVD processes

CIRCL
Computer Incident
Response Center
Luxembourg

Co-funded by
the European Union

Cédric Bonhomme
TLP:CLEAR

cedric.bonhomme@circl.lu

2024-10-08

Content at glance

Origin of the project

- Who is behind Vulnerability Lookup?
- Origin and Challenges we aim to address
- Primary goals

Main functionalities

- Current features
- And current sources
- Improving threat intelligence

Technical considerations

Overview and demo

Closing

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.

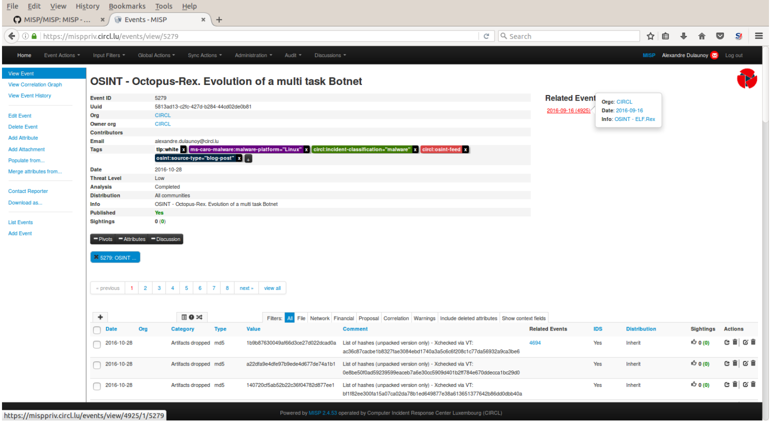
[1] https://github.com/cve-search/vulnerability-lookup

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

It's all about Open Source, Sharing and Intelligence

- We are always the first users of the tools we develop (URL Abuse, automated take-down requests, Passive DNS/SSL, cve-search, etc.). Only Open Source tool.
- Some tools adopted by entities such as NATO, Europol, Red Cross, NGO agencies, private sector, etc.
- Since 15 years we promote the sharing of information (IOCs, models, taxonomies, etc.) in various fields.
- Numerous ways to get information (PoC/exploit, remediations, descriptions, etc.) about vulnerabilities:
    - collaborative platforms: **MISP**
    - data collection, (dark) Web monitoring: **AIL**
    - official sources like NVD or CSAF feeds: **Vulnerability Lookup**
    - etc.

MISP - Open Source Threat Intelligence and Sharing Platform



OSINT - Octopus-Rex. Evolution of a multi task Botnet

Event ID	5279
Uuid	5813ad13-c2fc-427d-b284-44cd02de0b81
Org	CIRCL
Owner org	CIRCL
Contributors	
Email	alexandre.dulaunoy@circl.lu
Tags	tlp:white x ms-caro-malware:malware-platform="Linux" x circl:incident-classification="malware" x circl:osint-feed x osint:source-type="blog-post" x +
Date	2016-10-28
Threat Level	Low
Analysis	Completed
Distribution	All communities
Info	OSINT - Octopus-Rex. Evolution of a multi task Botnet
Published	Yes
Sightings	0 (0)

Related Events

2016-09-16 (4925)

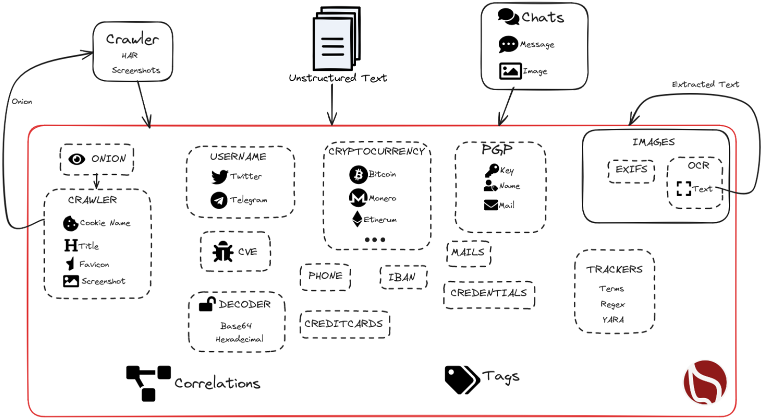
Orgc: CIRCL
Date: 2016-09-16
Info: OSINT - ELF.Rex

Date	Org	Category	Type	Value	Comment	Related Events	IDS	Distribution	Sightings	Actions
2016-10-28		Artifacts dropped	md5	1b9b87630049af66d3ce27d022dcad0a	List of hashes (unpacked version only) - Xchecked via VT: ac36c87cacbe1b8327fae3084ebd1740a3a5c6c6f208c1c77da56932a9ca3be6	4694	Yes	Inherit	0 (0)	
2016-10-28		Artifacts dropped	md5	a22dfa9e4dfe97b9ede4d677de74a1b1	List of hashes (unpacked version only) - Xchecked via VT: 0e8be50f0ad59239599eaceb7a6e30cc5909d401b2ff784e670ddecca1bc29d0		Yes	Inherit	0 (0)	
2016-10-28		Artifacts dropped	md5	140720cf5ab52b22c36f04782d877ee1	List of hashes (unpacked version only) - Xchecked via VT: bf1f82ee300fa15a07ca02da78b1ed649877e38a613651377642b86dd0dbb40a		Yes	Inherit	0 (0)	

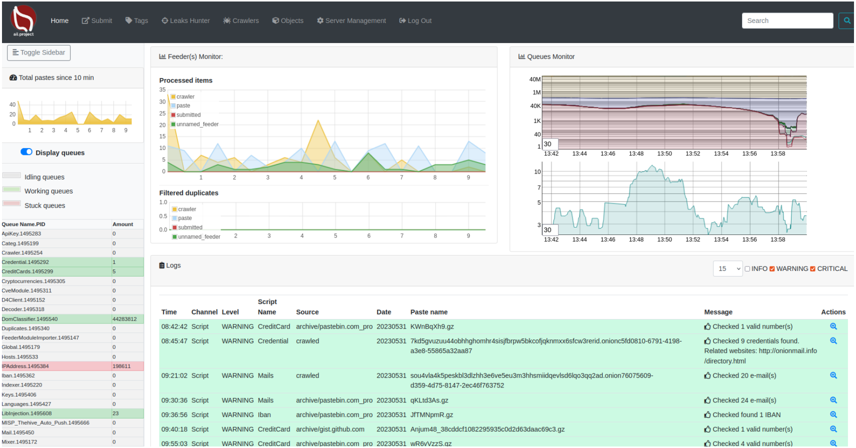
Powered by MISP 2.4.53 operated by Computer Incident Response Center Luxembourg (CIRCL)

https://misppriv.circl.lu

AIL framework - Analysis Information Leak framework



AIL framework - Analysis Information Leak framework



Queue Name.PID	Amount
ApiKey.1495283	0
Categ.1495199	0
Crawler.1495254	0
Credential.1495292	1
CreditCards.1495299	5
Cryptocurrencies.1495305	0
CveModule.1495311	0
D4Client.1495152	0
Decoder.1495318	0
DomClassifier.1495540	44283812
Duplicates.1495340	0
FeederModuleImporter.1495147	0
Global.1495179	0
Hosts.1495533	0
IPAddress.1495384	198611
Iban.1495362	0
Indexer.1495220	0
Keys.1495406	0
Languages.1495427	0
LibInjection.1495608	23
MISP_Thehive_Auto_Push.1495666	0
Mail.1495450	0
Mixer.1495172	0

Time	Channel	Level	Script Name	Source	Date	Paste name	Message	Actions
08:42:42	Script	WARNING	CreditCard	archive/pastebin.com_pro	20230531	KWnBqXh9.gz	Checked 1 valid number(s)	🔍
08:45:47	Script	WARNING	Credential	crawled	20230531	7kd5gvuzuu44obhhghomhr4sisjfbrpw5bkcofjqknmxx6sfcw3rerid.onionc5fd0810-6791-4198-a3e8-55865a32aa87	Checked 9 credentials found. Related websites: http://onionmail.info/directory.html	🔍
09:21:02	Script	WARNING	Mails	crawled	20230531	sou4vla4k5peskbl3dlzhh3e6ve5eu3m3hhsmiidqevlsd6lqo3qq2ad.onion76075609-d359-4d75-8147-2ec46f763752	Checked 20 e-mail(s)	🔍
09:30:36	Script	WARNING	Mails	archive/pastebin.com_pro	20230531	qKLtd3As.gz	Checked 24 e-mail(s)	🔍
09:36:56	Script	WARNING	Iban	archive/pastebin.com_pro	20230531	JfTMNpmR.gz	Checked found 1 IBAN	🔍
09:40:18	Script	WARNING	CreditCard	archive/gist.github.com	20230531	Anjum48_38cddcf1082295935c0d2d63daac69c3.gz	Checked 1 valid number(s)	🔍
09:55:03	Script	WARNING	CreditCard	archive/pastebin.com_pro	20230531	wR6vVzzS.gz	Checked 4 valid number(s)	🔍

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`

Primary goals

- Fast lookup.
- Agnostic to sources and formats.
- A tool was needed to support our use case for the CVD process, including commenting, bundling, publishing, and extending vulnerability information.
- Support the NIS2 activities at CIRCL.

Main functionalities of Vulnerability Lookup 1/2

What we have implemented so far (version 1.7.0).

- A fast lookup API to search for vulnerabilities and find correlations per vulnerability identifier.
- An API for adding new vulnerability including ID assigment, state and disclosure.
- Modular system to import **different vulnerability sources**.
- Support of **local source** per instance with custom IDs and JSON schemas (data validation).

Main functionalities of Vulnerability Lookup 2/2

- **CVE Publication as CNA**: Integration of Vulnogram.[4]
- Support for the Coordinated Vulnerability Disclosure process (in progress).
- Extensive support for RSS/Atom.
- Support for user accounts with Two-Factor Authentication.
- Vulnerability Lookup is also a collaborative platform[5].

The project is evolving rapidly.

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

[5] Comments, bundling, and soon sighting...

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)

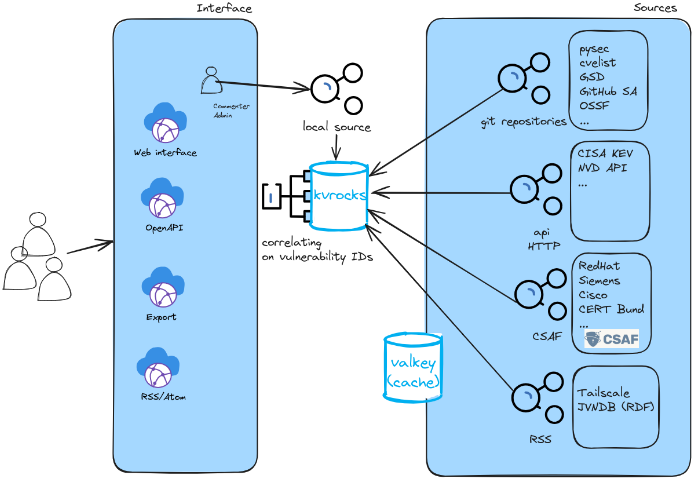
Open Data Initiative: Committed to regularly publishing comprehensive JSON dumps of all integrated sources as open data.

Improving threat intelligence

- **Tags:** Ability to attach tags to comments from the MISP taxonomies for vulnerabilities[6].
- **Sightings:** Allowing users to report whether they have witnessed a particular event, including the date, source of the sighting, and the object.
- **Comments:** To provide additional context about remediation, proof of concept, etc.
- **Bundles:** To allow analysts to combine similar vulnerabilities into a single container.

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

Vulnerability Lookup high level architecture

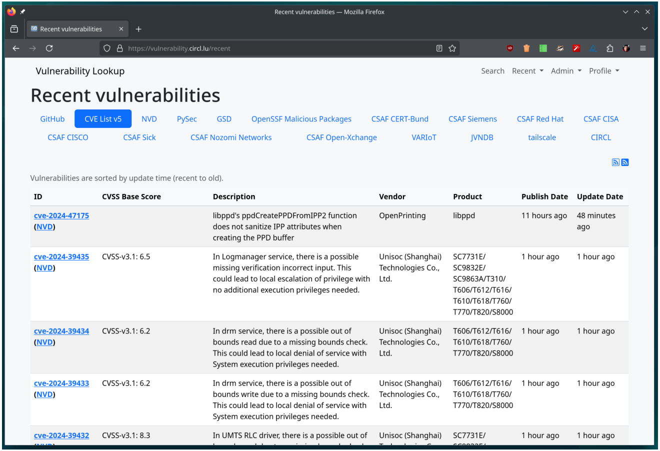


Overview of the vulnerability-lookup architecture - https://github.com/cve-search/vulnerability-lookup

Technology choices

- Runs on any GNU/Linux distribution and easy to deploy.
- Backend and API written in Python.
- Swagger (OpenAPI) is used to document the API.
- Kvrocks for the storage, and Valkey for the cache.
- PostgreSQL as a transactional database (optional).

Overview of the Web interface



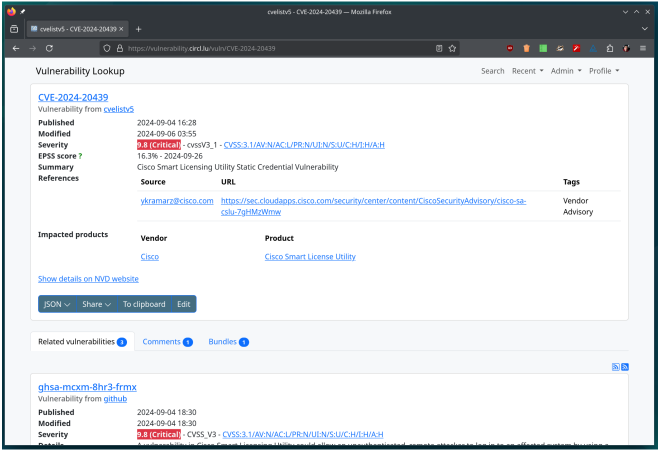
Recent vulnerabilities

Vulnerabilities are sorted by update time (recent to old).

ID	CVSS Base Score	Description	Vendor	Product	Publish Date	Update Date
cve-2024-47175 (NVD)		libppd's ppdCreatePPDFromIPP2 function does not sanitize IPP attributes when creating the PPD buffer	OpenPrinting	libppd	11 hours ago	48 minutes ago
cve-2024-39435 (NVD)	CVSS-v3.1: 6.5	In Logmanager service, there is a possible missing verification incorrect input. This could lead to local escalation of privilege with no additional execution privileges needed.	Unisoc (Shanghai) Technologies Co., Ltd.	SC7731E/ SC9832E/ SC9863A/T310/ T606/T612/T616/ T610/T618/T760/ T770/T820/S8000	1 hour ago	1 hour ago
cve-2024-39434 (NVD)	CVSS-v3.1: 6.2	In drm service, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	Unisoc (Shanghai) Technologies Co., Ltd.	T606/T612/T616/ T610/T618/T760/ T770/T820/S8000	1 hour ago	1 hour ago
cve-2024-39433 (NVD)	CVSS-v3.1: 6.2	In drm service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	Unisoc (Shanghai) Technologies Co., Ltd.	T606/T612/T616/ T610/T618/T760/ T770/T820/S8000	1 hour ago	1 hour ago
cve-2024-39432	CVSS-v3.1: 8.3	In UMTS RLC driver, there is a possible out of	Unisoc (Shanghai)	SC7731E/	1 hour ago	1 hour ago

Figure: Recent vulnerabilities

Overview of the Web interface


cvelistv5 - CVE-2024-20439 — Mozilla Firefox
cvelistv5 - CVE-2024-20439
https://vulnerability.circl.lu/vuln/CVE-2024-20439
Vulnerability Lookup
Search
Recent
Admin
Profile
JSON
Share
To clipboard
Edit
Related vulnerabilities 3
Comments 1
Bundles 1

CVE-2024-20439

Vulnerability from cvelistv5

Published	2024-09-04 16:28
Modified	2024-09-06 03:55
Severity	9.8 (Critical) - cvssV3_1 - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
EPSS score ?	16.3% - 2024-09-26
Summary	Cisco Smart Licensing Utility Static Credential Vulnerability

References

Source	URL	Tags
ykramarz@cisco.com	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cslu-7gHMzWmw	Vendor Advisory

Impacted products

Vendor	Product
Cisco	Cisco Smart License Utility

Show details on NVD website

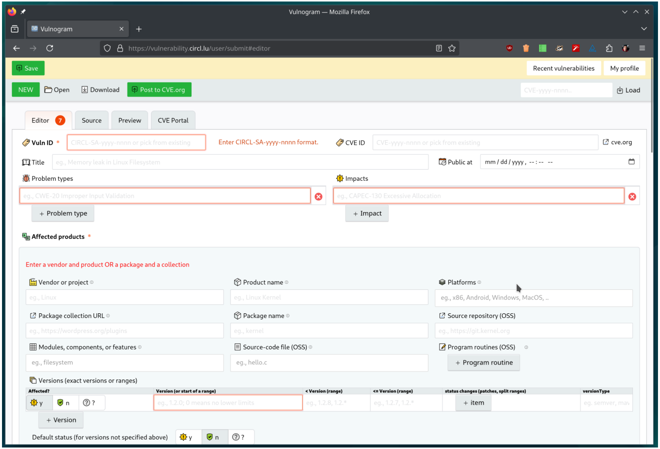
ghsa-mcxm-8hr3-frmx

Vulnerability from github

Published	2024-09-04 18:30
Modified	2024-09-04 18:30
Severity	9.8 (Critical) - CVSS_V3 - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Details	A vulnerability in Cisco Smart Licensing Utility could allow an unauthenticated, remote attacker to log in to an affected system by using a

Figure: A vulnerability with its details, correlations, comments, and bundles.

Overview of the Web interface

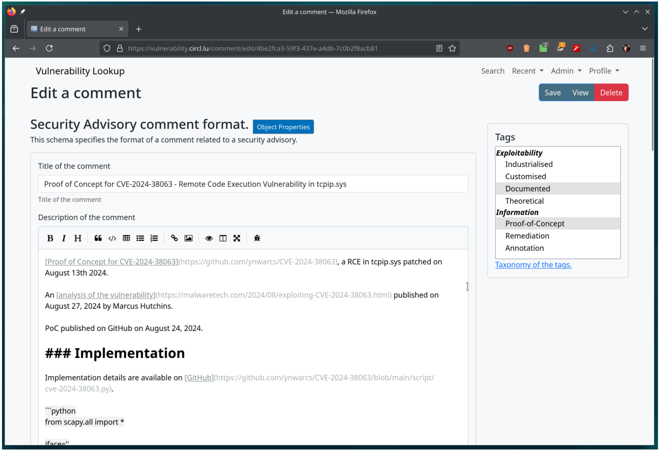

Vulnogram — Mozilla Firefox
Vulnogram
https://vulnerability.circl.lu/user/submit#editor
Save
Recent vulnerabilities
My profile
NEW
Open
Download
Post to CVE.org
CVE-yyyy-nnnn..
Load
Editor 7
Source
Preview
CVE Portal
Vuln ID *
CIRCL-SA-yyyy-nnnn or pick from existing
CVE ID
CVE-yyyy-nnnn or pick from existing
cve.org
Title
eg., Memory leak in Linux Filesystem
Public at
mm / dd / yyyy , -- : -- --
Problem types
eg., CWE-20 Improper Input Validation
+ Problem type
Impacts
eg., CAPEC-130 Excessive Allocation
+ Impact
Affected products *
Vendor or project
eg., Linux
Product name
eg., Linux Kernel
Platforms
eg., x86, Android, Windows, MacOS, ..
Package collection URL
eg., https://wordpress.org/plugins
Package name
eg., kernel
Source repository (OSS)
eg., https://git.kernel.org
Modules, components, or features
eg., filesystem
Source-code file (OSS)
eg., hello.c
Program routines (OSS)
+ Program routine
Versions (exact versions or ranges)
Affected?
Version (or start of a range)
< Version (range)
<= Version (range)
status changes (patches, split ranges)
versionType
y
n
?
eg., 1.2.0; 0 means no lower limits
eg., 1.2.8, 1.2.*
eg., 1.2.7, 1.2.*
+ item
eg. semver, mav
+ Version
Default status (for versions not specified above)
y
n
?

Enter CIRCL-SA-yyyy-nnnn format.

Enter a vendor and product OR a package and a collection

Figure: Vulnogram

Overview of the Web interface



Edit a comment — Mozilla Firefox
Edit a comment
https://vulnerability.circl.lu/comment/edit/4be2fca3-59f3-437e-a4db-7c0b2f8acb81
Vulnerability Lookup
Search
Recent
Admin
Profile
Save
View
Delete
Object Properties

Edit a comment

Security Advisory comment format.

This schema specifies the format of a comment related to a security advisory.

Title of the comment

Proof of Concept for CVE-2024-38063 - Remote Code Execution Vulnerability in tcpip.sys

Title of the comment

Description of the comment

~~~
[Proof of Concept for CVE-2024-38063](https://github.com/ynwarcs/CVE-2024-38063), a RCE in tcpip.sys patched on
August 13th 2024.

An [analysis of the vulnerability](https://malwaretech.com/2024/08/exploiting-CVE-2024-38063.html) published on
August 27, 2024 by Marcus Hutchins.

PoC published on GitHub on August 24, 2024.

### Implementation

Implementation details are available on [GitHub](https://github.com/ynwarcs/CVE-2024-38063/blob/main/script/
cve-2024-38063.py).

```python
from scapy.all import *

iface=''
~~~

Tags

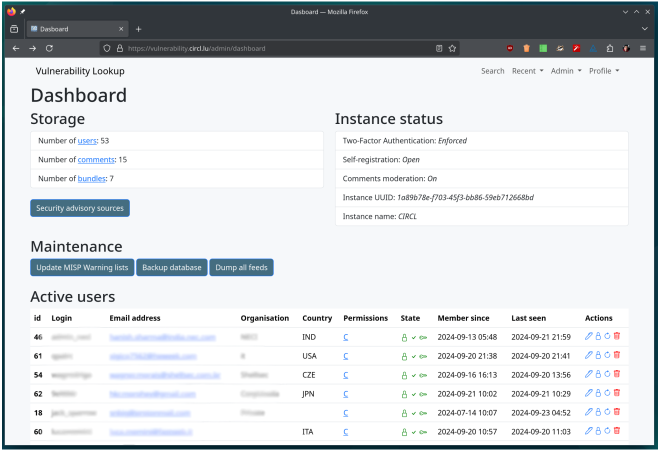
Exploitability
- Industrialised
- Customised
- Documented
- Theoretical

Information
- Proof-of-Concept
- Remediation
- Annotation

Taxonomy of the tags.

Figure: MISP warning lists

Overview of the Web interface



Dasboard — Mozilla Firefox
Dasboard
https://vulnerability.circl.lu/admin/dashboard
Vulnerability Lookup
Search
Recent
Admin
Profile

Dashboard

Storage

Number of users: 53

Number of comments: 15

Number of bundles: 7

Security advisory sources

Instance status

Two-Factor Authentication: *Enforced*

Self-registration: *Open*

Comments moderation: *On*

Instance UUID: *1a89b78e-f703-45f3-bb86-59eb712668bd*

Instance name: *CIRCL*

Maintenance

Update MISP Warning lists
Backup database
Dump all feeds

Active users

id	Login	Email address	Organisation	Country	Permissions	State	Member since	Last seen	Actions
46	[redacted]	[redacted]	[redacted]	IND	C	🔒 ✓ ⚷	2024-09-13 05:48	2024-09-21 21:59	✎ 🔒 ↻ 🗑
61	[redacted]	[redacted]	[redacted]	USA	C	🔒 ✓ ⚷	2024-09-20 21:38	2024-09-20 21:41	✎ 🔒 ↻ 🗑
54	[redacted]	[redacted]	[redacted]	CZE	C	🔒 ✓ ⚷	2024-09-16 16:13	2024-09-20 13:56	✎ 🔒 ↻ 🗑
62	[redacted]	[redacted]	[redacted]	JPN	C	🔒 ✓ ⚷	2024-09-21 10:02	2024-09-21 10:29	✎ 🔒 ↻ 🗑
18	[redacted]	[redacted]	[redacted]		C	🔒 ✓ ⚷	2024-07-14 10:07	2024-09-23 04:52	✎ 🔒 ↻ 🗑
60	[redacted]	[redacted]		ITA	C	🔒 ✓ ⚷	2024-09-20 10:57	2024-09-20 11:03	✎ 🔒 ↻ 🗑

Figure: Dashboard

Future development

- Sightings similar to those in MISP. Currently under development.
- We are interested in EPSS or similar models[7] and Vuln4Cast[8]. Experimental integration of EPSS. We would like to test it with our data set to regenerate the EPSS model.
- Enabling synchronization between Vulnerability Lookup instances.
- Full-text search across all sources.
- Data from the Fediverse / connection with AIL[9].

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

[7] https://www.first.org/epss

[8] https://github.com/FIRSTdotorg/Vuln4Cast

[9] https://www.ail-project.org

References

- Vulnerability lookup
  `https://github.com/cve-search/vulnerability-lookup`
- Online Vulnerability Lookup
  `https://vulnerability.circl.lu/recent`
- OpenAPI documentation
  `https://vulnerability.circl.lu/swagger.json`

Requests and Support

- 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