

What is OpenCVE ?

Please refer to [this file](#) to learn more. If you want to learn more about what it is, and how it works, you can check [the official documentation](#).

What is this fork ?

This fork adds several things to the OpenCVE project.

- A "client" system.

You can view this as a "category" feature. The goal is to add a client, and to register several Vendors or products in it. This way, you can follow your client, and be alerted whenever something impacting it happens.

- You can also add vendors or products to a followed client on the vendor and product list by hand.

- An new import function

You can import a client's subscriptions via an Excel file (xlsx) if it's format is correct (column "vendor", "product", "version" and "tag" are required).

If you are having problems with the installation or the deployed platform, email me at gael.lejeune@capgemini.com.

Cloning the library

```
git clone https://github.com/Gael-Lejeune/opencve-docker
```

Installation

Prerequisite

- Install Docker : <https://www.docker.com/products/docker-desktop>

If you want to know more about docker, you can read [here](#).

Installation steps

Configuration

Create a copy of the `opencve.cfg.example` file which is in the `conf` folder

```
cp ./conf/opencve.cfg.example ./conf/opencve.cfg
```

Edit the opencve.cfg file (remove the <> when you replace)

```
server_name = <your_listening_ip>:8000  
secret_key = "<your_secret_key>"
```

Listening_ip can be setup to 127.0.0.1

Secret_key should be between quotes and should not contain the character %, it should be a randomly generated key containing 32 characters.

Update the SMTP Configuration

For the moment, the outlook smtp server is used, please keep in mind that the email functions are not working for the moment, you are not forced to configure it.

```
[mail]  
; Choices are 'smtp' or 'sendmail'  
email_adapter = smtp  
  
; The 'From' field of the sent emails  
email_from = examplemail@outlook.com  
  
; Configuration to set up SMTP mails.  
smtp_server = smtp.office365.com  
smtp_port = 587  
smtp_use_tls = True  
smtp_username = examplemail@outlook.com  
smtp_password = examplepassword
```

Note that the email_from and smtp_username should be the same.

Check files & Line endings

Make sure that `./conf/opencve.cfg` and `./run.sh` are LF line terminated (and not CRLF, it could cause errors while building or running the container) If you want to learn more about LF and CRLF you can click [here](#). If you want to know how to change this using [Visual Studio Code](#), or [Notepad++](#).

Building & Cleaning

In the following section, if you are on a linux terminal, and if make is installed, you may use the make commands. Alternatively you could use the docker commands in your windows favorite terminal.

All the following command need to be used in a terminal, in the root folder of the project (you should be able to see files like "*makefile*" or "*Dockerfile*")

For Linux terminal users :

```
make
```

This will **not** import the data in the database. Check [Import data](#) for more informations on that part.

```
make clean
```

Please note that this command will prune your docker volumes, thus deleting any that is not currently used.

More details about the build

Build the OpenCVE image

```
make build
```

Create the container and start them

```
make up
```

Initialize & upgrade the database

```
make upgrade
```

Import data

```
make import
```

Create an admin

Please keep in mind that for now, you can only create users this way, as the email server is not set up. If you want to create a non-administrator account, simply remove the `--admin` option.

```
docker exec -it webserver opencv create-user myuser myuser@example.com --admin
>> Password:
>> Repeat for confirmation:
>> [*] User myuser created.
```

Create and start the beat

```
make beat
```

For windows terminal users

Build the OpenCVE image

```
docker compose build
```

Create the container and start them

```
docker-compose up -d postgres redis webserver celery_worker
```

Initialize & upgrade the database

```
docker exec -it webserver opencve upgrade-db
```

Import data

Please keep in mind that this process takes a long time and requires a lot of CPU power.

```
docker exec -it webserver opencve import-data
```

Alternatively, you can use the following command to import less CVEs, making it a bit faster and more suitable for testing.

```
docker exec -it webserver opencve import-light
```

Create an admin

```
docker exec -it webserver opencve create-user myuser myuser@example.com --admin
>> Password:
>> Repeat for confirmation:
>> [*] User myuser created.
```

Create, start the beat, and the other containers, use this function if you want to launch every service

```
docker-compose up -d postgres redis webserver celery_worker celery_beat
```

Check that everything is working fine

You can execute

```
docker ps
>> CONTAINER ID    IMAGE             COMMAND                                     CREATED          STATUS
PORTS              NAMES
>> 97e3ef4af44f    opencve:1.2.3    "./run.sh celery-beat"                   20 seconds ago  Up 58
minutes           celery_beat
>> faf7f59fff38    opencve:1.2.3    "./run.sh celery-wor..."               16 hours ago    Up 58
minutes           celery_worker
>> df0faac8526d    opencve:1.2.3    "./run.sh webserver ..."             16 hours ago    Up 58
minutes           0.0.0.0:8000->8000/tcp webserver
>> 63b7e90d2cd7    redis:buster     "docker-entrypoint.s..."              46 hours ago    Up 58
minutes           127.0.0.1:6379->6379/tcp redis
>> 38af0f416957    postgres:11      "docker-entrypoint.s..."              46 hours ago    Up 58
minutes           127.0.0.1:5432->5432/tcp postgres
```

If status is up everywhere, everything is working fine. You should now be able to reach the app on <your_listening_ip:your_port> on your favorite web browser.

Understanding the code

Tree

```
|— conf
|— opencve
|   |— opencve
|   |   |— api
|   |   |— checks
|   |   |— commands
|   |   |— controllers
|   |   |— migrations
|   |   |— models
|   |   |— static
|   |   |— tasks
|   |   |— templates
|   |   |— views
```

api

//TODO

Commands

This folder contains python scripts that are used to interact with the application from the command line. An example is `create_user.py` that is used to create a user:

```
root@df0faac8526d:/app# opencve create-user doc doc@test.com
Password:
Repeat for confirmation:
[*] User doc created.
```

If you want to create a new script, it is as follows
`example.py`

```
import click
#Import what you need
@click.command()
@click.argument("arg1")
@click.argument("arg2")
@with_appcontext
def example(arg1,arg2):
    //DO SOMETHING
```

Then add it to the `cli.py` file

```
from opencve.commands.example import example
.
.
.
cli.add_command(example)
```

After building and running the project again, you can access the webserver using :

```
docker exec -it webserver bash
```

and run

```
opencve example arg1 arg2
```

Alternatively, you could use :

```
docker exec -it webserver opencve example
```

Controllers

Contains some backend logic and models controllers.

Migrations

Contains the migrations files generated when building the project. Those can mostly be ignored as they are automatically generated.

Models

Models are used to create a table in the database. We can take the client.py as an example:

```
from opencve.context import _humanize_filter
from opencve.extensions import db
from opencve.models import BaseModel, clients_vendors, clients_products,
users_clients

class Client(BaseModel):
    __tablename__ = "clients"

    name = db.Column(db.String(), nullable=False, unique=True)

    # Relationships
    vendors = db.relationship("Vendor", secondary=clients_vendors)
    products = db.relationship("Product", secondary=clients_products)
    users = db.relationship("User", secondary=users_clients)

    @property
    def human_name(self):
        return _humanize_filter(self.name)

    def __repr__(self):
        return "<Client {}>".format(self.name)
```

In this example, the new table Client will inherit the BaseModel columns and will add the columns name, vendors, products and users.

As you can see, the last three columns are in a relationship with other table and we can assure that using:

```
from opencve.models import clients_vendors
vendors = db.relationship("Vendor", secondary=clients_vendors)
```

in **init.py** we have:


```
clients_vendors = db.Table(
    "clients_vendors",
    db.Column(
        "client_id", UUIDType(binary=False), db.ForeignKey("clients.id"),
        primary_key=True
    ),
    db.Column(
        "vendor_id",
        UUIDType(binary=False),
        db.ForeignKey("vendors.id"),
        primary_key=True,
    ),
)
```

which is used to link client vendors column with the vendors table.

Tasks

The task folder contains 3 main scripts , events.py, alerts.py and reports.py. I will explain one by one:

events.py

The script will check the nist database to see if there are any new CVEs. If yes, they will be downloaded and added to that database and an event will be created.

alerts.py

The script will check if there are any new events, if yes it will create alerts for the concerned users.

reports.py

The script will check if there are any new alerts, if yes it will send reports to the concerned users (via the platform and emails if smtp is configured)

Templates

Contains the HTML pages to be rendered. It uses jinja to interact with the views controllers.

Views

Used to control the templates and provide them with data This is an example:

```
from flask import request, render_template
from opencve.controllers.main import main
from opencve.controllers.clients import ClientController #We import the client
controller
from opencve.utils import get_clients_letters
@main.route("/clients") #The url of the page
def clients():
    clients, _, pagination = ClientController.list(request.args)
```

```

return render_template(
    "clients.html", #The path to the template
    clients=clients, # Arguments we can send to the HTML page
    letters=get_clients_letters(),
    pagination=pagination,
)

```

In the clients.html, we will be able to access the clients variable using jinja:

```

{% for client in clients.items() %}
    .
    .
    .
    .
{% endfor %}

```

Features that are specific to this fork

Please note that this section is about features that are currently in progress or likely to evolve. This section may not be up to date.

Client model

```

from opencve.context import _humanize_filter
from opencve.extensions import db
from opencve.models import BaseModel,
clients_vendors,clients_products,users_clients

class Client(BaseModel):
    __tablename__ = "clients"

    name = db.Column(db.String(), nullable=False, unique=True)

    # Relationships
    vendors = db.relationship("Vendor", secondary=clients_vendors)
    products = db.relationship("Product", secondary=clients_products)
    users = db.relationship("User", secondary=users_clients)

    @property
    def human_name(self):
        return _humanize_filter(self.name)

    def __repr__(self):
        return "<Client {}>".format(self.name)

```

In addition, we needed to create `clients_vendors`, `clients_products` and `users_clients` in order to assure the relationship between the client table and vendors, products and users table respectively. We discussed those relationships before and how to create them in the `init.py` file.

In `admin.py`, I needed to add the `ClientModelView` as below :

```
from opencve.models.clients import Client
class ClientModelView(AuthModelView):
    page_size = 20
    create_modal = False
    edit_modal = False
    can_view_details = True
    column_list = ["name", "created_at"]
```

Client tables are now added automatically when building the project.

Command to create a client

The `create_client.py` script is used to create a client, it can be used as follows:

```
docker exec -it webserver opencve create-client <client-name>
```

The user is able to manage the client subscriptions : The user should be created beforehand.

A view to see all the existing clients

The page `templates/clients.html` alongside `views/client.py` and `controllers/subscriptions.py` are used to view the client table and manage subscription for users.

The screenshot displays the 'Clients' management interface. On the left is a dark sidebar with the 'glejeune' logo and navigation links: Dashboard, Reports, Vulnerabilities (CVE), Vendors (CPE), Categories (CWE), and Clients. The main content area has a header 'Clients' and a sub-header 'clients (1)'. Below this is a table with columns: Client, Vendors, Products, and Actions. The table contains one entry: 'Test' with 1 vendor and 2 products, and an 'Unsubscribe' button. To the right of the table is a search bar with a magnifying glass icon and a 'Search' button. Below the search bar is a 'Filter by letter' section with a grid of letters A-Z, @, and 0-9. At the bottom right is a 'Create a new client' form with a 'Create' button and a text input for 'Client name'. The footer of the page reads 'Copyright © 2021 OpenCVE.'

It is used exactly like the vendors page but to manage clients.

A view to see the details of a client and modify it

The user is now able to see and update the client subscriptions manually (we will see that next) or using an excel file.

We can do that by navigating to `"/client/<client name>"`.

The screenshot shows the OpenCVE web application interface. The left sidebar contains navigation links: Dashboard, Reports, Vulnerabilities (CVE), Vendors (CPE), Categories (CWE), and Clients. The main content area is titled 'test' and shows the client details for 'test'. It includes sections for 'Client vendors (1)' (listing Microsoft), 'Client products (2)' (listing Log4j and Enterprise Linux Server), an 'Upload File' section with instructions and a file selection button, and an 'Edit Client name' section with a text input field and a 'Delete' button. The breadcrumb trail at the top right indicates 'OpenCVE > Clients > test'.

Using an excel file (.xlsx), the user can update the client products. The excel file format is described on the web page. We've implemented a searching algorithm that will look for the product in the database if the tag is not precised. If a tag is precised, it has to be in the database.

A	B	C	D	E	F	G
Name	Domain	Vendor	Product	OS Version	Comment	OpenCVE tag
AZRSEA1LZBXPXP1	PRD	RedHat	REHL (64 bit)	Red Hat Enterprise Linux Server release 7.6 (Maipo)	Obsolete	enterprise_linux_server
AZRSEAWDC01	PRD	Microsoft	Windows Server (64 bit)	Windows Server 2016 Datacenter	Maintained	windows_server_2016

The `read_excel` is the function that will read the excel input and populate the database, it can be found at `controllers/clients.py`. The searching function can be found in the same file.

For the moment, the function is not perfectly optimized and can only use .xlsx files.

Updated Dashboard

Updated dashboard to be able to see the CVEs related to a followed client.

This was done by updating the `template/home.html` page alongside `"controllers/home.py"`.

The main code was to check the current user clients and add their respective vendors and products to the vendors list.

Last CVE updates

19 Jan 2022

CVE-2021-44228 has changed 04:15

Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

CVSS v3 **10.0 CRITICAL**
CVSS v2 **9.3 HIGH**

References changed 0 changed, 1 added, 0 removed

Vendors 9 Apache, Cisco, Debian and 6 more
Products 153 Log4j, Advanced Malware Protection Virtual Private Cloud Appliance, Automated Subsea Tuning and 150 more

18 Jan 2022

CVE-2022-21881 has changed 20:02

Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21879.

CVSS v3 **7.8 HIGH**
CVSS v2 **7.2 HIGH**

Subscriptions

Clients (1) Test

Tags

Last Reports

Date	Vendors & Products
19/01/22	Debian, Microsoft, Suse Linux Enterprise Server and 4 more

Added client Action in vendor and products

If the current user is following a client, he will be able to add new vendors and products to the client subscriptions directly from the vendors or products pages:

Vendors

Vendors (26557)

Vendor	Products	Actions	test
-	2	Subscribe	Add
01org	1	Subscribe	Add
\\$0.99 Kindle Books Project	1	Subscribe	Add
Overkill	1	Subscribe	Add
1000guess	1	Subscribe	Add
100plus	1	Subscribe	Add
101 Project	1	Subscribe	Add
1024cms	1	Subscribe	Add
1024 Cms	1	Subscribe	Add
1024tools	1	Subscribe	Add
10-4 Aps	1	Subscribe	Add
10-strike	2	Subscribe	Add
10web	5	Subscribe	Add
111webcalendar	1	Subscribe	Add

Search

Search

Filter by letter

A	B	C	D	E	F	G	H	I	J	K	L	M	N
O	P	Q	R	S	T	U	V	W	X	Y	Z	@	0
1	2	3	4	5	6	7	8	9					

Managing reports and emails

In order to create alerts for users subscribed to a client we edited the tasks/alerts.py script

```
# Product contains the separator
if PRODUCT_SEPARATOR in v:
    vendor = Vendor.query.filter_by(
        name=v.split(PRODUCT_SEPARATOR)[0]
    ).first()
    product = Product.query.filter_by(
        name=v.split(PRODUCT_SEPARATOR)[1], vendor_id=vendor.id
```

```

).first()
clients = Client.query.filter(
    Client.products.contains(product)
).all()
for user in product.users:
    if user not in users.keys():
        users[user] = {"products": [], "vendors": []}
    users[user]["products"].append(product.name)
for client in clients:
    for user in client.users:
        if user not in users.keys():
            users[user] = {"products": [], "vendors": []}
            users[user]["products"].append(product.name)

# Vendor
else:
    vendor = Vendor.query.filter_by(name=v).first()
    clients = Client.query.filter(
        Client.vendors.contains(vendor)
    ).all()
    for user in vendor.users:
        if user not in users.keys():
            users[user] = {"products": [], "vendors": []}
            users[user]["vendors"].append(vendor.name)
    for client in clients:
        for user in client.users:
            if user not in users.keys():
                users[user] = {"products": [], "vendors": []}
                users[user]["vendors"].append(vendor.name)

```

We loop through the user clients and select the vendors and products from them.

This will create a list of users that will receive emails.

Encountred problems

- When you want to upgrade the DB, you will sadly have to make clean and thus re-import the data. The "import-light" function may be optimized to make it even faster and thus help with this problem.
- Setting up the SMTP server is tricky, the problem is that the "email_from" and "smtp_username" should be the same else it won't work. The logs didn't explain this and i had to do alot of testing to figure it out.
- Running the default present tests is still a challenge
- Please use info() or logger.info() to debug or display logs as print() may not display correctly