

Shyam Bhanushali

CVE-2019-14287- Sudo Privilege Escalation Vulnerability

Description: "A flaw was found in the way sudo implemented running commands with arbitrary user ID. If a sudoers entry is written to allow the attacker to run a command as any user except root, this flaw can be used by the attacker to bypass that restriction."

Configuring the vulnerability in my kali system.

Step 1: Downloading the vulnerable sudo version(1.8.27) on the system.

Command:

wget

https://github.com/sudo-project/sudo/releases/download/SUDO_1.8.27/sudo_1.8.27-1_ubuntu1604_amd64.deb

```
root@kali2:~# wget https://github.com/sudo-project/sudo/releases/download/SUDO_1.8.27/sudo_1.8.27-1_ubuntu1604_amd64.deb
--2021-04-14 15:03:39-- https://github.com/sudo-project/sudo/releases/download/SUDO_1.8.27/sudo_1.8.27-1_ubuntu1604_amd64.deb
Resolving github.com (github.com)... 140.82.113.4
Connecting to github.com (github.com)|140.82.113.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://github-releases.githubusercontent.com/57972154/6b401480-e0a8-11e9-9acd-ecabd9efc9e7?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20210414%2Fus-east-1%2F%3A%2Faws4_request&X-Amz-Date=20210414T190328Z&X-Amz-Expires=300&X-Amz-Signature=3f0b16e87aa8c5727fb170402c92ddf0f98331f2b4cddae907972676299a60fdb6X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=57972154&response-content-disposition=attachment%3B%20filename%3Dsudo_1.8.27-1_ubuntu1604_amd64.deb&response-content-type=application%2Foctet-stream [following]
--2021-04-14 15:03:39-- https://github-releases.githubusercontent.com/57972154/6b401480-e0a8-11e9-9acd-ecabd9efc9e7?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20210414%2Fus-east-1%2F%3A%2Faws4_request&X-Amz-Date=20210414T190328Z&X-Amz-Expires=300&X-Amz-Signature=3f0b16e87aa8c5727fb170402c92ddf0f98331f2b4cddae907972676299a60fdb6X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=57972154&response-content-disposition=attachment%3B%20filename%3Dsudo_1.8.27-1_ubuntu1604_amd64.deb
Resolving github-releases.githubusercontent.com (github-releases.githubusercontent.com)... 185.199.108.154, 185.199.109.154, 185.199.110.154, ...
Connecting to github-releases.githubusercontent.com (github-releases.githubusercontent.com)|185.199.108.154|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1368752 (1.3M) [application/octet-stream]
Saving to: 'sudo_1.8.27-1_ubuntu1604_amd64.deb'
```

Step 2: Installing this version of SUDO.

Command:

dpkg -i sudo_1.8.27-1_ubuntu1604_amd64.deb

```
root@kali2:~# dpkg -i sudo_1.8.27-1_ubu1604_amd64.deb
(Reading database ... 323261 files and directories currently installed.)
Preparing to unpack sudo_1.8.27-1_ubu1604_amd64.deb ...
Unpacking sudo (1.8.27-1) over (1.8.10p3-1+deb8u2) ...
Setting up sudo (1.8.27-1) ...
Installing new version of config file /etc/pam.d/sudo ...
Installing new version of config file /etc/sudoers ...
Processing triggers for man-db (2.7.0.2-5) ...
root@kali2:~# sudo --version
```

Step 3: Checking if the installation was successful or not

Command:

sudo --version

```
root@kali2:~# sudo --version
Sudo version 1.8.27
Configure options: --prefix=/usr --with-all-in
tor=/usr/bin/editor --with-timeout=15 --with-p
dir=/usr/share/man --libexecdir=/usr/lib --wit
ith-sssd-lib=/usr/lib/x86_64-linux-gnu --disab
Sudoers policy plugin version 1.8.27
Sudoers file grammar version 46
```

The installation of sudo version 1.8.27 was successful.

Step 4: Adding a low level user.

Command:

adduser admin

In this case, I'll be adding a user called admin and set an easy password for demonstration purposes.

```
root@kali2:~# adduser admin
Adding user `admin' ...
Adding new group `admin' (1001) ...
Adding new user `admin' (1000) with group `admin' ...
Creating home directory `/home/admin' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] Y
```

Step 5: Configuring sudoers file

Command:

nano /etc/sudoers

```
root@kali2:~# nano /etc/sudoers
```

```
root@kali2: ~
File Edit View Search Terminal Help
GNU nano 2.2.6 File: /etc/sudoers
# for the new value, or press ENTER for the default
## of the user they are running the command as (root by default).
# Defaults targetpw # Ask for the password of the target user
# ALL=ALL=(ALL) ALL # WARNING: only use this together with 'Defaults targetpw'
    Home Phone []:
## Read drop-in files from /etc/sudoers.d
## (the '#' here does not indicate a comment)
#includedir /etc/sudoers.d
```

Adding an entry for user admin at the end of the sudoers file. This configuration allows user "admin" to run "/bin/bash" command as any other user except root.

admin ALL = (ALL, !root) /bin/bash

```
root@kali2: ~
File Edit View Search Terminal Help
GNU nano 2.2.6 File: /etc/sudoers
r the new value, or press ENTER for the default
## of the user they are running the command as (root by default).
# Defaults targetpw # Ask for the password of the target user
# ALL=(ALL) ALL # WARNING: only use this together with 'Defaults targetpw'
Home Phone []:
## Read drop-in files from /etc/sudoers.d
## (the '#' here does not indicate a comment)
#include_dir=/etc/sudoers.d
admin ALL=(ALL,!root) /bin/bash
```

However due to a flaw in this, the user admin could run any command as root just by specifying the user-ID of root(id = 1) that we will see in the exploitation video.

Step 6: Next step is to start the ssh service on the machine so that users can log into it and try exploiting the box.

Command:

service ssh start

service ssh status

```
root@kali2:~# service ssh start
root@kali2:~# service ssh status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled)
   Active: active (running) since Sun 2021-04-11 19:34:18 EDT; 5 days ago
 Main PID: 865 (sshd)
   CGroup: /system.slice/ssh.service
           └─865 /usr/sbin/sshd

Apr 15 18:58:02 kali2 sshd[22967]: pam_unix(sshd:auth): check pass; user unknown
Apr 15 18:58:02 kali2 sshd[22967]: pam_unix(sshd:auth): authentication fail...44
Apr 15 18:58:03 kali2 sshd[22961]: Failed password for invalid user test fr...h2
Apr 15 18:58:03 kali2 sshd[22962]: Failed password for root from 192.168.50...h2
Apr 15 18:58:03 kali2 sshd[22964]: Failed password for invalid user webadmi...h2
Apr 15 18:58:04 kali2 sshd[22973]: Connection closed by 192.168.50.144 [preauth]
Apr 15 18:58:04 kali2 sshd[22972]: Connection closed by 192.168.50.144 [preauth]
Apr 15 18:58:04 kali2 sshd[22967]: Failed password for invalid user sysadmi...h2
Apr 15 19:09:00 kali2 sshd[22980]: Accepted password for admin from 192.168...h2
Apr 15 19:09:00 kali2 sshd[22980]: pam_unix(sshd:session): session opened f...0)
Hint: Some lines were ellipsized, use -l to show in full.
root@kali2:~#
```

References:

<https://access.redhat.com/security/cve/cve-2019-14287>