Shyam Bhanushali

Exploit Configuration using Ansible(Ubuntu)

CVE-2019-14287- Sudo Privilege Escalation Vulnerability

Sudo Version:

Sudo version 1.8.27

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.”

Prerequisites:

1. Ansible must be installed on the machine.

    Commands:

    a. sudo apt-add-repository --yes --update ppa:ansible/ansible
    b. sudo apt install ansible

2. SSH must be installed and enabled

Commands:

a. sudo apt update
b. sudo apt install openssh-server
c. sudo systemctl status ssh
d. Sudo ufw allow ssh

My Ansible Script:

```
- hosts: localhost
  become: true

  tasks:
    - name: Download sudo repository
      get_url:
        url:
https://github.com/sudo-project/sudo/releases/download/SUDO_1_8_27/sudo_1.8.27-1_ubu1604_amd64.deb
        dest: /tmp/
        mode: 600

    - name: Installing sudo
      apt:
        update_cache: yes
        deb: /tmp/sudo_1.8.27-1_ubu1604_amd64.deb
        force: yes

    - name: Add the user 'admin' with a specific uid and a primary group of 'admin'
      user:
        name: admin
        password: "{{ 'liverpool' | password_hash('sha512') }}"

    # Validate the sudoers file before saving
    - lineinfile:
        path: /etc/sudoers
        state: present
        insertafter: EOF
        line: 'admin  ALL = (ALL, !root) /bin/bash'
```

```
    validate: '/usr/sbin/visudo -cf %s'

  - name: "SSH service start"
    service:
      name: ssh
      state: started
```

Target VM: Ubuntu

Usage:

Command:

ansible-playbook playbook.yml

```
shyam@ubuntu:~/ansible$ ansible-playbook playbook.yml
[WARNING]: provided hosts list is empty, only localhost is available. Note that
the implicit localhost does not match 'all'

PLAY [localhost] ***********************************************************

TASK [Gathering Facts] *****************************************************
ok: [localhost]

TASK [Download sudo repository] ********************************************
changed: [localhost]

TASK [Installing sudo] *****************************************************
changed: [localhost]

TASK [Add the user 'admin' with a specific uid and a primary group of 'admin'] ***
changed: [localhost]

TASK [lineinfile] **********************************************************
changed: [localhost]

TASK [SSH service start] ***************************************************
ok: [localhost]

PLAY RECAP *****************************************************************
localhost                  : ok=6    changed=4    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

shyam@ubuntu:~/ansible$
```

We can see that our ansible playbook executed successfully and our exploit is configured.