Nro. Alerta:	EC-2022-15	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	27-enero-2022	**Vulnerabilidad de escalada de privilegios de Polkit - PwnKit**	Versión 1.0

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de incidente: Escalada de Privilegios
Nivel de riesgo: Alta

II. ALERTA

El grupo de investigación de seguridad informática Qualys dio a conocer una vulnerabilidad denominada PwnKit que afecta a ciertas distribuciones de sistemas operativos UNIX; permitiendo a cualquier usuario sin privilegios obtener privilegios totales de root.

Figura 1.- Ilustración asociada a PwnKit.
Fuente: Qualys

III. INTRODUCCIÓN

Esta vulnerabilidad hace referencia a un fallo de corrupción de memoria en **pkexec de PolKit** [1] (PolicyKit) ; a continuación, se mencionan ciertas características de Polkit:

- Controla los privilegios de todo el sistema; en sistemas operativos similares a Unix.
- Proporciona una forma organizada para que los procesos no privilegiados se comuniquen con los procesos privilegiados.
- Ejecuta comandos con privilegios elevados usando el comando pkexec seguido del comando que se pretende ejecutar.
- pkexec está instalado de forma predeterminada en la mayoría de distribuciones de Linux.

Este fallo conocido como PwnKit fue informada por el grupo de investigación Qualys en noviembre de 2021; así mismo, esta vulnerabilidad ha estado existente durante más de 12 años, afectando a todas las versiones de pkexec desde su primera versión en mayo de 2009.

A continuación se mencionan características de esta vulnerabilidad:

[1] Programa raíz de SUID que se instala de forma predeterminada en todas las principales distribuciones de Linux

Nro. Alerta:	EC-2022-15	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	27-enero-2022	**Vulnerabilidad de escalada de privilegios de Polkit - PwnKit**	Versión 1.0

Descripción	Detalle
Fecha de publicación de CVE	25 de enero de 2022.
Vulnerabilidad reportada al proveedor por parte del grupo de investigación	11 de noviembre de 2021.
CVE asociado	CVE-2021- 4034
Puntuación CVSS	8.1

Tabla 1. Características generales de la vulnerabilidad.

IV. VECTOR DE ATAQUE: Local

Este problema no se puede explotar de forma remota; sin embargo, si un atacante puede iniciar sesión como cualquier usuario sin privilegios, puede permitirle obtener privilegios de root.

El fallo ocurre en un componente que controla los privilegios de todo el sistema, el mismo que viene instalado en la mayoría de distribuciones de sistemas operativos UNIX.

A continuación, se describe cómo funciona la vulnerabilidad PwnKit.

```
435 main (int argc, char *argv[])
436 {
...
534   for (n = 1; n < (guint) argc; n++)
535     {
...
568     }
...
610   path = g_strdup (argv[n]);
...
629   if (path[0] != '/')
630     {
...
632       s = g_find_program_in_path (path);
...
639       argv[n] = path = s;
640     }
```

Figura 2.- Ilustración asociada a vulnerabilidad PwnKit.
Fuente: Qualys

- pkexecla main()función procesa los argumentos de la línea de comandos y argcel

número de ARGUMENTOS es cero.

- La función intenta acceder a la lista de argumentos de todos modos y termina tratando de usar un argvvector vacío ARGument de cadenas de argumentos de línea de comandos.
- El resultado que arroja es que la memoria fuera de los límites se lee y escribe, lo que un atacante puede explotar para inyectar una variable de entorno que puede causar que se cargue código arbitrario desde el almacenamiento y que el programa lo ejecute como raíz.

En el siguiente enlace se puede observar la prueba de concepto correspondiente: https://blog.qualys.com/vulnerabilities-threat-research/2022/01/25/pwnkit-local-privilege-escalation-vulnerability-discovered-in-polkits-pkexec-cve-2021-4034

V. IMPACTO

La explotación de esta vulnerabilidad permite que cualquier usuario sin privilegios obtenga privilegios de root en el host vulnerable, teniendo repercusiones sobre la confidencialidad, integridad y disponibilidad; en el caso de que un actor de amenazas combine el problema de escalada de polkit con una vulnerabilidad de ejecución remota de código, el atacante puede obtener la ejecución del código como root sin limitaciones.

VI. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- Revisar las actualizaciones disponibles de las diferentes distribuciones y proceder con la instalación respectiva; por ejemplo Debian https://security-tracker.debian.org/tracker/CVE-2021-4034 , Ubuntu https://ubuntu.com/security/CVE-2021-4034 y RedHat https://access.redhat.com/security/vulnerabilities/RHSB-2022-001
- Una mitigación temporal para los sistemas operativos que aún no han enviado un parche es usar el siguiente comando para quitar a pkexec el bit setuid: **chmod 0755 /usr/bin/pkexec**

VII. REFERENCIAS:

Claburn, T. (26 de 01 de 2022). *The Register*. Obtenido de The Register: https://www.theregister.com/2022/01/26/pwnkit_vulnerability_linuix/

González, G. (26 de 01 de 2022). *Genbeta*. Obtenido de Genbeta:

https://www.genbeta.com/linux/bug-linux-hace-12-anos-permite-obtener-acceso-root-casi-cualquier-distro-han-explotado

Ilascu, I. (25 de 01 de 2022). *Bleepingcomputer*. Obtenido de Bleepingcomputer: https://www.bleepingcomputer.com/news/security/linux-system-service-bug-gives-root-on-all-major-distros-exploit-released/

Jogi, B. (25 de 01 de 2022). *Qualys Comunidad*. Obtenido de Qualys Comunidad: https://blog.qualys.com/vulnerabilities-threat-research/2022/01/25/pwnkit-local-privilege-escalation-vulnerability-discovered-in-polkits-pkexec-cve-2021-4034

Paganini, P. (26 de 01 de 2022). *Securityaffairs*. Obtenido de Securityaffairs: https://securityaffairs.co/wordpress/127199/security/linux-cve-2021-4034-bug.html

Vuldb. (26 de 01 de 2022). *Vuldb*. Obtenido de Vuldb: https://vuldb.com/es/?id.191603

Trustwave. (26 de 01 de 2022). *Trustwave*. Obtenido de Trustwave: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/trustwave-action-response-polkit-privilege-escalation-vulnerability-pwnkit-cve-2021-4034/