Vulnerabilidad PwnKit (CVE-2021-4034)

BCSC-VULNERABILIDAD-PWNKIT

TLP:WHITE

www.basquecybersecurity.eus

Enero 2022

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

SOBRE EL BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Respuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

1. RESUMEN EJECUTIVO

El pasado 25 de enero, el equipo de Qualys hizo pública una vulnerabilidad de corrupción de memoria en *pkexec* de Polkit, un programa root de SUID que se instala de forma predeterminada en las principales distribuciones de Linux. La vulnerabilidad se ha registrado con el CVE-2021-4034, aunque también se le ha denominado *PwnKit* (juego de palabras con el nombre de la aplicación vulnerable Polkit).

Polkit (anteriormente denominado PolicyKit) es un componente utilizado para controlar los privilegios de todo el sistema en sistemas operativos similares a Unix. Proporciona una forma organizada para que los procesos sin privilegios se comuniquen con los procesos con privilegios. Es posible usar polkit para ejecutar comandos con privilegios elevados a través del comando *pkexec* seguido del comando que se pretende ejecutar con permisos de administrador.

La explotación exitosa de esta vulnerabilidad permite que cualquier usuario sin privilegios obtenga privilegios de administrador en el host vulnerable. Los investigadores de seguridad de Qualys han podido verificar de forma independiente la vulnerabilidad, desarrollar un exploit (que no han hecho público) y obtener privilegios completos de root en las instalaciones predeterminadas de Ubuntu, Debian, Fedora y CentOS. A pesar de que Qualys no quiso difundir el código para la explotación de la vulnerabilidad, a las pocas horas de hacer pública la vulnerabilidad se publicó un exploit funcional. No se descarta que otras distribuciones de Linux sean vulnerables y potencialmente explotables. Esta vulnerabilidad se ha mantenido oculta durante más de 12 años ya que afecta a todas las versiones de *pkexec* desde su primera versión en mayo de 2009.

Se trata de una vulnerabilidad fácilmente explotable, dado que reúne varios requisitos que favorecen su explotación. Por un lado, pkexec está instalado de forma predeterminada en las principales distribuciones de Linux, además se trata de un comando vulnerable desde su creación, en mayo de 2009. Por otro lado, cualquier usuario local sin privilegios puede explotar el fallo y obtener privilegios completos de root. Asimismo, hay que tener en cuenta que este fallo es explotable incluso si polkit no se está ejecutando.

2. ANÁLISIS TÉCNICO

La vulnerabilidad CVE-2021-4034 afecta al comando *pkexec* de polkit, un componente para controlar los privilegios de todo el sistema en sistemas operativos similares a Unix. A través del comando *pkexec* un usuario puede ejecutar comandos con privilegios elevados.

La vulnerabilidad se aprovecha del principio de la función *main() de pkexec*, la cual procesa los argumentos de la línea de comandos y busca el programa a ejecutar, si su ruta no es absoluta, en los directorios de la variable de entorno *PATH.* Hay que tener en cuenta que si el número de argumentos de la línea de comandos *argc* es 0 (si la lista de argumentos *argv* que pasamos a *execve()* está vacía, es decir, {NULL}), entonces argv[0] es NULL. Por ejemplo, si la variable de entorno PATH es "PATH=nombre", y el directorio "nombre" existe y contiene un archivo ejecutable llamado "valor", un puntero a la cadena "nombre/valor" se escribe fuera de los límites de *envp[0].* En otras palabras, esta escritura fuera de los límites nos permite reintroducir una variable de entorno "no segura" (por ejemplo, LD_PRELOAD) en pkexec. Estas variables "no seguras" normalmente se eliminan (por ld.so) del entorno de los programas SUID antes de que se ejecute la función main().

Para conseguir una explotación exitosa de este fallo, es necesario tener en cuenta que para imprimir un mensaje de error a stderr, pkexec llama a la función g_printerr() de GLib (biblioteca GNOME). Por ejemplo, las funciones validar_environment_variable() y log_message() llaman a g_printerr(). g_printerr() normalmente imprime mensajes de error UTF-8, pero puede imprimir mensajes en otro juego de caracteres si la variable de entorno Charset no es UTF-8. Para convertir mensajes de UTF-8 a otro charset, g_printerr() llama a la función de glibc iconv_open(). Para convertir mensajes de un conjunto de caracteres a otro, se ejecuta iconv_open() en pequeñas bibliotecas compartidas; normalmente, estos tripletes ("from" charset, "to" juego de caracteres y nombre de la biblioteca) se leen desde un archivo de configuración predeterminado, /usr/lib/gconv/gconv-módulos. Alternativamente, la variable de entorno GCONV_PATH puede obligar a iconv_open() a leer otro archivo de configuración; naturalmente, GCONV_PATH (variable de entorno "no segura" ya que conduce a la ejecución de bibliotecas arbitrarias), es eliminada por ld.so del entorno de los programas SUID.

Desafortunadamente, CVE-2021-4034 permite al atacante volver a introducir GCONV_PATH en entorno de pkexec, y ejecutar una biblioteca propia compartida como administrador.

A pesar de que Qualys no quiso difundir el código para la explotación de la vulnerabilidad, a las pocas horas de hacer pública la vulnerabilidad se publicó un exploit funcional. En el siguiente enlace pueden consultar el código de explotación de Python para CVE-2021-4034.

3. MITIGACIÓN / SOLUCIÓN

Como es habitual, para prevenir esta y otras vulnerabilidades, desde el BCSC se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible.

Dado que todas las versiones de Polkit a partir de 2009 son vulnerables, se recomienda a los administradores que prioricen la aplicación de los parches que los autores de Polkit han hechos públicas en su GitLab.

Todas las distribuciones de Linux tuvieron acceso al parche un par de semanas antes de la divulgación coordinada del 25 de enero por parte de Qualys. Además, Ubuntu ya ha enviado actualizaciones para PolicyKit para abordar la vulnerabilidad en las versiones 14.04 y 16.04 ESM (mantenimiento de seguridad extendido), así como en las versiones más recientes 18.04, 20.04 y 21.04. Los usuarios solo necesitan ejecutar una actualización estándar del sistema y luego reiniciar el dispositivo para que los cambios surtan efecto. Red Hat también entregó una actualización de seguridad para polkit en Workstation y en productos Enterprise para arquitecturas compatibles, así como para soporte de ciclo de vida extendido, TUS y AUS.

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
```

4. REFERENCIAS ADICIONALES

- PwnKit: Local Privilege Escalation Vulnerability Discovered in polkit's pkexec (CVE-2021-4034)
- Qualys Security Advisory
- Linux system service bug gives root on all major distros, exploit released
- Linux distros haunted by Polkit-geist for 12+ years: Bug grants root access to any user
- SUID y SGID: Ejecutar un programa con permisos elevados
- Como establecer la variable PATH
- Python exploit code for CVE-2021-4034 (pwnkit)
- Extended Security Maintenance
- Mantenimiento de Seguridad Extendido
- Red Hat Enterprise Linux Telecommunications Update Service (TUS) Life Cycle
- What is Advanced mission critical Update Support (AUS)?
- Error de Codificacion UTF8

Reportar incidente

Si has detectado algún incidente de ciberseguridad, avísanos para que tomemos las medidas oportunas para evitar su propagación.

900 104 891

incidencias@bcsc.eus

Catálogo de ciberseguridad

¿Necesitas ayuda con tu ciberseguridad o la de tu empresa?