USTIC-ALERT 01/22. Actualización Información PwnKit: Vulnerabilidad en Linux que permite escalada de privilegios.(07/02/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones, continuando con el comunicado publicado en el Espacio de Coordinación TIC (https://ws001.sspa.juntadeandalucia.es/confluence/x/7rPwBQ), alerta de la actualización de información sobre la **vulnerabilidad PwnKit, CVE-2021-4034, de criticidad alta** que **afecta a Linux**.

Como ya es conocido, se trata de una vulnerabilidad de corrupción de memoria en el componente pkexec de PolKit y, que se instala por defecto, en las principales distribuciones de Linux. **Podría permitir a un usuario no privilegiado obtener privilegios de root en un host vulnerable**, aprovechando esta vulnerabilidad en su configuración por defecto. Se le ha asignado el identificador CVE-2021-4034. **Destaca su facilidad de explotación**, ya que es suficiente con manipular las variables de entorno, sin necesidad de eludir protecciones.

Debido a la criticidad alta de esta vulnerabilidad rogamos encarecidamente que se sea especialmente diligente en su resolución. Llamamos vuestra atención sobre la urgencia de aplicar las recomendaciones indicadas y la adopción de medidas para hacer frente a la vulnerabilidad. Para ello, **se ha complementado la información que hay al respecto con la publicación del webinar** celebrado el 7 de febrero **donde** los **compañeros expertos de la USTIC han tratado el funcionamiento, explotación y mitigación de esta vulnerabilidad.**

Recursos Afectados

- La vulnerabilidad se encuentra en el **componente *pkexec* de PolKit**, que está en la configuración por defecto de la **mayoría de distribuciones Linu**x.
- **Todas las versiones de PolKit** desde la primera introducción de *pkexec* son vulnerables; es decir, **desde** la versión **0.113 del año 2009** (*Es posible que existan versiones anteriores a las aquí mencionadas que también se encuentren afectadas. Rogamos su comprobación).*
- **Todas las distribuciones *Major* de Linux, inluyendo Ubuntu, Debian, Fedora y CentOS**, se ven afectadas, ya que PolKit (antes PolicyKit) es un sistema para la gestión de permisos ampliamente usado en Linux.

Recomendaciones Actualizadas (07/02/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones recomienda encarecidamente aplicar los siguientes pasos:

Mitigación

1º. Solución a la vulnerabilidad:

Actualizar todas las distribuciones de Linux que proporcionan un *backport* de la corrección (reinicio necesario):

- Ubuntu 14.04 y 16.04 ESM.
- Ubuntu 18.04, 20.04 y 21.04.
- RedHat en productos Workstation y Enterprise para arquitecturas soportadas, así como para el apoyo al ciclo de vida ampliado, TUS y AUS.
- Debian Stretch, Buster, Bellseye, unstable.

2º. Workaround de la vulnerabilidad:

Como medida de mitigación temporal se puede ejecutar el siguiente comando:

```
chmod 0755 /usr/bin/pkexec
```

Webinar sobre la vulnerabilidad (07/02/2022):

El 7 de febrero se ha celebrado un **webinar** en el que se ha tratado el funcionamiento, explotación y mitigación de esta vulnerabilidad y que ha sido impartido por los compañeros expertos de la USTIC en esta materia. En el siguiente enlace podéis acceder a la grabación de la sesión web Webinar Vulnerabilidad Crítca en Polkit y, a continuación, podéis consultar la documentación vista en el mismo Vulnerabilidad CVE-2021-4034 (PwnKit).pptx

---

En caso de haber detectado la explotación de esta vulnerabilidad :

debe reportar el incidente mediante correo electrónico a sau.cges.sspa@juntadeandalucia.es indic ando en el *Asunto: [Compromiso PwnKit]*

Para cualquier otra duda o consulta al respecto, puede ponerse en contacto con ustic.stic.sspa@juntadeandalucia.es. **Les seguiremos informando.**

Gracias por su atención.

Unidad de Seguridad TIC

Subdirección de Tecnologías de la Información y Comunicaciones

Servicio Andaluz de Salud