BOLETÍN DE ALERTA

Boletín Nro.: 2022-06

Fecha de publicación: 26/1/2022

Tema: Vulnerabilidad de escalamiento de privilegios en Linux.

Sistema operativo afectado:

- Ubuntu 14.04
- Ubuntu 16.04
- Fedora 35
- CentOS 8.5
- Red Hat Enterprise Linux 8
- Red Hat Enterprise Linux 7
- Red Hat Enterprise Linux 7.3 Advanced Update Support
- Red Hat Enterprise Linux 7.4 Advanced Update Support
- Red Hat Enterprise Linux 7.6 Advanced Update Support
- Red Hat Enterprise Linux 7.7 Telco Extended Update Support
- Red Hat Virtualization 4 for Red Hat Enterprise Linux 8
- Red Hat Virtualization 4 for Red Hat Enterprise Linux 7
- Red Hat Enterprise Linux 6 Extended Life-cycle Support
- Red Hat Enterprise Linux 8

Para una lista más detallada de los productos Red Hat afectados, visualizar la lista que se encuentra en la siguiente página.

Descripción:

La vulnerabilidad identificada como CVE-2021-4034 de severidad alta, con una puntuación de 7.8. Esta se debe a un error en el componente vulnerable *PolKit*, el cual permitiría a un usuario sin privilegios poder realizar un escalamiento de estos con el objetivo de obtener privilegios *root*.

Al iniciar un nuevo proceso, el kernel de Linux crea un vector con todos los argumentos de comando (argv), otro vector con variables de entorno (envp) y un valor entero que representa el recuento de argumentos (argc). El kernel de Linux posiciona tanto el vector de argumentos como el vector de variables de entorno de forma contigua en la memoria.

Cómo el primer valor del vector de argumentos contiene el nombre del ejecutable (por ejemplo, pkexec para el ejecutable pkexec), esto implica que los argumentos enviados al proceso por el usuario se colocan después de este valor.

Pkexec no valida el recuento de argumentos, asume que siempre será al menos 1 y que el segundo valor es NULL.

Si un atacante lograra que el vector de argumentos esté vacío, *pkexec* interpretará el contenido de la matriz de entorno como la aplicación que se ejecutará. Un atacante podría aprovechar esto manipulando estas variables para que contengan valores y cargas útiles específicas, lo que le permitiría ejecutarse como un usuario privilegiado sin que se solicite ninguna autenticación.

Si bien, la vulnerabilidad no se puede explotar de forma remota y no permite la ejecución de código arbitrario, el atacante que ya posee un equipo vulnerado podría utilizar esta vulnerabilidad para escalar sus privilegios y lograr los privilegios de administrador (root), como así también por un usuario legitimo sin privilegios administrativos en el sistema.

Si bien la vulnerabilidad fue descubierta y reportada en el 2021, el parche de solución correspondiente se publicó recién hace unos días. Debido a la cantidad de detalles técnicos y exploits funcionales existentes y publicados en internet en la actualidad, dicha vulnerabilidad se torna aún más crítica, arriesgando exponencialmente los sistemas afectados.

Impacto:

El atacante podría explotar esta vulnerabilidad para realizar un escalamiento de privilegios desde un usuario sin privilegios al usuario con mayores privilegios posible (*root*)

Detección:

Se ha desarrollado el siguiente script para verificar si el Linux que posee instalado es vulnerable.

- https://access.redhat.com/sites/default/files/cve-2021-4034--2022-01-25-0936.sh

Solución:

Recomendamos instalar las actualizaciones de seguridad del kernel correspondiente a cada sistema operativo, utilizando el gestor de paquetes (yum, apt, dnf).

Para los usuarios de Red Hat se recomienda seguir la siguiente guía:

- RHSB-2022-001 Polkit Privilege Escalation - (CVE-2021-4034) - Red Hat Customer Portal

Información adicional:

- https://access.redhat.com/security/vulnerabilities/RHSB-2022-001
- https://security-tracker.debian.org/tracker/CVE-2021-4034
- https://ubuntu.com/security/CVE-2021-4034