Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Fallo de seguridad en el Kernel de Linux (19158 lectures)

Per **Carles Pina i Estany**, ***cpina*** (http://pinux.info)

Creado el 19/03/2003 11:21 modificado el 19/03/2003 11:21

En casi todos los kernels 2.2.x y en los 2.4.x hasta la fecha (2.4.20 y el último 2.4.21-pre5), si no hay el parche concreto del fallo de seguridad hay un error que provoca escalada de privilegios (pasar de usuario a root) de forma directa y rápida. El fallo es local (se necesita cuenta shell en la máquina). Actualización rápida necesaria.

Notas rápidas:

- Leyendo este e-mail[1] de Alan Cox vemos que hay un error en el Kernel de Linux, 2.2.x y 2.4.x hasta la fecha (2.4.20 y 2.4.21-pre5).
- Parece que si tenemos el parche de grsecurity no nos afecta.
- Si hacemos *"echo /dev/null" > /proc/sys/kernel/modprobe"* desactivamos los módulos (Linux no sabrá como cargarlos) y el exploit que corre por aquí tampoco nos afecta (al menos por lo que he podido comprobar). Claro que si el núcleo necesita cargar un módulo no lo podrá hacer.
- Si tenemos un Kernel SIN soporte de módulos (sin posibilidad de tener módulos) tampoco nos afecta (por lo que he comprobado)
- El fallo es local, necesitamos una cuenta en el sistema para poderlo explotar. Si es un ordenador en el cual nadie puede entrar mediante una shell (o parecidos) no hay problema (aunque mejor lo arreglamos, no?).

Ver que las tres soluciones, excepto el parche aplicado al Kernel pueden no ser totalmente 100% fiables, así que mejor aplicamos el parche[2] (parche tambien disponible en el comentario[1] de Alan Cox)

En Slashdot[3] tambien se comenta.[4]

El error parece ser que cuando el Kernel hace un proceso hijo, nos podemos asociar en él mediante ptrace, con permisos de root..

Lista de enlaces de este artículo:

1. http://www.spinics.net/lists/kernel/msg162986.html
2. http://www.hardrock.org/kernel/2.4.20/linux-2.4.20-ptrace.patch
3. http://www.slashdot.org
4. http://slashdot.org/articles/03/03/18/199208.shtml?tid=106&a

---

E-mail del autor: carles _ARROBA_ pinux.info