BOLETÍN DE ALERTA

Boletín Nro.: 2022-17

Fecha de publicación: 10/03/2022

Tema: Múltiples vulnerabilidades en kernel de Linux.

Versiones afectadas:

- Kernel de Linux de 5.4 a 5.6.10.

Descripción:

En las últimas semanas hemos publicado 3 (tres) noticias sobre vulnerabilidades de severidad alta, que afectan al kernel de Linux. Estas vulnerabilidades permitirían a un atacante realizar escalamiento de privilegios y ataques de denegación de servicio (DoS), las mismas se resumen a continuación:

- CVE-2022-0492 de severidad alta, sin puntuación asignada aún. Esta se debe a una falla lógica en la función *kernel/cgroup/cgroup-v1.c* de la funcionalidad de grupos de control (*cgroups*) del kernel de Linux. Esto permitiría a un atacante realizar un escalamiento de privilegios al usuario administrador (root).

- CVE-2022-0847 de severidad alta, con una puntuación de 7.8. Esta se debe a la falta de inicialización adecuada de la estructura *pipe_buffer* en las funciones *copy_page_to_iter_pipe y push_pipe* encontradas para el miembro "*flags*" de una nueva estructura de *pipe buffer* del kernel de Linux. La explotación de esta vulnerabilidad permitiría que un usuario local sin privilegios utilice esta falla para sobrescribir datos en archivos arbitrarios de solo lectura, logrando obtener un escalamiento de privilegios.

- CVE-2022-25636 de severidad alta, con una puntuación asignada de 7.8. Esta vulnerabilidad se debe a un error en la función *nft_fwd_dup_netdev_offload* del componente *nf_dup_netdev.c*. Esto permitiría a un atacante con privilegios bajos realizar un escalamiento de privilegios o realizar un ataque de denegación de servicio (DoS) en el sistema afectado.

Impacto:

La explotación de estas vulnerabilidades permitiría a un atacante realizar escalamiento de privilegios y ataque de denegación de servicio (DoS).

Detección:

Verificar si se posee instalada una de las versiones del kernel afectado:

- Kernel de Linux de 5.4 a la 5.6.10.

Así mismo, RedHat ha desarrollado un script de detección para determinar si un sistema es actualmente vulnerable.

Adicionalmente el siguiente enlace enumera las configuraciones de contenedores vulnerables y proporciona instrucciones sobre cómo probar si un entorno de contenedor es vulnerable:

- https://unit42.paloaltonetworks.com/cve-2022-0492-cgroups/#Am-I-Affected

Solución:

CVE-2022-25636:

Se recomienda actualizar a la versión más reciente del kernel proveída por Linux:

- https://www.kernel.org/

CVE-2022-0847:

Se recomienda descargar y actualizar la versión más reciente del kernel proveída por Linux:

- https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=9d2231c5d74e13b2a0546fee6737ee4446017903

CVE-2022-0492:

Se recomienda actualizar a la última versión del kernel de Linux (de su respectiva distribución). Para los casos en los que no sea posible la actualización, recomendamos implementar una de las mitigaciones expuestas en los siguientes enlaces para protección contra contenedores maliciosos:

AppArmor o SELinux:

- https://kubernetes.io/docs/tutorials/security/apparmor/

Seccomp:

- https://kubernetes.io/docs/tutorials/security/seccomp/

Adicionalmente, para protegerse contra los procesos de host malintencionados que intenten escalamiento de privilegios (en escenarios en los que la actualización no es posible) recomendamos:

1. Deshabilitar los espacios de nombres de usuario sin privilegios mediante el siguiente comando:

sudo sysctl -w kernel.unprivileged_userns_clone=0

Nota: tener en cuenta que algunos servicios como *Podman* se basan en espacios de nombres de usuario sin privilegios y es posible que no funcionen según lo previsto.

2. Evitar que los procesos establezcan el *release_agent* en cualquier montaje de *cgroup* mediante el siguiente script:

```
#!/bin/bash
set -e
mask_dir=/var/lib/cve_2022_0492_release_agent_mask
cgroup_dir=/sys/fs/cgroup
if [ ! -z "$1" ]; then cgroup_dir=$1 ; fi
        echo "[+] Creating mask at $mask_dir/mask"
sudo mkdir -p $mask_dir
sudo mount -t tmpfs release_agent_mask $mask_dir
sudo touch $mask_dir/mask
sudo mount -o remount,ro $mask_dir
for release_agent in $(find $cgroup_dir -name 'release_agent') ;do
        echo "[+] Mounting read-only mask over $release_agent"
        sudo mount --bind $mask_dir/mask $release_agent
done
```

Finalmente, recomendamos a los usuarios de *Prisma Cloud* que revisen *Compute/Monitor/Compliance* y determinen si alguno de sus contenedores se ejecuta sin Seccomp. Los usuarios también pueden optar por bloquear los contenedores que se ejecutan sin Seccomp.

Información adicional:

- https://nvd.nist.gov/vuln/detail/CVE-2022-0492
- https://access.redhat.com/security/cve/cve-2022-0847
- https://nvd.nist.gov/vuln/detail/CVE-2022-25636

- https://cert.gov.py/noticias/vulnerabilidad-de-escalamiento-de-privilegios-en-linux-1
- https://cert.gov.py/noticias/vulnerabilidad-de-escalamiento-de-privilegios-en-linux-2
- https://cert.gov.py/noticias/vulnerabilidad-de-escalamiento-de-privilegios-en-kernel-de-linux