Surgieron detalles sobre una vulnerabilidad de alta gravedad ya parcheada en el kernel de Linux que podría ser objeto de abuso para escapar de un contenedor con el fin de ejecutar comandos arbitrarios en el host del contenedor.

La deficiencia reside en una característica del kernel de Linux llamada grupos de control, también conocida como cgroups versión 1 (v1), que permite que los procesos se organicen en grupos jerárquicos, lo que permite limitar y monitorear el uso de recursos como CPU, memoria, E/S de disco y red.

Rastreada como CVE-2022-0492, con puntuación CVSS de 7.0, la vulnerabilidad se refiere a un caso de escalada de privilegios en la funcionalidad release_agent de cgroups v1, un script que se ejecuta luego de la finalización de cualquier proceso en cgroup.

> *«El problema se destaca como una de las escaladas de privilegios de Linux más simples descubiertas en los últimos tiempos: el kernel de Linux expuso por error una operación privilegiada a usuarios sin privilegios»,* dijo el investigador de Unit 42, Yuval Avrahami.

La página de manual para cgroups explica su función de la siguiente forma:

> *«La invocación o no del programa release_agent cuando un cgroup en particular se vacía se determina por el valor en el archivo notificar_on_release en el directorio cgroup correspondiente. Si este archivo contiene el valor 0, entonces no se invoca el programa release_agent. Si contiene el valor 1, se invoca el programa release_agent. El valor predeterminado para este archivo en el cgroup raíz es 0».*

Específicamente, el equipo de inteligencia de amenazas de Palo Alto Networks, dijo que el error es consecuencia de una falta de verificación acerca del proceso que configura el archivo release_agent, para conocer que tenga privilegios administrativos, lo que lo

preparaba para una posible explotación.

Dicho de otra forma, si un atacante sobrescribe este archivo release_agent, el núcleo puede verse obligado a llamar a un binario arbitrario configurado en el agente de versión con los permisos más altos posibles, un escenario que podría permitir efectivamente una toma de control completa de la máquina.

Sin embargo, solo los procesos con privilegios «raíz» pueden escribir en el archivo, lo que significa que la vulnerabilidad solo permite que los procesos raíz aumenten los privilegios.

> *«A primera vista, una vulnerabilidad de escalada de privilegios que solo puede ser explotada por el usuario raíz puede parecer extraña. Ejecutar como root no significa necesariamente control total sobre la máquina: hay un área gris entre el usuario root y los privilegios completos que incluye capacidades, espacios de nombres y contenedores. En estos escenarios donde un proceso root no tiene control total sobre la máquina, CVE-2022-0492 se convierte en una vulnerabilidad grave»,* dijo Avrahami.

Aunque los contenedores que se ejecutan con AppArmor o SELinux están protegidos contra la falla, se recomienda a los usuarios que apliquen los parches en vista del hecho de que otros procesos de host maliciosos podrían abusar de ellos para elevar los privilegios.

Esto está lejos de ser la primera vez que release_agent resurge como un vector de ataque. En julio de 2019, el investigador de Google Project Zero, Felix Wilhelm, demostró un exploit de prueba de concepto (PoC) *«rápido y sucio»* que aprovecha la función para salir de los contenedores privilegiados de Kubernetes y Docker.

Después, en noviembre de 2021, la empresa de seguridad nativa de la nube, Aqua, reveló detalles de una campaña de minería de criptomonedas que usó exactamente la misma técnica de escape de contenedores para colocar el minero de monedas XMRig en hosts infectados, lo que la convierte en la primera instancia registrada de explotación en el mundo

real.

> *«CVE-2022-0492 marca otra vulnerabilidad de Linux que puede explotarse para el escape de contenedores. Afortunadamente, los entornos que siguen las mejores prácticas están protegidos de esta vulnerabilidad. Los entornos con controles de seguridad laxos que alojan contenedores no confiables o expuestos públicamente están, como era de esperar, en alto riesgo»*, agregó Avrahami.