Se han revelado múltiples vulnerabilidades de seguridad en el sistema de implementación y empaquetado del software Snap de Canonical, la más crítica de las cuales, puede explotarse para escalar privilegios y obtener privilegios de root.

Los complementos son paquetes de aplicaciones autónomos que están diseñados para funcionar en sistemas operativos que usan el kernel de Linux y se pueden instalar con una herramienta llamada snapd.

La vulnerabilidad, rastreada como CVE-2021-44731, se refiere a una falla de escalada de privilegios en la función snap-confine, un programa utilizado internamente por snapd para construir el entorno de ejecución para aplicaciones snap. La deficiencia tiene una calificación de 7.8 en el sistema de puntuación CVSS.

> *«La explotación exitosa de esta vulnerabilidad permite que cualquier usuario sin privilegios obtenga los privilegios de root en el host vulnerable. Se puede abusar de la vulnerabilidad para obtener privilegios de root completos en instalaciones predeterminadas de Ubuntu»,* dijo Bharat Jogi, director de investigación de vulnerabilidades y amenazas en Qualys.

Red Hat, en un aviso independiente, describió el problema como una *«condición de carrera»* en el componente de confinamiento rápido.

> *«Existe una condición de carrera en el confinamiento instantáneo cuando se prepara un espacio de nombres de montaje privado para un complemento. Esto podría permitir que un atacante local obtenga privilegios de root montando sus propios contenidos dentro del espacio de nombres de montaje privado del complemento y haciendo que snap-confine ejecute código arbitrario y, por lo tanto, aumente la escalada de privilegios»,* dijo la compañía.

Además, la empresa de seguridad cibernética descubrió otras seis vulnerabilidades:

- CVE-2021-3995: Desmontaje no autorizado en libmount de util-linux
- CVE-2021-3996: Desmontaje no autorizado en libmount de util-linux
- CVE-2021-3997: Recursividad descontrolada en los archivos systemd-tmpfiles de systemd
- CVE-2021-3998: Valor de retorno inesperado de realpath() de glibc
- CVE-2021-3999: Desbordamiento/subdesbordamiento de búfer fuera de uno en getcwd() de glibc
- CVE-2021-44730: Ataque de enlace duro en sc_open_snapd_tool() de snap-confine

La vulnerabilidad se informó al equipo de seguridad de Ubuntu el 27 de octubre de 2021, después de esto, se lanzaron parches el 17 de febrero como un proceso de divulgación coordinado.

Qualys también dijo que, si bien la falla no se puede explotar remotamente, un atacante que haya iniciado sesión como un usuario sin privilegios puede *«rápidamente»* explotar la falla para obtener permisos de root, lo que requiere que los parches se apliquen lo antes posible para mitigar las amenazas potenciales.