Se han dado a conocer los detalles de una vulnerabilidad de seguridad de ocho años en el kernel de Linux que, según los investigadores, es *«tan desagradable como Dirty Pipe».*

Nombrada como DirtyCred por un grupo de académicos de la Universidad Northwestern, la vulnerabilidad de seguridad explota una falla previamente desconocida (CVE-2022-2588) para escalar los privilegios al nivel máximo.

> *«DirtyCred es un concepto de explotación del kernel que intercambia las credenciales del kernel sin privilegios con las privilegiadas para escalar los privilegios. En lugar de sobrescribir los campos de datos críticos en el montón del kernel, DirtyCred abusa del mecanismo de reutilización de la memoria del montón para obtener privilegios»,* dijeron los investigadores Zhenpeng Lin, Yuhang Wu y Xinyu Xing.

Esto implica tres pasos:

- Liberar una credencial sin privilegios en uso con la vulnerabilidad
- Asignar credenciales privilegiadas en la ranura de memoria liberada activando un proceso de espacio de usuario privilegiado como su, mount o ssh
- Operar como un usuario privilegiado

Este método de explotación, según los investigadores, lleva la Dirty Pipe al siguiente nivel, haciéndola más general y potente de una forma que podría funcionar en cualquier versión del kernel afectado.

> *«Primero, en lugar de vincularse a una vulnerabilidad específica, este método de explotación permite que cualquier vulnerabilidad con capacidad doble libre*

> *demuestre una capacidad similar a la de una Dirty Pipe»,* dijeron los investigadores.

> *«En segundo lugar, si bien es como la Dirty Pipe que podría eludir todas las protecciones del kernel, nuestro método de explotación podría incluso demostrar la capacidad de escapar activamente del contenedor de la que Dirty Pipe no es capaz».*

Dirty Pipe, rastreada como CVE-2022-0847 (puntaje CVSS: 7.8) y que afecta a las versiones del kernel de Linux a partir de la 5.8, se refiere a una vulnerabilidad de seguridad en el subsistema de tuberías que permite que los procesos sin privilegios escriban en archivos legibles arbitrarios, lo que lleva a una escalada de privilegios.

La vulnerabilidad explotable se llamó así por la vulnerabilidad Dirty Cow, descubierta en 2016 en función de sus similitudes.

Debido a que los objetos se aíslan en función de su tipo y no de sus privilegios, los investigadores recomiendan aislar las credenciales privilegiadas de las no privilegiadas utilizando la memoria virtual para evitar ataques entre cachés.