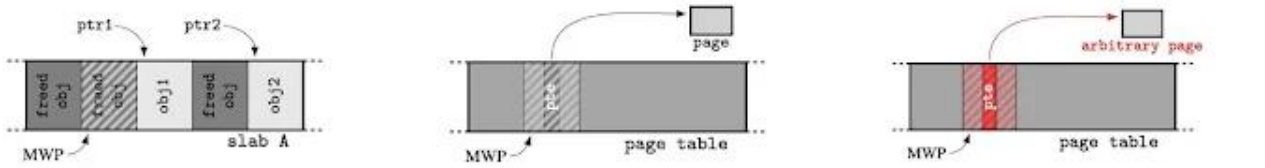
Los investigadores en ciberseguridad han revelado una nueva técnica de explotación del núcleo de Linux, denominada SLUBStick, que podría ser utilizada para escalar una vulnerabilidad de montón limitada a una primitiva de lectura y escritura de memoria arbitraria.

> *«Inicialmente, explota un canal lateral de temporización del asignador para realizar un ataque de caché cruzada de manera confiable. Concretamente, la explotación de la filtración del canal lateral eleva la tasa de éxito a más del 99% para cachés genéricas de uso frecuente»,* mencionó un grupo de académicos de la Universidad Tecnológica de Graz [PDF].

Las vulnerabilidades de seguridad de memoria que afectan al núcleo de Linux tienen capacidades limitadas y son mucho más difíciles de explotar debido a características de seguridad como la Prevención de Acceso en Modo Supervisor (SMAP), la Aleatorización del Espacio de Direcciones del Núcleo (KASLR) y la integridad del flujo de control del núcleo (kCFI).

Aunque se han desarrollado ataques de caché cruzada de software como una forma de contrarrestar las estrategias de endurecimiento del núcleo, como la separación de montón de grano grueso, los estudios han demostrado que los métodos existentes solo tienen una tasa de éxito del 40%.

SLUBStick se ha demostrado en las versiones 5.19 y 6.2 del núcleo de Linux utilizando nueve fallos de seguridad (por ejemplo, doble liberación, uso después de liberación y escritura fuera de límites) descubiertos entre 2021 y 2023, lo que lleva a la escalada de privilegios a root sin autenticación y escapes de contenedores.



(a) *Stage 1* deallocates objects `obj1` and `obj2` to trigger the recycling process of `slab A`'s memory chunk, with a Memory Write Primitive (MWP) referring to it.

(b) *Stage 2* reclaims the recycled memory chunk for a page table used by the userspace address translation, containing one entry, `pte`, which refers to the user-accessible `page`.

(c) *Stage 3* triggers the MWP to manipulate the page table entry `pte`. This manipulated entry indexes then the `arbitrary page`, allowing it to be overwritten from the userspace.

Figure 5: High-level overview of SLUBStick subdivided into three stages exploiting an MWP.

La idea central detrás del enfoque es ofrecer la capacidad de modificar los datos del núcleo y obtener una primitiva de lectura y escritura arbitraria de memoria de una manera que supere de manera confiable las defensas existentes como KASLR.

Sin embargo, para que esto funcione, el modelo de amenaza asume la presencia de una vulnerabilidad de montón en el núcleo de Linux y que un usuario sin privilegios tenga capacidades de ejecución de código.

> *«SLUBStick explota sistemas más recientes, incluyendo las versiones 5.19 y 6.2, para una amplia variedad de vulnerabilidades de montón»,* comentaron los investigadores.