Investigadores de seguridad cibernética descubrieron dos ataques distintos que podrían explotarse contra los procesadores Intel modernos para filtrar información confidencial sobre los entornos de ejecución de confianza (TEE) de la CPU.

Llamado SGAxe, el primero de los defectos es una evolución del ataque CacheOut previamente descubierto (CVE-2020-0549) a inicios del año, que permite a un atacante recuperar el contenido del caché L1 de la CPU.

> *«Al utilizar el ataque extendido contra los enclaves SGX arquitectónicos firmados y provistos por Intel, recuperamos la clave de certificación secreta utilizada para probar de forma criptográfica la autenticidad de los enclaves a través de la red, lo que nos permite pasar enclaves falsos como genuinos»,* dijo el grupo de académicos de la Universidad de Michigan.

La segunda línea de ataque, denominada CrossTalk, por investigadores de la Universidad VU de Amsterdam, permite la ejecución de código controlado por el atacante en un núcleo de CPU para apuntar a enclaves SGX que se ejecutan en un núcleo completamente diferente y determinar las claves privadas del enclave.

Un TEE, como las Extensiones de Protección de Software de Intel (SGX), se refiere a un enclave seguro, un área dentro de un procesador que garantiza la confidencialidad e integridad del código y los datos. Ofrece protecciones contra la modificación de software y datos confidenciales por parte de actores maliciosos que pueden haber entrado en la máquina de destino.

## SGAxe: Extracción de datos confidenciales de enclaves SGX

SGAxe se basa en el ataque de ejecución especulativo CacheOut para robar datos SGX. Según los investigadores, si bien Intel tomó medidas para abordar los ataques de canal

lateral contra SGX a través de varias actualizaciones de microcódigo y nuevas arquitecturas, las mitigaciones resultaron ineficaces.

La vulnerabilidad, como resultado permite un ataque de ejecución transitoria que puede recuperar claves criptográficas SGX de una máquina Intel totalmente actualizada, en la que confía el servidor de certificación de Intel.

> *«En pocas palabras, usamos CacheOut para recuperar las claves de sellado desde el espacio de direcciones del enclave de citas de producción de Intel. Finalmente, utilizamos las claves de sellado recuperadas para descifrar el almacenamiento a largo plazo del enclave de citas, obteniendo las claves de certificación EPID de las máquinas»*, dijeron los investigadores.

Al romper esta confianza, SGAxe facilita a un atacante la creación de un enclave corrupto que pasa el mecanismo de certificación de Intel, lo que resulta en la pérdida de las garantías de seguridad.

> *«Con las claves de certificación de producción de la máquina comprometidas, los secretos proporcionados por el servidor pueden ser leídos inmediatamente por la aplicación de host no confiable del cliente, mientras que no se puede confiar en la exactitud de todas las salidas supuestamente producidas por enclaves que se ejecutan en el cliente. Esto hace que las aplicaciones DRM basadas en SGX sean inútiles, ya que cualquier secreto provisto se pude recuperar trivialmente»*, agregaron los investigadores.

Aunque Intel emitió correcciones para CacheOut en enero a través de una actualización de microcódigo para proveedores OEM y posteriormente a través de actualizaciones de BIOS

para usuarios finales, las mitigaciones para SGAex requerirán parchear la causa raíz detrás de CacheOut (también conocido como L1D Eviction Sampling).

> *«Es importante tener en cuenta que SGAex se basa en CVE-2020-0549, que ha sido mitigado en microcódigo (confirmado por los investigadores en su documento actualizado CacheOut) y distribuido al ecosistema»,* dijo Intel en un aviso de seguridad.

Intel también realizará una recuperación de Trusted Compute Base (TCB) para invalidar todas las claves de certificación previamente firmadas.

> *«Este proceso garantizará que su sistema se encuentre en un estado seguro de modo que pueda volver a utilizar la certificación remota»,* dijeron los investigadores.

## CrossTalk: Fuga de información en núcleos de CPU

CrossTalk (CVE-2020-0543), el segundo exploit SGX, es lo que la Universidad VU llama un ataque MDS (Microarchitectural Data Sampling). Aprovecha un búfer de *«puesta en escena»* que se puede leer en todos los núcleos de la CPU para montar ataques de ejecución transitorios en los núcleos y extraer la clave privada completa de ECDSA de un enclave seguro que se ejecuta en un núcleo de CPU separado.

> *«El almacenamiento intermedio retiene los resultados de instrucciones de ejecución realizadas previamente en todos los núcleos de CPU. Por ejemplo, contiene los números aleatorios devueltos por el DRNG de hardware externo, los hashes de estado de bootguard y otros datos confidenciales»*, agregaron los investigadores.

CrossTalk funciona leyendo el búfer de ensayo durante la ejecución transitoria para filtrar datos confidenciales a los que acceden las instrucciones de víctimas ejecutadas previamente.

El hecho de que el búfer retiene la salida de las instrucciones RDRAND y RDSEED, hace posible que una parte no autorizada rastree los números aleatorios generados y, por lo tanto, compromete las operaciones criptográficas que sustentan el enclave SGX, incluido en el proceso de certificación remota ya mencionado.

Con las CPU Intel lanzadas de 2015 a 2019, contando las CPU Xeon E3 y E, susceptibles a los ataques, los investigadores de la Universidad VU dijeron que compartieron con Intel una prueba de concepto que demuestra la fuga del contenido del almacenamiento intermedio provisional en septiembre de 2018, seguido de un PoC implementando la filtración RDRAND/RDSEED entre núcleos en julio de 2019.

> *«Las mitigaciones contra los ataques de ejecución transitorios existentes son en gran medida ineficaces. La mayoría de las mitigaciones actuales dependen del aislamiento espacial en los límites que ya no son aplicables debido a la naturaleza del núcleo cruzado de estos ataques. Las nuevas actualizaciones de microcódigo que bloquean todo el bus de memoria para estas instrucciones pueden mitigar los ataques, pero solo si hay problemas similares que aún no se encuentran».*

Como respuesta, Intel abordó la falla en una actualización de microcódigo distribuida a los proveedores de software ayer después de un período de divulgación prolongado de 21 meses debido a la dificultad de implementar una solución.

La compañía recomendó a los usuarios de los procesadores afectados que actualicen a la última versión del firmware proporcionada por los fabricantes del sistema para abordar el problema.