Un equipo de investigadores de seguridad cibernética demostró una técnica nueva para secuestrar los Intel SGX, un espacio de confianza aislado por hardware en las CPU modernas de Intel, que encripta datos extremadamente sensibles para protegerlos de los atacantes aún cuando un sistema se ve comprometido.

Plundervolt es el nombre que se le dio al ataque, identificado como CVE-2019-11157, se basa en el hecho de que los procesadores modernos permiten que la frecuencia y el voltaje se ajusten cuando sea necesario, lo que según los investigadores, puede modificarse de forma controlada para inducir errores en la memoria al voltear los bits.

Bit Flip es un fenómeno ampliamente conocido por el ataque Rowhammer, en el que los atacantes secuestran celdas de memoria vulnerables al cambiar su valor de 1 a 0, o viceversa, modificando la carga eléctrica de las celdas de memorias vecinas.

Sin embargo, ya que la memoria del enclave de Software Guard Extensions (SGX) está cifrada, el ataque Plundervolt aprovecha la misma idea de voltear bits al inyectar fallas en la CPU antes de que se escriban en la memoria.

Plundervolt es más parecido a ataques de ejecución especulativos como Foreshadow y Spectre, pero mientras Foreshadow y Spectre atacan la confidencialidad de la memoria de enclave SGX al permitir que los atacantes lean datos del enclave seguro, Plundervolt ataca la integridad SGX para lograr lo mismo.

Para esto, Plundervolt depende de una segunda técnica llamada CLKSCREW, un vector de ataque previamente documentado que explota la administración de energía de la CPU para violar los mecanismos de seguridad del hardware y tomar el control de un sistema operativo.

> *«Mostramos que un adversario privilegiado puede inyectar fallas en los cálculos de enclave protegido. Fundamentalmente, dado que las fallas ocurren dentro del paquete del procesador, es decir, antes de que los resultados se envíen a la memoria, la protección de integridad de memoria de Intel SGX no puede defenderse*

> *de nuestros ataques»,* dijeron los investigadores.

Como se ve en los videos, al aumentar o disminuir de forma sutil el voltaje entregado a un CPU objetivo, un atacante puede desencadenar fallas computacionales en los algoritmos de cifrado utilizados por los enclaves SGX, lo que permite a los hackers descifrar fácilmente los datos SGX.

> *«Demostramos la efectividad de nuestros ataques al inyectar fallas en las implementaciones RSA-CRT y AES-NI de Intel, que se ejecutan en un enclave SGX, y reconstuimos claves criptográficas completas con esfuerzos computaciones insignificantes»,* agregaron los investigadores.
>
> *«Dado un par de textos cifrados correctos y defectuosos en el mismo texto sin formato, este ataque puede recuperar la clave AES completa de 128 bits con una complejidad computacional de solo 232 + 256 cifrados en promedio. Hemos ejecutado este ataque en la práctica, y solo tomó un par de minutos extraer la clave AES completa del enclave, incluidas las fases de inyección de fallas y cálculo clave».*

El ataque Plundervolt, que afecta a todos los procesadores Intel Core habilitados con SGX a partir de la generación Skylate, fue descubierto e informado en privado a Intel en junio de 2019 por un equipo de seis investigadores europeos de la Universidad de Birmingham, la Universidad Tecnológica de Graz y KU Leuven.

En respuesta a los hallazgos de los investigadores, Intel lanzó ayer microcódigo y actualizaciones de BIOS para abordar Plundervolt bloqueando el voltaje a la configuración predeterminada, junto con otras 13 vulnerabilidades de gravedad alta y media.

> *«Intel ha trabajado con proveedores de sistemas para desarrollar una actualización*

> *de microcódigo que mitigue el problema al bloquear el voltaje a la configuración predeterminada. No tenemos conocimiento de que ninguno de estos problemas se utilicen en la naturaleza, pero como siempre, recomendamos instalar actualizaciones de seguridad lo antes posible»,* dice Intel.

Los modelos de CPU afectados por el ataque Pludervolt son:

- Procesadores Intel Core de 6a, 7a, 8a y 9a generación
- Procesador Intel Xeon E3 v5 y v6
- Procesador Intel Xeon E-2100 y familias E-2200

Lista completa de productos afectados aquí.

Además de lanzar una prueba de concepto (PoC) en GitHub, el equipo de investigadores también lanzó un sitio web dedicado con preguntas frecuentes y un documento técnico titulado *Plundervolt: Ataques de inyección de fallas basados en software contra Intel SGX.*