| Centro Nacional de Seguridad Digital | **ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°187** | **Fecha: 10-08-2023** |
|---|---|---|
| | | **Página: 4 de 12** |

| | | | |
|---|---|---|---|
| Componente que reporta | **CENTRO NACIONAL DE SEGURIDAD DIGITAL** | | |
| Nombre de la alerta | Ataque Downfall permite la extracción de contraseñas y claves de cifrado del microprocesador Intel | | |
| Tipo de Ataque | Robo de información | Abreviatura | RobInfo |
| Medios de propagación | Red, Internet, Redes sociales | | |
| Código de familia | K | Código de Sub familia | K01 |
| Clasificación temática familia | Uso inapropiado de recursos | | |

Descripción

1. **ANTECEDENTES:**


Una variedad de procesadores Intel Core y los dispositivos que los utilizan son vulnerables a "Downfall", una nueva clase de ataques posible gracias a CVE-2022-40982, que permite a los atacantes acceder y robar datos confidenciales como contraseñas, claves de cifrado, correos electrónicos, datos privados, y datos de otros usuarios, en la misma PC personal o en la nube.

2. **DETALLES:**

El investigador de seguridad cibernética Daniel Moghimi en Google elaboró recientemente un ataque de CPU 'Downfall' que permite a los atacantes extraer datos de los chips Intel compartidos por los usuarios.

Los investigadores de ciberseguridad rastrearon esta vulnerabilidad como CVE-2022-40982, la cual afecta a los chips desde la 6ta generación Skylake hasta la 11va generación Tiger Lake de Intel con problemas de canal lateral de ejecución transitoria.

"[CVE-2022-40982] es causado por funciones de optimización de memoria en los procesadores Intel que revelan involuntariamente los registros internos del hardware al software. Esto permite que el software no confiable acceda a los datos almacenados por otros programas, que normalmente no deberían ser accesibles", explicó Daniel Moghimi, científico investigador de Google.

En un escenario de ataque hipotético, una aplicación maliciosa instalada en un dispositivo podría armar el método para robar información confidencial como contraseñas y claves de cifrado, lo que socavaría de manera efectiva las protecciones de Intel Software Guard eXtensions (SGX).

El problema tiene sus raíces en las funciones de optimización de memoria introducidas por Intel en sus procesadores, específicamente aquellos con conjuntos de instrucciones AVX2 y AVX-512, lo que hace que el software no confiable supere las barreras de aislamiento y acceda a los datos almacenados por otros programas.

Esto, a su vez, se logra mediante dos técnicas de ataque de ejecución transitoria denominadas Gather Data Sampling (GDS) y Gather Value Injection (GVI), la última de las cuales combina GDS con Load Value Injection (LVI).

"[Downfall y Zenbleed] permiten que un atacante viole el límite de software y hardware establecido en los procesadores modernos", señalaron Tavis Ormandy y Moghimi. "Esto podría permitir que un atacante acceda a datos en registros de hardware internos que contienen información que pertenece a otros usuarios del sistema, tanto en diferentes máquinas virtuales como en diferentes procesos".

3. **RECOMENDACIONES:**

- Instalar el firmware más reciente del fabricante de su sistema.
- Actualizar el microcódigo flash de la plataforma a través de la tabla de interfaz de firmware, ya que la nueva actualización del microcódigo evita que los atacantes observen los resultados de las instrucciones de recopilación.

| | |
|---|---|
| Fuente de Información: | • hxxps://gbhackers.com/downfall-attack/#google_vignette<br>• hxxps://www.helpnetsecurity.com/2023/08/09/downfall-cve-2022-40982/<br>• hxxps://unaaldia.hispasec.com/2023/08/downfall-el-nuevo-ataque-de-fuga-de-datos-en-las-cpu-que-afecta-a-los-procesadores-intel.html<br>• hxxps://thehackernews.com/2023/08/collidepower-downfall-and-inception-new.html<br>• hxxps://www.redeszone.net/noticias/seguridad/procesadores-intel-downfall-robo-datos/ |