Un investigador de seguridad cibernética descubrió un conjunto de siete nuevas vulnerabilidades de hardware que no pueden ser reparadas y afectan a todos los equipos de escritorio y portátiles vendidos en los últimos 9 años, con Thunderbolt o puertos USB-C compatibles con Thunderbolt.

ThunderSpy, como se nombró colectivamente a las vulnerabilidades, pueden explotarse en 9 escenarios realistas de ataques, principalmente para robar datos o leer y escribir toda la memoria del sistema de una computadora bloqueada o inactiva, aún cuando las unidades están protegidas con cifrado de disco completo.

Björn Ruytenberg de la Universidad Tecnológica de Eindhoven, afirma que el ataque ThunderSpy *«puede requerir abrir la carcasa de una computadora portátil objetivo con un destornillados, pero no deja rastro de intrusión y se puede quitar en solo unos minutos».*

En otras palabras, la falla no está vinculada a la actividad de la red ni a ningún componente relacionado, por lo que no se puede explotar remotamente.

> *«ThunderSpy funciona incluso si se siguen las mejores prácticas de seguridad al bloquear o suspender su computadora al salir brevemente, y si el administrador del sistema configuró el dispositivo con arranque seguro, contraseñas seguras de BIOS y sistema operativo, ya habilitado el cifrado de disco completo»*, dijo el investigador.

Además de cualquier computadora con sistema operativo Windows o Linux, las MacBook de Apple con tecnología Thunderbolt, excepto las versiones de retina, vendidas desde 2011, también son vulnerables al ataque ThunderSpy.

La lista de siete vulnerabilidades de ThunderSpy afecta a las versiones 1, 2 y 3 de Thunderbolt, y puede explotarse para crear identidades arbitrarias de dispositivos Thunderbolt, clonar dispositivos Thunderbolt autorizados por el usuario, y finalmente, obtener conectividad PCIe para realizar ataques DMA.

- Esquemas de verificación de firmware inadecuados
- Esquema de autenticación de dispositivo débil
- Uso de metadatos de dispositivos no autenticados
- Ataque de degradación utilizando compatibilidad con versiones anteriores
- Uso de configuraciones de controlador no autenticadas
- Deficiencias de la interfaz flash SPI
- Falta de seguridad de Thunderbolt en Boot Camp

Anteriormente, se han demostrado los ataques de acceso directo a memoria (DMA) contra el puerto Thunderbolt mediante los ataques ThunderClap.

Los ataques basados en DMA permiten a los atacantes comprometer las computadoras específicas en cuestión de segundos con solo enchufar dispositivos maliciosos de conexión en caliente, como una tarjeta de red externa, mouse, teclado, impresora o almacenamiento, en el puerto Thunderbolt o el último puerto USB-C.

Resumidamente, los ataques DMA son posibles debido a que el puerto Thunderbolt funciona a un nivel muy bajo y con un alto acceso privilegiado a la computadora, lo que permite que los periféricos conectados eludan las políticas de seguridad del sistema operativo y lean/escriban directamente en la memoria del sistema, que puede contener información confidencial, incluyendo contraseñas, inicios de sesión bancarios, archivos privados y actividad del navegador.

Para evitar ataques de DMA, Intel introdujo algunas contramedidas, y una de ellas fueron los *«niveles de seguridad»*, que evitan que los dispositivos no autorizados basados en Thunderbolt PCIe se conecten sin la autorización del usuario.

> *«Para fortalecer aún más la autenticación del dispositivo, se dice que el sistema proporciona 'autenticación criptográfica de las conexiones' para evitar que los dispositivos falsifiquen los dispositivos autorizados por el usuario»*, dijo el

> investigador.

Sin embargo, al combinar las tres primeras fallas de ThunderSpy, un atacante puede romper la función de «niveles de seguridad» y cargar un dispositivo Thunderbolt malintencionado no autorizado falsificando las identidades de los dispositivos Thunderbolt, como se muestra en una demostración de video compartida por Ruytenberg.

> *«Los controladores Thunderbolt almacenan los metadatos del dispositivo en una sección de firmware denominada ROM de dispositivo (DROM). Hemos encontrado que el DROM no se verifica criptográficamente. Después del primer problema, esta vulnerabilidad permite construir identidades de dispositivo Thunderbolt falsificadas. Además, cuando se combina con el segundo problema, las identidades falsificadas pueden comprender parcial o totalmente datos arbitrarios»,* agregó.
>
> *«Además, mostramos la anulación no autenticada de las configuraciones de nivel de seguridad, incluida la capacidad de deshabilitar la seguridad de Thunderbolt por completo, y restaurar la conectividad de Thunderbolt si el sistema se limita a pasar exclusivamente a través de USB y/o Display Port».*

Según Ruytenberg, algunos de los últimos sistemas disponibles en el mercado desde 2019 incluyen la protección DMA Kernel que mitiga parcialmente las vulnerabilidades de ThunderSpy.

> *«Concluimos este informe demostrando la capacidad de desactivar permanentemente la seguridad de Thunderbolt y bloquear todas las futuras actualizaciones de firmware».*

Para saber si un sistema está afectado por la vulnerabilidades de ThunderSpy, Ryutenberg

también lanzó una herramienta gratuita y de código abierto llamada Spycheck.

Cuando el investigador informó sobre las vulnerabilidades a Intel, la compañía dijo que ya era consciente de algunas de ellas, sin planes de parchearlas o revelarlas al público.

Ryutenberg asegura haber encontrado más vulnerabilidades potenciales en el protocolo Thunderbolt, que actualmente forma parte de una investigación en curso y se espera que se revele pronto como ThunderSpy 2.