Los investigadores de seguridad descubrieron una nueva clase de vulnerabilidad de seguridad que incluye a todos los sistemas operativos principales, como Microsoft Windows, Apple MacOS, Linux y FreeBSD, que permite a los atacantes evitar los sistemas de protección para defenderse de ataques DMA.

Conocidos desde hace años, los ataques basados en el acceso directo a la memoria (DMA) permiten que un atacante ponga en peligro la computadora específica en pocos segundos al conectar un dispositivo malicioso de conexión en caliente, como una tarjeta de red externa, mouse, teclado, impresora, almacenamiento y tarjeta gráfica.

Los ataques basados en DMA son posibles ya que el puerto Thunderbolt permite que los periféricos conectados eviten las políticas de seguridad del sistema operativo y la memoria del sistema de lectura / escritura directa que contiene información confidencial, incluidas las contraseñas, los inicios de sesión bancarios, los archivos privados y la actividad del navegador.

Esto significa que con el simple hecho de conectar un dispositivo infectado, creado con herramientas como Interception, se puede manipular el contenido de la memoria y ejecutar código arbitrario con privilegios mucho más altos que los periféricos de bus serie universal, permitiendo a los atacantes eludir la pantalla de bloqueo o controlar las PC de forma remota.

Para bloquear los ataques basados en DMA, la mayoría de los sistemas operativos y dispositivos aprovechan la técnica de protección de la unidad de administración de memoria de entrada/salida (IOMMU) para controlar qué dispositivo periférico puede acceder a la memoria y qué región de la memoria.

Fallas de ThuderClap omiten IOMMU para volver a habilitar los ataques DMA

Un equipo de investigadores de ciberseguridad de la Universidad de Cambridge, la Universidad de Rice, y SRI International presentó un conjunto de nuevas vulnerabilidades en distintos sistemas operativos principales que podrían permitir a los hackers eludir la

protección de IOMMU.

Al imitar la funcionalidad de un dispositivo periférico legítimo, un atacante puede engañar a los sistemas operativos para que le den acceso a regiones sensibles de la memoria.

En un documento publicado a inicios de la semana, los investigadores detallaron la información técnica acerca de las nuevas vulnerabilidades que afirmaron haber descubierto utilizando una pila de hardware / software, llamada Thunderclap, que construyen y también lanzan en el código abierto.

> *«Nuestro trabajo aprovecha las vulnerabilidades en el uso del sistema operativo IOMMU para comprometer un sistema objetivo por medio de DMA, incluso en presencia de un IOMMU que está habilitado y configurado para defenderse de los ataques DMA»*, dijeron los investigadores.

Además, los investigadores destacaron que, dado que IOMMU no se habilita de forma predeterminada en la mayoría de los sistemas operativos y que los dispositivos modernos tienen USB-C, la superficie de ataque DMA ha aumentado significativamente, lo que anteriormente se limitaba principalmente a dispositivos Apple con puertos Thunderbolt 3.

> *«El aumento de las interconexiones de hardware como Thunerbolt 3 sobre USB-C, que combina la entrada de alimentación, la salida de video y el DMA de dispositivo periférico sobre el mismo puerto, aumenta enormemente la aplicabilidad en el mundo real de las vulnerabilidades de Thunderclap»*, agregaron.

> *«Particularmente, todas las computadoras portátiles y computadoras de escritorio Apple producidas desde 2011 son vulnerables, con la excepción del MacBook de 12 pulgadas. Muchas computadoras portátiles y algunas computadoras de escritorio, diseñadas para funcionar con Windows o Linux producidas desde 2016 también son*

> *afectadas; verifique si su computadora portátil es compatible con Thunderbolt*».

Cómo protegerse de las vulnerabilidades de Thunderclap

Los investigadores informaron de sus hallazgos a todos los principales proveedores de hardware y sistemas operativos, y la mayoría de ellos enviaron una mitigación importante para hacer frente a las vulnerabilidades de Thunderclap.

> *«En macOS 10.12.4 y versiones posteriores, Apple abordó la vulnerabilidad específica de la tarjeta de red que utilizamos para lograr una shell de root. Recientemente, Intel contribuyó con parches a la versión 5.0 del kernel de Linux»*, dijeron los investigadores.
>
> *«El proyecto FreeBSD indicó que los dispositivos periféricos no están actualmente dentro de su modelo de amenaza para la respuesta de seguridad».*

Aunque no todos los parches de software pueden bloquear por completo los ataques DMA, se recomienda a los usuarios que instalen las actualizaciones de seguridad disponibles para reducir la superficie de ataque. Según los investigadores, la mejor manera de protegerse por completo es deshabilitar los puertos Thunderbolt en su máquina, si es aplicable.

Además, los investigadores también desarrollaron un hardware de prueba de concepto que puede ejecutar las vulnerabilidades de ThunderClap en sistemas operativos específicos, pero optaron por no lanzarlo en público por ahora.