Patrick Wardle, ex hacker de la NSA y ahora director de investigación en Digita Security, ha descubierto una vulnerabilidad de día cero en el sistema MacOS que podría permitir a una aplicación maliciosa hacer clic en los objetos con los que no tenga interacción el usuario.

> *«Con un solo clic, es posible eludir por completo innumerables mecanismos de seguridad. Ejecutar la aplicación que no es de confianza?, un clic, permitir. Autorizar el acceso al llavero? un clic, permitir. Cargar la extensión del kernel de terceros? un clic, permitir»,* explica Wardle.

El analista descubrió esta vulnerabilidad sobre las interacciones «sintéticas» con una interfaz de usuario como *«el ratón es más poderoso que la espada»,* demostrando un ataque que es capaz de realizar clics sintéticos generados por un software en lugar de un humano.

Wardle descubrió de forma accidental que High Sierra interpreta incorrectamente dos eventos consecutivos del mouse inactivo como clic legítimo, lo que permite a los atacantes interactuar mediante programación con advertencias de seguridad, pidiendo a los usuarios elegir entre «permitir» o «denegar» y acceder a datos o características confidenciales.

> *«La interfaz de usuario es ese único punto de falla. Si tiene una forma de interactuar sintéticamente con estas alertas, tiene una forma muy poderosa y genérica de eludir todos estos mecanismos de seguridad»,* dice Wardle.

Explica también que la vulnerabilidad puede aprovecharse para eliminar todas las contraseñas del llavero o cargar extensiones maliciosas del kernel al realizar clic virtual en «permitir» en el indicador de seguridad y obtener el control total de la máquina objetivo.

El experto indica que encontró dicha vulnerabilidad accidentalmente al copiar y pegar el código y que sólo dos líneas del código son suficientes para romper por completo el mecanismo de seguridad.

Wardle no informó a Apple al respecto y prefirió revelar públicamente los detalles del error en la conferencia DefCon hacker.

> *«Por supuesto, los proveedores de sistemas operativos como Apple son muy conscientes del vector de ataque y por lo tanto se esfuerzan por diseñar su interfaz de usuario de una forma que sea resistente a los eventos sintéticos. Desafortunadamente, fallaron»,* explicó Wardle.

Mientras tanto, la próxima versión de MacOS de Apple, Mojave, ha arreglado la amenaza mediante el bloqueo de eventos sintéticos, lo que reduce el alcance de las funciones de accesibilidad en las aplicaciones que utilizan de forma legítima dicha característica.