Microsoft alertó el miércoles sobre una vulnerabilidad de seguridad ahora parcheada, que afecta a los sistemas operativos de Apple, que de ser explotada, podría permitir a los hackers escalar privilegios en el dispositivo e implementar malware.

> *«Un atacante podría aprovechar esta vulnerabilidad de escape de sandbox para obtener privilegios elevados en el dispositivo afectado o ejecutar comandos maliciosos como instalar cargas útiles adicionales»,* dijo Jonathan Bar Or, del Microsoft 365 Defender Research Team.

Rastreada como CVE-2022-26706 (puntuación CVSS: 5.5), la vulnerabilidad de seguridad afecta a iOS, iPadOS, macOS, tvOS y watchOS, y fue reparada por Apple en mayo de 2022.

Al llamarlo un problema de acceso que afecta el componente LaunchServices (launchd), la compañía dijo que *«un proceso en un espacio aislado puede eludir las restricciones del espacio aislado»,* y agregó que mitiga el problema con restricciones adicionales.

Aunque App Sandbox de Apple está diseñado para regular estrictamente el acceso de una aplicación de terceros a los recursos del sistema y los datos del usuario, la vulnerabilidad hace posible eludir estas restricciones y comprometer la máquina.

> *«La función principal del sandbox es contener el daño al sistema y los datos del usuario si el usuario ejecuta una aplicación comprometida»*, dijo Apple en su documentación.

> *«Aunque el sandbox no evita los ataques contra su aplicación, reduce el daño que*

> *puede causar un ataque exitoso al restringir su aplicación al conjunto mínimo de privilegios que requiere para funcionar correctamente».*

Microsoft dijo que descubrió la falla durante sus intentos de encontrar una forma de escapar de la zona de pruebas y ejecutar comandos arbitrarios en macOS ocultando el código malicioso en una macro de Microsoft Office específicamente diseñada.

Específicamente, la prueba de concepto (PoC) del tamaño de un tweet ideada por Apple, aprovecha los servicios de lanzamiento como un medio para ejecutar un comando abierto, una utilidad usada para abrir archivos y lanzar aplicaciones, en una carga útil de Python que contiene instrucciones no autorizadas.

Cabe mencionar que cualquier archivo que se deje caer por una aplicación de espacio aislado se adjunta automáticamente al atributo extendido *«com.apple.quarantine»* para activar un aviso que requiere el consentimiento explícito del usuario antes de la ejecución.

Sin embargo, esta restricción se puede eliminar utilizando la opción -stdin para el comando de apertura asociado con el archivo de explotación de Python.

> *«-stdin omitió la restricción del atributo extendido «com.apple.quarentine», ya que no había forma de que Python supiera que el contenido de su entrada estándar se originó a partir de un archivo en cuarentena»,* dijo Bar Or.