Un hacker anónimo con el alias «*SandboxEscaper*«, lanzó hoy un código de vulnerabilidad de prueba de concepto (PoC) para una nueva vulnerabilidad de Día Cero que afecta al sistema operativo Windows 10, siendo la quinta publicación en menos de un año.

El pirata informático publicó el material en GitHub, se trata de un problema de escalamiento de privilegios que podría permitir a un atacante local o malware obtener y ejecutar código con privilegios de sistema administrativo en las máquinas seleccionadas, lo que finalmente permitirá que el atacante obtenga control total de la computadora.

La vulnerabilidad reside en el Programador de Tareas, una utilidad que permite a los usuarios de Windows programar el inicio de programas o secuencias de comandos en un momento predefinido o después de intervalos de tiempo específicos.

El código de explotación de SandboxEscaper hace uso de SchRpcRegisterTask, un método en el Programador de Tareas para registrar las tareas en el servidor, que no verifica correctamente los permisos, por lo que puede utilizarse para establecer un permiso arbitrario de DACL (lista de control de acceso discrecional).

> *«Esto dará lugar a una llamada al siguiente RPC '_SchRpcRegisterTask', que está expuesto por el servicio del programador de tareas»*, dijo el hacker.

Un programa malintencionado o un atacante con pocos privilegios puede ejecutar un archivo .job con formato incorrecto para obtener privilegios del sistema, lo que eventualmente le permite al atacante obtener acceso completo al sistema de destino.

SandboxEscaper también compartió un video de prueba de concepto que muestra el nuevo exploit 0-Day de Windows en acción.

La vulnerabilidad ha sido probada y se confirmó que funciona correctamente en una versión totalmente parcheada y actualizada de Windows 10 de 32 bits y 64 bits, así como en Windows Server 2016 y 2019.

Aparte de esto, el hacker aseguró que todavía tiene 4 errores más que no han sido revelados, tres de los cuales llevan a una escalada local de privilegios y el cuarto permite a los atacantes eludir la seguridad de la zona de pruebas.

Los detalles y el código de explotación para el nuevo zero-day de Windows se han producido a tan solo una semana después de las actualizaciones de parches mensuales de Microsoft, lo que significa que no existe un parche para dicha vulnerabilidad en la actualidad, lo que permite a cualquier persona explotar y avisar de ella.

Los usuarios de Windows 10 deben esperar una solución de seguridad para esta vulnerabilidad hasta las actualizaciones de seguridad del próximo mes, a menos que Microsoft presente una actualización de emergencia.