Un investigador anónimo apodado como SandboxEscaper, compartió hoy de forma pública un segundo exploit de día cero que se puede utilizar para evitar una vulnerabilidad de elevación de privilegios que fue recientemente parcheada en el sistema Microsoft Windows.

SandboxEscaper es conocido por eliminar públicamente ataques Zero-Day en Windows que no cuentan con parches. En el último año, el hacker reveló más de 12 vulnerabilidades de este tipo en Windows, sin tener que informarle a la compañía sobre los problemas.

Hace solo dos semanas, el pirata informático reveló cuatro nuevos exploits de Windows, uno de ellos era uno que podría permitir a los atacantes evitar una vulnerabilidad de elevación de privilegios (CVE-2019-0841) en Windows, que existía cuando el Servicio de Implementación de Windows AppX (AppXSVC) manejaba incorrectamente los enlaces.

Ahora, el pirata informático asegura que encontró una nueva forma de eludir el parche de seguridad de Microsoft por la misma vulnerabilidad, lo que permite que una aplicación maliciosa especialmente diseñada aumente sus privilegios y tome el control completo de la máquina Windows parcheada.

ByeBear, como se apodó al explot, abusa del navegador Microsoft Edge para escribir la lista de control de acceso discrecional (DACL), como privilegio del SISTEMA. Esto se puede observar en el video:

> *«Va a aumentar la prioridad de los subprocesos para aumentar nuestras probabilidades de ganar la condición de carrera que esto explota. Si su VM se bloquea significa que tiene un núcleo o configura su VM para que tenga múltiples procesadores en lugar de múltiples núcleos»,* explicó SandboxExplorer.

> *«Este error definitivamente no está restringido al borde. Esto también se activará con otros paquetes. Por lo tanto, definitivamente puede encontrar una forma de desencadenar este error en silencio sin tener una ventana emergente. O probablemente podría minimizar el borde tan pronto como sea posible»,* agregó.

Las siguientes actualizaciones del parche de Microsoft saldrán el 11 de junio, es necesario esperar a esa fecha para ver si la compañía reconocería cuatro vulnerabilidades anteriores y lanzaría los parches de seguridad.