Un investigador de seguridad cibernética publicó este lunes un código de explotación de prueba de concepto (PoC) para una vulnerabilidad recientemente descubierta que afecta a Google Chrome, además de otros navegadores basados en Chromium como Microsoft Edge, Opera y Brave.

Lanzado por Rajvardhan Agarwal, el exploit de trabajo se refiere a una vulnerabilidad de ejecución remota de código en el motor de renderizado de JavaScript V8 que alimenta los navegadores web. Se cree que es la misma falla demostrada por Bruno Keith y Niklas Baumstark de Dataflow Security, en el concurso de piratería Pwn20sn 2021 la semana pasada.

Keith y Baumstark recibieron 100 mil dólares por aprovechar la vulnerabilidad para ejecutar código malicioso dentro de Chrome y Edge.

Según la captura de pantalla compartida por Agarwal, el archivo PoC HTML y su archivo JavaScript asociado se pueden cargar en un navegador basado en Chromium para aprovechar la falla de seguridad e iniciar la aplicación de calculadora de Windows. Cabe señalar que el exploit debe estar encadenado con otra falla que puede permitir escapar de las protecciones de la sandbox de Chrome.

Al parecer, Argawal pudo desarrollar el PoC mediante ingeniería inversa del parche que el equipo Chromium de Google impulsó al componente de código abierto luego de que se compartieran los detalles de la vulnerabilidad con la compañía.

> *«Tener nuestros propios errores no estaba en mi tarjeta de bingo para 2021. No estoy seguro de que Google haya sido demasiado inteligente para agregar esta prueba de regresión de inmediato»,* dijo Baumstark.