Surgieron detalles sobre una vulnerabilidad crítica de ejecución remota de código recientemente parcheada en el motor V8 JavaScript y WebAssembly, utilizado en los navegadores basados en Google Chrome y Chromium.

La vulnerabilidad se relaciona con un caso de use-after-free en el componente de optimización de instrucciones, cuya explotación exitosa podría *«permitir que un atacante ejecute código arbitrario en el contexto del navegador».*

La falla, que se identificó en la versión del Canal Dev de Chrome 101, fue informada a Google por Weibo Wang, un investigador de seguridad de la compañía de seguridad cibernética de Singapur, Numen Cyber Technology, y desde entonces la compañía la solucionó en silencio.

> *«Esta vulnerabilidad ocurre en la etapa de selección de instrucciones, donde se seleccionó la instrucción correcta y resultó en una excepción de acceso a la memoria»,* dijo Wang.

Las fallas de uso después de liberar ocurren cuando se accede a la memoria liberada anteriormente, lo que induce un comportamiento indefinido y hace que un programa se bloquee, use datos corruptos o incluso logre la ejecución de código arbitrario.

Lo que es más preocupante es que la falla se puede explotar de forma remota por medio de un sitio web especialmente diseñado para eludir las restricciones de seguridad y ejecutar código arbitrario para comprometer los sistemas objetivo.

> *«Esta vulnerabilidad se puede explotar aún más utilizando técnicas de rociado de montones, y luego conduce a una vulnerabilidad de confusión de tipos. La vulnerabilidad permite a un atacante controlar los punteros de función o escribir*

> *código en ubicaciones arbitrarias en la memoria y, en última instancia, conducir a la ejecución del código»*, explicó Wang.

La compañía no ha revelado la vulnerabilidad a través del portal de seguimiento de errores de Chromium para que tantos usuarios como sea posible instalen primero la versión parcheada. Además, Google no asigna ID de CVE para vulnerabilidades encontradas en canales de Chrome no estables.

Los usuarios de Chrome, especialmente los desarrolladores que utilizan la edición Dev de Chrome para realizar pruebas y asegurarse de que sus aplicaciones sean compatibles con las últimas funciones de Chrome y los cambios de API, deben actualizar a la última versión disponible del software.

Esta no es la primera vez que se descubren vulnerabilidades de uso después de liberar en V8. En 2021, Google abordó 7 errores del mismo tipo en Chrome que se explotaron en ataques del mundo real.

Este año, también se corrigió una vulnerabilidad use-after-free explotada activamente en el componente de animación.