Una vulnerabilidad en la función PDFium de Google Chrome, podría ser aprovechada por un adversario para corromper la memoria y potencialmente ejecutar código remoto.

PDFium permite a los usuarios abrir archivos PDF dentro de Chrome. Cisco Talos recientemente descubrió una vulnerabilidad que permitiría a un atacante enviar una página web maliciosa a un usuario y luego causar un acceso a la memoria fuera de los límites.

La vulnerabilidad de corrupción de memoria de documentos activos de Google Chrome PDFium JavaScript, rastreada como CVE-2020-6513, reside en la forma en que Google Chrome 83.0.4103.61 ejecuta JavaScript dentro de documentos PDF.

Una página web especialmente diseñada podría provocar un acceso a la memoria fuera de límite. Para activar la vulnerabilidad, la víctima debe visitar una página web maliciosa o abrir un documento PDF malicioso.

La vulnerabilidad recibió un puntaje de gravedad de 6.3 en la escala CVSS 3.0. Google ha corregido el problema en la última versión del navegador web, por lo que es recomendable actualizar de inmediato.

El investigador Aleksandar Nikolic, emitió un reporte en el que muestra una prueba de concepto (PoC), que causa un estado de tiempo de ejecución V8 específico que desencadena la corrupción de memoria, lo que resulta en un acceso fuera de los límites. Es posible abusar de esto para causar daños graves en la memoria y potencialmente conducir a la ejecución de código arbitrario.