Google implementó soluciones para cinco vulnerabilidades de seguridad en su navegador web Chrome, incluida una que está siendo explotada en la naturaleza, lo que la convierte en la decimoséptima vulnerabilidad de este tipo que se revela desde inicios de año.

Rastreada como CVE-2021-4102, la vulnerabilidad se relaciona con un error del tipo use-after-free en el motor V8 JavaScript y WebAssembly, que podría tener graves consecuencias que van desde la corrupción de datos válidos hasta la ejecución de código arbitrario. El crédito por descubrir e informar la vulnerabilidad se atribuyó a un investigador anónimo.

Aún no se sabe exactamente cómo se está abusando de la vulnerabilidad en los ataques en el mundo real, pero la compañía emitió una declaración concisa que dice que está *«al tanto de los informes de que existe un exploit para CVE-2021-4102 en la naturaleza».*

Esto se hace en un intento de garantizar que la mayoría de los usuarios estén actualizados con una solución y evitar una mayor explotación por parte de otros actores de amenazas.

CVE-2021-4102 es la segunda vulnerabilidad use-after-free en V8 que la compañía ha tenido que solucionar en menos de tres meses después de informes de explotación activa, con la vulnerabilidad anterior, CVE-2021-37975, también reportada por un investigador anónimo, conectado a una actualización que se envió el 30 de septiembre.

Con esta última actualización, Google ha abordado un récord de 17 0-day en Chrome solo en 2021:

- CVE-2021-21148: desbordamiento del búfer de pila en V8
- CVE-2021-21166: Problema de reciclaje de objetos en audio
- CVE-2021-21193: use-after-free en Blink
- CVE-2021-21206: use-after-free en Blink
- CVE-2021-21220: validación insuficiente de una entrada que no es de confianza en V8 para x86_64
- CVE-2021-21224: confusión de tipos en V8
- CVE-2021-30551: confusión de tipos en V8

- CVE-2021-30554: uso gratuito en WebGL
- CVE-2021-30563: confusión de tipos en V8
- CVE-2021-30632: Escritura fuera de límites en V8
- CVE-2021-30633: Use-after-free en API de base de datos indexada
- CVE-2021-37973: Use-after-free en Portals
- CVE-2021-37975: Use-after-free en V8
- CVE-2021-37976: fuga de información en el núcleo
- CVE-2021-38000: validación insuficiente de entradas no confiables en Intents
- CVE-2021-38003: implementación inadecuada en V8

Se recomienda a los usuarios de Chrome que actualicen a la última versión (96.0.4664.110) para Windows, Mac y Linux para evitar cualquier riesgo potencial de explotación activa.