Google lanzó otra actualización de su navegador web Chrome para Windows, Mac y Linux, con el fin de corregir cuatro vulnerabilidades de seguridad, incluyendo una vulnerabilidad de día cero que está siendo explotada en la naturaleza.

Rastreada como CVE-2021-30554, la vulnerabilidad de alta gravedad se refiere a un error de uso posterior libre en WebGL, también conocida como Biblioteca de Gráficos Web, una API de JavaScript para renderizar gráficos interactivos 2D y 3D dentro del navegador.

La explotación exitosa de la vulnerabilidad puede significar la corrupción de datos válidos, lo que provocaría un bloqueo e incluso la ejecución de códigos o comandos no autorizados.

El problema se informó a Google de forma anónima el pasado 15 de junio, según confirmó el gerente del programa técnico de Chrome, Srinivas Sista, y agregó que la compañía es *«consciente de que existe un exploit para CVE-2021-30554 en la naturaleza».*

Aunque por lo generar se suele limitar los detalles de la vulnerabilidad hasta que la mayoría de los usuarios se actualicen con la solución, el desarrollo se produce en menos de 10 días después de que Google abordara otra vulnerabilidad de día cero explotada en ataques activos (CVE-2021-30551).

CVE-2021-30554 es también la octava vulnerabilidad Zero Day parcheada por Google desde inicios del año.

> *«Estoy contento de que estemos mejorando en la detección de estos exploits y de las excelentes asociaciones que tenemos para reparar las vulnerabilidades, pero sigo preocupado por cuántos se están descubriendo de forma continua y el papel de los proveedores comerciales»,* dijo Shane Huntley, director del Grupo de Análisis de Amenazas de Google.

Es recomendable que los usuarios de Chrome actualicen el navegador a la última versión (91.0.4472.114).