Google lanzó el jueves actualizaciones de software para abordar otra vulnerabilidad de día cero en su navegador web Chrome.

Rastreada como CVE-2022-4135, la vulnerabilidad de alta gravedad se describió como un desbordamiento del búfer de almacenamiento dinámico en el componente GPU. A Clement Lecigne, del Threat Analysis Group (TAG) de Google, se le atribuye el informe de la falla el 22 de noviembre de 2022.

Los hackers pueden armar los errores de desbordamiento de búfer basados en heap para bloquear un programa o ejecutar código arbitrario, lo que lleva a un comportamiento no deseado.

> *«Google es consciente de que existe un exploit para CVE-2022-4135»,* dijo la compañía.

Pero al igual que otros problemas explotados activamente, los detalles técnicos se han retenido hasta que la mayoría de los usuarios se actualicen con una solución y así evitar más abusos.

Con la última actualización, Google resolvió ocho vulnerabilidades de día cero en Chrome desde inicios de año:

- CVE-2022-0609: Use-after-free en Animation
- CVE-2022-1096: Confusión de tipo en V8
- CVE-2022-1364: Confusión de tipos en V8
- CVE-2022-2294: Desbordamiento del búfer almacenado dinámico en WebRTC
- CVE-2022-2856: Validación insuficiente de entrada no confiable en Intents
- CVE-2022-3075: Validación de dats insuficientes en Mojo
- CVE-2022-3723: Confusión de tipos en V8

Se recomienda a los usuarios actualizar a la versión 107.0.5304.121 para macOS y Linux y

107.0.5304.121/.122 para Windows con el fin de mitigar posibles amenazas.

También se recomienda a los usuarios de navegadores web basados en Chromium, como Microsoft Edge, Brave, Opera y Vivaldi, que apliquen las correcciones en cuanto estén disponibles.