A un mes de haber parcheado una vulnerabilidad de día cero explotada activamente en Chrome, Google lanzó el 2 de marzo correcciones para otra vulnerabilidad de día cero en el navegador web, que también está siendo explotada en la naturaleza.

Chrome 89.0.4389.72, lanzado para Windows, Mac y Linux este martes, viene con 47 correcciones de seguridad, la más grave de estas, se refiere a un *«problema del ciclo de vida de los objetos en el audio»*.

Rastreada como CVE-2021-21166, la vulnerabilidad es uno de los dos errores reportados el mes pasado por Alison Huffman, de Microsoft Browser Vulnerabillity Research, el 11 de febrero de 2021.

Una falla separada del ciclo de vida de un objeto, también identificada en el componente de audio, fue reportada a Google el 4 de febrero, el mismo día en que estuvo disponible la versión estable de Chrome 88.

Google reconoció que existe un exploit para la vulnerabilidad en la naturaleza, pero no llegó a compartir más detalles para permitir que la mayoría de los usuarios instalen las correcciones y evitar que otros actores de amenazas creen exploits dirigidos al día cero.

> *«Google es consciente de los informes de que un exploit para CVE-2021-21166 existe en la naturaleza»*, dijo Prudhvikumar Bommana.

El 4 de febrero, la compañía emitió una solución para una falla de desbordamiento de búfer de pila, explotada activamente (CVE-2021-21148) en su motor de renderizado V8 JavaScript.

Además, el año pasado, Google resolvió cinco días cero de Chrome, que estaban siendo explotados activamente en la naturaleza en un lapso de tiempo de un mes, entre el 20 de

octubre y el 12 de noviembre de 2020.

Es importante actualizar inmediatamente el navegador web para mantenerse al día con las actualizaciones de seguridad.