Google corrigió otra vulnerabilidad de día cero explotada activamente en el navegador web Chrome, lo que significa una segunda solución de este tipo lanzada por la compañía en un mes.

La compañía envió este viernes la versión 89.0.4389.90 para Windows, Mac y Linux, que se espera sea implementada en los próximos días para todos los usuarios.

Aunque la actualización contiene un total de cinco correcciones de seguridad, la vulnerabilidad más importante corregida por Google se refiere a un uso libre posterior en su motor de renderizado Blink. La vulnerabilidad se rastrea como CVE-2021-21193.

Los detalles de la vulnerabilidad fueron informados a Google por un investigador de seguridad cibernética anónimo el 9 de marzo.

Como sucede siempre con las vulnerabilidades explotadas activamente, Google emitió una declaración concisa reconociendo que existía un exploit para CVE-2021-21193, pero se abstuvo de compartir información adicional hasta que la mayoría de los usuarios estén actualizados en las correcciones y eviten que otros actores de amenazas creen exploits apuntando a este día cero.

> *«Google está al tanto de los informes de que existe un exploit para CVE-2021-21193 en la naturaleza»,* dijo el gerente del programa técnico de Chrome, Prudhvikumar Bommana.

Con esta actualización, Google ha solucionado tres vulnerabilidades de día cero en Chrome desde inicios de año.

A inicios del mes, la compañía emitió una solución para un *«problema del ciclo de vida de los objetos en el audio»* (CVE-2021-21166) que, según dijo, estaba siendo explotado activamente.

Antes, el 4 de febrero, la compañía corrigió otra falla de desbordamiento de búfer de pila explotada activamente (CVE-2021-21148) en su motor de renderizado V8 JavaScript.

Los usuarios de Chrome pueden actualizar a la última versión dirigiéndose a Configuración > Ayuda > Acerca de Google Chrome.