Google parcheó dos vulnerabilidades de día cero en el navegador web Chrome para escritorio, siendo estas la cuarta y quinta vulnerabilidades explotadas activamente y abordadas por la compañía en las últimas semanas.

La compañía lanzó la versión 86.0.4240.198 para Windows, Mac y Linux, que dijo que se implementará en los siguientes días/semanas para todos los usuarios.

Rastreadas como CVE-2020-16013 y CVE-2020-16017, las vulnerabilidades fueron descubiertas e informadas a Google por fuentes *«anónimas»,* a diferencia de casos anteriores, que fueron descubiertos por el equipo de seguridad de élite Project Zero de la compañía.

Google reconoció que existen exploits para ambas vulnerablidades en la naturaleza, pero no llegó a compartir más detalles para permitir que la mayoría de los usuarios instalen las correcciones.

Según las notas de la versión, los dos defectos son:

- CVE-2020-16013: El 9 de noviembre se informó sobre una *«implementación inapropiada»* de su motor de renderizado V8 JavaScript
- CVE-2020-16017: El 7 de noviembre se informó un problema de corrupción de memoria de uso después de la liberación en la función de aislamiento de sitios de Chrome.

Cabe mencionar que el día cero que parcheó la compañía la semana pasada, CVE-2020-16009, también se refería a una implementación inapropiada de V8, lo que llevó a la ejecución remota de código. No está claro hasta ahora si las dos fallas están relacionadas.

En la última semana Google reveló una serie de vulnerabilidades de día cero explotadas activamente, dirigidas a Chrome, Windows, iOS y MacOS, y aunque parece que algunos de estos problemas se unieron para formar una cadena de exploits, la compañía aún no ha revelado detalles sobre quién puede estarlos usando y quiénes eran los objetivos previstos.