Una vulnerabilidad en Apple Safari, que se explotó a inicios de 2022, se solucionó originalmente en 2013 y se reintrodujo en diciembre de 2016, según un nuevo informe de Google Project Zero.

La vulnerabilidad, rastreada como CVE-2022-22620 (puntaje CVSS: 8.8), se refiere a un caso de vulnerabilidad de use-after-free en el componente WebKit, que podría ser explotado por una pieza de contenido web especialmente diseñado para obtener la ejecución de código arbitrario.

A inicios de febrero de 2022, Apple envió parches para la vulnerabilidad en Safari, iOS, iPadOS y macOS, aunque reconoció que *«puede haber sido explotado activamente».*

> *«En este caso, la variante se parchó por completo cuando se informó inicialmente de la vulnerabilidad en 2013. Sin embargo, la variante se reintrodujo tres años después durante grandes esfuerzos de refactorización. La vulnerabilidad continuó existiendo durante 5 años hasta que se arregló como un día cero en estado salvaje en enero de 2022»,* dijo Maddie Stone, de Google Project Zero.

Aunque los errores de 2013 y 2022 en la API de historial son esencialmente los mismos, las rutas para desencadenar la vulnerabilidad son diferentes. Después, los cambios de código posteriores realizados años después revivieron la falla de día cero de entre los muertos como un *«zombie».*

Al afirmar que el incidente no es exclusivo de Safari, Stone enfatizó además tomarse el tiempo adecuado para auditar el código y los parches para evitar instancias de duplicación de las correcciones y comprender los impactos de seguridad de los cambios que se llevan a cabo.

> *«Tanto las confirmaciones de octubre de 2016 como las de diciembre de 2016 fueron muy grandes. La confirmación de octubre cambió 40 archivos con 900*

> *adiciones y 1225 eliminaciones. La confirmación de diciembre cambió 95 archivos con 1336 adiciones y 1325 eliminaciones»,* dijo Stone.

> *«Parece insostenible que los desarrolladores o revisores comprendan en detalle las implicaciones de seguridad de cada cambio en esos compromisos, especialmente porque están relacionados con la semántica de por vida».*