Google implementó este viernes un parche de seguridad de emergencia en su navegador web Chrome para abordar una vulnerabilidad de seguridad que se sabe que ya tiene un exploit en la naturaleza.

Rastreada como CVE-2021-37973, la vulnerabilidad se describe como use after free en Portals API, un sistema de navegación de páginas web que permite que una página muestre otra página como un recuadro y *«realice una transición sin problemas a un nuevo estado, donde la página anteriormente insertada se convierte en el documento de nivel superior».*

Clément Lecigne, de Google Threat Analysis Group (TAG), es a quien se le atribuyó el mérito por informar la vulnerabilidad. No se han revelado detalles adicionales relacionados con la debilidad a la luz de la explotación activa y para permitir que la mayoría de los usuarios apliquen el parche, pero Google dijo que es «*consciente de que existe un exploit para CVE-2021-37973 en la naturaleza».*

La actualización llega un día después de que Apple se moviera para cerrar un agujero de seguridad explotado activamente en versiones anteriores de iOS y macOS (CVE-2021-30869), que el TAG señaló como *«utilizado junto con una ejecución remota de código de N días dirigida a Webkit. Con la última solución, Google abordó un total de 12 fallas de día cero en Chrome desde inicios de 2021».*

Las vulnerabilidades abordadas son:

- CVE-2021-21148: Desbordamiento del búfer de pila en V8
- CVE-2021-21116: Problema de reciclaje de objetos en audio
- CVE-2021-21193: Use after free en Blink
- CVE-2021-21206: Use after free en Blink
- CVE-2021-21220: Validación insuficiente de una entrada que no es de confianza en V8 para x86:64
- CVE-2021-21224: Confusión de tipos en V8
- CVE-2021-30551: Confusión de tipos en V8
- CVE-2021-30554: Use-after-free en WebGL

- CVE-2021-30563: Confusión de tipos en V8
- CVE-2021-30632: Escritura fuera de límites en V8
- CVE-2021-30633: Use after free en API de base de datos indexada

Se recomienda a los usuarios de Chrome que actualicen a la última versión (94.0.4606.61) para Windows, Mac y Linux.