Google impulsó el jueves correcciones de seguridad urgentes para su navegador web Chrome, incluyendo un par de nuevas vulnerabilidad de seguridad que, según la compañía, están siendo explotadas en la naturaleza, lo que las convierte en el cuarto y quinto 0-Day activamente conectados solo este mes.

Las vulnerabilidades, rastreadas como CVE-2021-37975 y CVE-2021-37976, son parte de un total de cuatro y se refieren a una falla de uso después de la ausencia en el motor V8 JavaScript y WebAssembly, así como a una fuga de información en el núcleo.

Google se ha abstenido de compartir más detalles acerca de cómo se utilizaron las vulnerabilidades de día cero en los ataques hasta que la mayoría de los usuarios se actualicen con los parches, pero dijo que es consciente de que *«exploits para CVE-2021-37975 y CVE-2021-37976 existen en la naturaleza».*

Se acreditó a un investigador anónimo por el informe de CVE-2021-37975. El descubrimiento de CVE-2021-37976 por otro lado, involucra a Clément Lecigne, de Google Threat Analysis Group, a quien también se le atribuyó CVE-2021-37973, otra vulnerabilidad de uso después de libre explotada activamente en la API de portales de Chrome que se informó la semana pasada, planteando la posibilidad de que las dos fallas se hayan unido como parte de una cadena de exploits para ejecutar código arbitrario.

Con la última actualización, Google abordó un récord de 14 días cero en el navegador web desde principios del año.

- CVE-2021-21148: desbordamiento del búfer de pila en V8
- CVE-2021-21166: Problema de reciclaje de objetos en audio
- CVE-2021-21193: Usar después de usarlo gratis en Blink
- CVE-2021-21206: Usar después de usarlo gratis 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
- CVE-2021-37973: Use-after-free en Portals

Se recomienda a los usuarios del navegador web Chrome que actualicen a la última versión.