Google lanzó una nueva actualización de seguridad para el navegador web Chrome para Windows, Mac y Linux, con múltiples correcciones, incluyendo una vulnerabilidad de día cero que está siendo explotada en la naturaleza.

El último parche resuelve un total de ocho vulnerabilidades, una de las cuales se refiere un problema de confusión de tipos en su motor de código abierto y JavaScript V8 (CVE-2021-30563). Google dio el crédito a un investigador anónimo por informar la vulnerabilidad el 12 de julio.

Como ocurre generalmente con las vulnerabilidades explotadas activamente, la compañía emitió una declaración en la que reconoce que *«existe un exploit para CVE-2021-30563 en la naturaleza»*, mientras se abstiene de compartir todos los detalles sobre la vulnerabilidad subyacente utilizada en los ataques debido a su gravedad y la posibilidad de que hacerlo pueda dar lugar a más abusos.

CVE-2021-30563 también marca el noveno día cero abordado por Google para combatir ataques del mundo real contra usuarios de Chrome desde inicios de 2021.

- CVE-2021-21148: Desbordamiento del búfer de pila en V8
- CVE-2021-21166: 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

Los usuarios de Chrome deben actualizar a la última versión (91.0.4472.164) para evitar ataques cibernéticos.