Zerodium, una plataforma de compra y venta de exploits y vulnerabilidades, publicó en Twitter que detectó una vulnerabilidad de Díaz Cero en el navegador Tor, que permitiría saltar las medidas de protección por medio de una puerta trasera, permitiendo así ejecutar código malicioso de forma remota.

Según Zerodium, dicha vulnerabilidad fue detectada en la versión 7 del navegador Tor, y ya se ha parcheado en la nueva actualización para la versión 8. El fallo permite la ejecución de código malicioso aún cuando la extensión NoScript esté activada.

Para esto, sólo era necesario configurar el «Content-Type» de una página web como *«text/html;/jason».* El exploit no hace nada por sí solo, ya que debe encadenarse con otros exploits para que se encarguen de sacarle provecho, aún así, Zerodium lo describe como un *«fallo grave».*

Al parecer, la compañía estuvo al tanto de la vulnerabilidad desde hace algunos meses, pero no la reveló porque el ganar dinero gracias a esto es su negocio. Por lo tanto, en una entrevista para el medio ZDNet, confirma que la hizo pública por haber llegado al *«final de su vida».*

> De igual forma, reconocen haberla hecho pública para *«concienciar la falta de auditorías de seguridad de los componentes principales del navegador Tor».*

Otro investigador de seguridad, bajo el nombre de @x0rz en Twitter, publicó un vídeo de 20 segundos en el que muestra lo fácil que es sacar provecho de dicha vulnerabilidad.

Por otro lado, el desarrollador de la extensión NoScript confirmó que lanzó un parche compatible con Tor Browser 7 que ya está disponible para su descarga.