Los mantenedores del proyecto Tails, emitieron una advertencia acerca de que el navegador Tor, que se incluye con el sistema operativo no es seguro para acceder o ingresar información confidencial.

> *«Le recomendamos que deje de usar Tails hasta el lanzamiento de 5.1 (31 de mayo) si usa Tor Browser para información confidencial (contraseñas, mensajes privados, información personal, etc.)»,* dijo el proyecto en un aviso.

Tails, abreviatura de The Amnesic Incognito Live System, es una distribución de Linux basada en Debian, orientada a la seguridad cuyo objetivo es preservar la privacidad y el anonimato mediante la conexión a Internet mediante la red Tor.

La alerta llega cuando Mozilla, el 20 de mayo de 2022, implementó correcciones para dos vulnerabilidades críticas de día cero en su navegador Firefox, una versión modificada del cual actúa como la base del navegador Tor.

Rastreadas como CVE-2022-1802 y CVE-2022-1529, las dos vulnerabilidades son lo que se conoce como contaminación prototipo que podría armarse para obtener la ejecución de código JavaScript en dispositivos que ejecutan versiones vulnerables de Firefox, Firefox ESR, Firefox para Android y Thunderbird.

> *«Por ejemplo, después de visitar un sitio web malicioso, un atacante que controle este sitio web podría acceder a la contraseña u otra información confidencial que envíe a otros sitios web durante la misma sesión de Tails»*, dice el aviso de Tails.

Las vulnerabilidades fueron demostradas por Manfred Paul en la 15° edición del concurso de hacking Pwn20wn celebrada en Vancouver la semana pasada, por el que el investigador recibió 100,000 dólares.

Sin embargo, los navegadores Tor que tienen habilitado el nivel de seguridad «*más seguro*«, así como el cliente de correo electrónico Thunderbird en el sistema operativo, son inmunes a las vulnerabilidades, ya que JavaScript está deshabilitado en ambos casos.

Además, las vulnerabilidades no rompen las protecciones de anonimato y cifrado integradas en Tor Browser, lo que significa que los usuarios de Tails que no manejan información confidencial pueden continuar usando el navegador web.

> *«Esta vulnerabilidad se solucionará en Tails 5.1 (31 de mayo), pero nuestro equipo no tiene la capacidad de publicar una versión de emergencia antes»,* dijeron los investigadores.