Investigadores del equipo de Ingeniería de Seguridad de la Información de Google, detallaron varios problemas de seguridad en el diseño del sistema anti seguimiento en Safari de Apple, la Prevención de Seguimiento Inteligente (ITP).

ITP está diseñado para restringir las cookies y es la respuesta de Apple a los vendedores en línea que rastrean a los usuarios en todos los sitios web. Sin embargo, los investigadores de Google afirman en un documento que ITP realmente filtra los hábitos de navegación web de los usuarios de Safari, *«permitiendo un seguimiento persistente entre sitios y permitiendo filtraciones de información entre sitio, incluida la búsqueda entre sitios»*.

Algunos de los errores fueron solucionados por las actualizaciones de seguridad de Apple en diciembre para Safari 13.04 y iOS 13.3. Pero los investigadores de seguridad de Google, aseguran que las mitigaciones no resuelven completamente los problemas de privacidad. *«Tales soluciones no resolverán el problema subyacente».*

John Wilander, ingeniero de Apple WebKit, detrás de ITP, agradeció a Google por su ayuda en diciembre con una publicación de blog, y dijo que la compañía publicitaria *«pudo explotar tanto la capacidad de detectar cuándo el contenido web es tratado de forma diferente al rastrear la prevención y las cosas malas que son posibles con dicha detección».*

Los investigadores de Google, Artur Janc, Krzysztof Kotowicz, Lukas Weichselbaum y Roberto Clapis, han detallado cinco ataques que explotan el diseño de ITP, que se basa en un algoritmo en el dispositivo para crear una lista de ITP que contiene detalles acerca de los sitios web visitados. El problema es que los sitios pueden usar la lista para descubrir información sobre los sitios web que visitan los usuarios de Safari.

> *«Cualquier sitio puede emitir solicitudes entre sitios, aumentando el número de ataques de ITP para un dominio arbitrario y obligando a que se agregue a la lista de ITP del usuario»,* dijeron los investigadores.
>
> *«Al verificar los efectos secundarios de la activación de ITP para una solicitud HTTP*

> *entre sitios determinada, un sitio web puede determinar si su dominio está presente en la lista ITP del usuario, puede repetir este proceso y revelar el estad de ITP para cualquier dominio»,* agregaron.

Google y Apple están en desacuerdo acerca de la mejor forma de proteger a los usuarios del seguimiento entre sitios. Apple introdujo ITP en Safari para MacOS e iOS en 2017, y aunque Chrome tiene una mayor participación en el escritorio, los cambios de Apple supuestamente perjudicaron a las compañías y editores de tecnología publicitaria.

Wilander dijo que Safari, Firefox, Edge basado en Chromium y Brave, implementaron alguna forma de prevención de rastreo entre sitios, pero Google Chrome no lo ha hecho.

Justin Schuh, director de ingeniería de Google Chrome, insiste en que Apple no ha resuelto los errores de ITP que Google le informó y sugiere que la función tiene fallas fatales debido a que crea problemas de seguridad y privacidad aún peores que los que fue diseñada para abordar.

> *«Este es un problema mayor que el ITP de Safari que introduce vulnerabilidades de privacidad mucho más serias que los tipos de rastreo que se supone debe mitigar. La búsqueda entre sitios y los canales secundarios relacionados que expone también son vulnerabilidades de seguridad abusivas»,* dijo Schuh.

También mencionó que se presentan problemas paralelos con el XSS Auditor de Chrome, una característica de seguridad de hace 10 años que detecta ataques de secuencias de comandos en sitios cruzaros.

Google dijo en julio que eliminaría la función en parte porque introdujo muchas *«filtraciones de información entre sitios»*, y Google descubrió que *«arreglar todas las filtraciones de información ha resultado difícil».*

> *«Para agregar algo de contexto, se descubrió que el Auditor XSS de Chrome introducía exactamente la misma clase de vulnerabilidades de canal lateral. Después de varias idas y venidas con el equipo que descubrió el problema, determinamos que era inherente al diseño y tuvimos que eliminar el código»*, escribió Schuh.