Mozilla comenzó a implementar una nueva función de seguridad para su navegador web Firefox, en canales nightly y beta, que tiene como objetivo proteger a los usuarios contra una nueva clase de ataques de canal lateral de sitios maliciosos.

Nombrada como *«Aislamiento del sitio»,* la implementación carga cada sitio web por separado en su propio proceso de sistema operativo, y como resultado, evita que el código no confiable de un sitio web malicioso acceda a información confidencial almacenada en otros sitios.

> *«Este rediseño fundamental de la arquitectura de seguridad de Firefox amplía los mecanismos de seguridad actuales al crear límites a nivel de proceso del sistema operativo para todos los sitios cargados en Firefox para escritorio. Aislar cada sitio en un proceso de sistema operativo separado hace que sea aún más difícil para los sitios maliciosos leer los datos secretos o privados de otro sitio»*, dijo Mozilla en un comunicado.

La motivación para el aislamiento del sitio se remonta a enero de 2018 cuando se revelaron públicamente las vulnerabilidades de Spectre y Meltdown, lo que obligó a los proveedores de navegadores y fabricantes de chips a incorporar defensas para neutralizar los ataques que podrían romper los límites entre diferentes aplicaciones y permitir que un adversario lea las contraseñas, claves de cifrado y otra información valiosa directamente desde la memoria del núcleo de una computadora.

Es preocupante que estos ataques de canal lateral de sincronización se puedan lanzar de forma remota a través de sitios web que ejecutan código JavaScript malicioso, lo que requiere que los fabricantes de navegadores, incluido Mozilla, ofrezcan mitigaciones al reducir la precisión de las funciones de medición del tiempo. Sin embargo, los parches actuales para Spectre han sido una «curita» y no ofrecen protección contra todas las variantes teóricas de los ataques.

> *«A pesar de reducción de seguridad existentes, la única forma de proporcionar protecciones de memoria necesarios para defenderse de Spectre, es confiar en las garantías de seguridad que vienen con el aislamiento de contenido de distintos sitios mediante la separación del proceso del sistema operativo»*, dijo Anny Gakhokidze, de Mozilla.

De esta forma comenzó la iniciativa de Mozilla para el aislamiento de sitios en abril de 2018 bajo el nombre de Project Fission. Aunque la arquitectura actual de Firefox permite que el proceso principal privilegiado genere ocho procesos de contenido web, también podría abrir la puerta a un escenario en el que dos sitios web completamente diferentes terminen en el mismo proceso, y por lo tanto, compartan la memoria del proceso, poniendo así sitios web legítimos en riesgo de ataques de ejecución especulativa.

Esto también significa que una página web que viene incrustada con múltiples subtramas de distintos sitios (por ejemplo, espacios publicitarios en páginas web), compartirá la misma memoria de proceso, lo que a su vez permitirá que un sitio de nivel superior obtenga secretos de un subtrama incrustado que no debería tener acceso en primer lugar.

Entonces entra en juego Site Isolation. Carga cada sitio web en su propio proceso, sin mencionar los que están incrustados en la página, y aísla su memoria entre sí, lo que dificulta que un dominio malicioso acceda a la información ingresada en un dominio diferente.

Además de fortalecer la seguridad de Firefox al ofrecer separación de procesos a nivel de sistema operativo para cada sitio, también se espera que Site Isolation brinde otros beneficios de rendimiento, incluido el uso eficiente del hardware subyacente y una estabilidad mejorada, ya que un subframe o un bloqueo de pestañas ya no afectarán otros sitios web o procesos.

Los usurios que ejecutan compilaciones de Firefox Nightly pueden habilitar la función navegando a *«about:preferences#experimental»* y marcar la casilla de verificación *«Fission (Site Isolation)»*. Quienes utilicen la versión Beta pueden hacerlo en *«about:config»* y

configurando «*fission.autostart*» en true.