Mozilla está comenzando a implementar Firefox 95 con una nueva tecnología de espacio aislado llamada RLBox, que evita que el código no confiable y otras vulnerabilidades de seguridad causen *«defectos accidentales así como ataques a la cadena de suministro».*

Nombrado como RLBox e implementado en colaboración con investigadores de la Universidad de California en San Diego y la Universidad de Texas, el mecanismo de protección mejorado está diseñado para fortalecer el navegador web contra posibles debilidades en las bibliotecas disponibles para reproducir audio y video, entre otro contenido.

Con este fin, Mozilla está incorporando *«sanboxing de grano fino»* en cinco módulos, incluido su motor de representación de fuentes Graphite, el corrector ortográfico Hunspell, el formato de contenedor multimedia Ogg, el analizador Expat XML y el formato de compresión de fuentes web Woff2.

El marco utiliza WebAssembly, un estándar abierto que define un formato de código binario portátil para programas ejecutables que se pueden abrir en navegadores web modernos, para aislar el código potencialmente inseguro, una versión prototipo del cual se envió en febrero de 2020 a usuarios de Mac y Linux.

Todos los navegadores principales están diseñados para ejecutar contenido web en su propio entorno de espacio aislado como un medio para evitar que los sitios maliciosos aprovechen una vulnerabilidad del navegador para comprometer el sistema operativo subyacente.

Firefox también implementa Site Isolation, que carga cada sitio web por separado en su propio proceso y, como resultado, bloquea el código arbitrario alojado en un sitio web fraudulento para que no acceda a información confidencial almacenada en otros sitios.

El problema con estos enfoques, según Mozilla, es que los ataques por lo general funcionan uniendo dos o más fallas que tienen como objetivo violar el proceso de espacio aislado que

contiene el sitio sospechoso y romper las barreras de aislamiento, socavando efectivamente las medidas de seguridad implementadas.

> *«La adaptación del aislamiento puede ser una labor intensa, muy propensa a errores de seguridad y requiere una atención crítica al rendimiento. RLBox minimiza la carga de convertir Firefox para utilizar de forma segura y eficiente código que no es de confianza»,* dijeron los investigadores.

RLBox tiene como objetivo aumentar la seguridad del navegador mediante el sandboxing C/C++ de terceros: bibliotecas de idiomas que son vulnerables a los ataques que interfieren con otros procesos del navegador y limitan el daño potencial.

Dicho de otro modo, el objetivo es aislar las bibliotecas en cajas de arena livianas de modo que los actores de amenazas no puedan explotar las vulnerabilidades en estos subcomponentes para afectar el resto del navegador.

> *«En vez de izar el código en un proceso separado, se copila en WebAssembly luego WebAssembly se compila en código nativo. La transformación impone dos restricciones clave al código de destino: no puede saltar a partes inesperadas del resto del programa y no puede acceder a la memoria fuera de una región específica, incluso una vulnerabilidad de día cero en cualquiera de estas bibliotecas no debería representar una amenaza para Firefox»,* dijo el ingeniero principal de Mozilla, Boby Holley.

Mozilla dijo que el sandboxing multiplataforma para Graphite, Hunspell y Ogg se incluye en Firefox 95 en las versiones de escritorio y móviles del navegador, mientras que se espera que Expat y Woff2 obtengan soporte para la función en Firefox 96.