Un investigador de seguridad descubrió que una acción tan simple como descargar un archivo HTML adjunto y abrirlo de forma local en el navegador, podría resultar en una técnica utilizada por hackers para robar archivos almacenados en la computadora de la víctima.

Barak Tawily, investigador de seguridad, compartió sus hallazgos con The Hacker News, afirmando que desarrolló con éxito un nuevo ataque de prueba de concepto contra la última versión de Firefox, al aprovechar un problema conocido por 17 años en el navegador.

El ataque aprovecha la forma en que Firefox implementa la Política de Mismo Origen (SOP) para el URI de «file://», que permite que cualquier archivo en una carpeta en un sistema tenga acceso a los archivos en la misma carpeta y subcarpetas.

Debido a que la política del mismo origen para el esquema de archivos no se ha definido claramente en el RFC por IETF, cada navegador y software lo han implementado de forma diferente, algunos tratan a todos los archivos en una carpeta como el mismo origen, mientras que otros tratan a cada archivo como un origen diferente.

Tawily dijo que Firefox es el único navegador importante que no cambió su insegura implementación de la SOP para el esquema URI de archivo y también es compatible con Fetch API sobre el protocolo de archivo.

Demostración del robo de archivos locales de Firefox

Aunque la debilidad de implementación en Firefox ya se ha discutido en Internet varias veces a lo largo de los años, esta es la primera vez que alguien crea un ataque PoC completo que pone en riesgo la seguridad y la privacidad de millones de usuarios de Firefox.

Como se muestra en el video, Tawily explotó este problema conocido en combinación con un ataque de clickjacking y un error de *«cambio de contexto»* que permitía que su código de explotación automáticamente haga lo siguiente:

- Obtener la lista de todos los archivos ubicados en la misma carpeta y subcarpetas

donde el navegador ha descargado el HTML malicioso o la víctima lo ha guardado manualmente
- Leer el contenido de cualquier archivo específico o todos, utilizando Fetch API
- Enviar los datos recolectados a un servidor remoto por medio de solicitudes HTTP

Para que los atacantes logren realizar el ataque con éxito, deben engañar a las víctimas para que descarguen y abran un archivo HTML malintencionado en el navegador web Firefox, y luego hacer clic en un botón falso para activar la vulnerabilidad.

Tawily mencionó que todas las acciones malintencionadas podrían suceder de forma secreta en segundo plano en pocos segundos, tan pronto como hacen clic en el lugar del botón en la página maliciosa.

Además, esta técnica solo permite que el archivo HTML malicioso acceda a otros archivos multimedia en la misma carpeta y subcarpetas.

En su escenario de ataque de PoC, Tawily mostró cómo un atacante puede robar fácilmente las claves secretas SSH de las víctimas de Linux, si un usuario guarda los archivos descargados en el directorio de usuarios, que también contiene claves SSH en su subcarpeta.

Firefox no parcheará la vulnerabilidad en corto plazo

El investigador informó el problema a Mozilla, a lo que la compañía respondió que *«nuestra implementación de la Política del Mismo Origen permite que todos los archivos con URL file:// puedan acceder a los archivos en la misma carpeta y subcarpetas».*

Esto significa que la compañía no tiene planes para solucionar este problema en el navegador, al menos por ahora. Tawily mencionó un enfoque alternativo para el problema:

> *«Desde el punto de vista de la seguridad, creo que esto debería abordarse en el lado de la RFC, eso debería hacer que los agentes de usuario (navegadores)*

> *implementen el enfoque más seguro y no permitan a los desarrolladores cometer tales errores que dejan al cliente expuesto a tales ataques».*

En 2015, los investigadores descubrieron una vulnerabilidad similar, pero que se podía ejecutar remotamente, en la política del mismo origen para Firefox, misma que los atacantes explotaron para robar los archivos almacenados en las computadoras de los usuarios de dicho navegador cuando hacían clic en anuncios maliciosos en sitios web.

Este nuevo ataque requiere más de ingeniería social, sin embargo, muchos usuarios de Firefox podrían ser víctimas del ataque.