Investigadores de seguridad cibernética revelaron el martes los detalles sobre una vulnerabilidad de suplantación de la barra de direcciones, que afecta a múltiples navegadores móviles como Safari y Opera Touch, dejando abierta una puerta para ataques de spear-phishing y entrega de malware.

Otros navegadores que resultan afectados son UCWeb, Yandex Browser, Bolt Browser y RITS Browser.

Las vulnerabilidades fueron descubiertas por el investigador de seguridad paquistaní, Rafay Baloch, y reportadas conjuntamente por Baloch y la compañía Rapid7 en agosto de 2020, antes de que fueran abordadas por los fabricantes de navegadores en las últimas semanas.

UCWeb y Bolt Browser siguen sin corregir el problema, mientras que Opera Mini asegura emitir una solución el 11 de noviembre de 2020.

El error se debe al uso de código JavaScript ejecutable malicioso en un sitio web arbitrario para obligar al navegador web a actualizar la barra de direcciones mientras la página todavía se carga en otra dirección elegida por el atacante.

> *«La vulnerabilidad se produce debido a que Safari conserva la barra de direcciones de la URL cuando se solicita a través de un puerto arbitrario, la función de intervalo establecido recarga bing.com:8080 cada 2 milisegundos, y por lo tanto, el usuario no puede reconocer la redirección de la URL original a la falsificada»,* dijo Rafay Baloch en su análisis.
>
> *«Lo que hace que esta vulnerabilidad sea más efectiva en Safari es que de forma predeterminada no revela el número del puerto en la URL a menos que el foco se establezca mediante el cursor»,* agregó.

En otras palabras, un atacante puede configurar un sitio web malicioso y atraer al objetivo

para que abra un enlace desde un correo electrónico o mensaje de texto falsos, lo que lleva a un destinatario desprevenido a descargar malware o arriesgarse a que roben sus credenciales.

La investigación también encontró que la versión para macOS de Safari es vulnerable al mismo error, que según Rapid7, se ha abordado en una actualización de macOS Big Sur lanzada la semana pasada.

Cabe señalar que esta no es la primera vez que se detecta una vulnerabilidad de este tipo en Safari. En 2018, Baloch reveló una falla similar de suplantación de barra de direcciones que hizo que el navegador conservara la barra de direcciones y cargara el contenido de la página falsificada a través de un retraso de tiempo inducido por JavaScript.

> *«Con la sofisticación cada vez mayor de los ataques de spear phishing, la explotación de vulnerabilidades basadas en el navegador, como la suplantación de la barra de direcciones, puede exacerbar el éxito de los ataques de spear-phishing y, por lo tanto, resultar muy letales»,* dijo Baloch.
>
> *«En primer lugar, es fácil persuadir a la víctima para que robe credenciales o distribuya malware cuando la barra de direcciones apunta a un sitio web confiable y no proporciona indicadores falsos, en segundo lugar, debido a que la vulnerabilidad explota una característica específica en un navegador, puede evadir anti-esquemas y soluciones de phishing»*, agregó.