AOL Search permite la descarga de archivos malware en los equipos

Con motivo del Black Hat Europe, Oren Hafif presentó como trabajo personal una investigación realizada utilizando el portal AOL Search, demostrando que este posee una vulnerabilidad que permite a terceras personas llevar a cabo de forma remota el ataque RFD.

El problema para el usuario es que no sospecha de cuál puede ser la finalidad de este archivo, y más teniendo en cuenta de que solo ha realizado una búsqueda y han aparecido unos resultados.

El archivo a descargar puede ser cualquiera, desde un ejecutable hasta un .zip, pasando por ejemplo por una archivo de consola. En la prueba realizada por el investigador se podía ver cómo se podía ejecutar la calculadora de un sistema operativo Windows gracias a un archivo de consola con las instrucciones suficiente. Teniendo en cuenta la capacidad que se otorga a la tercera persona implicada en el proceso, abrir la calculadora es lo más benévolo que podría suceder en este caso.

En lo referido a navegadores, todos ellos reaccionan de igual forma, y es que hay que tener en cuenta que **no se trata de un error del navegador sino que la configuración del sitio web** no es para nada la más adecuada, aunque hay que decir que uno no es vulnerable.

AOL y la vulnerabilidad RFD

Del ingles Reflected File Download, no resulta una vulnerabilidad muy común, o al menos que esté presente en sitios web y además de forma habitual. Hafif se encargó de programar un complemento para Google Chrome que evitaba que este navegador fuese vulnerable a este tipo de ataques.

Sin embargo, el problema va más allá de solo este servicio, ya que algunos investigadores han concretado que el fallo de seguridad se extiende a todos los servicios que se encuentran bajo el dominio de AOL.

Fuente: softpedia, redeszone