Descubierta vulnerabilidad de Firefox. Actualiza tu navegador hoy.

by javier - Sábado, agosto 08, 2015

http://memoriasdeunsysadmin.tk/2015/08/08/descubierta-vulnerabilidad-de-firefox-actualiza-tu-navegador-hoy/

El pasado 5 de agosto se hizo público, en un sitio de noticias de Rusia, un nuevo exploit que se aprovecha de una vulnerabilidad relacionada al visor de PDF nativo de Mozilla Firefox. La vulnerabilidad por lo tanto, NO está presente en firefox para android ni en ningún otro producto de Mozilla que no incluye esta característica.

Si bien este bug no permite ejecución de código, el exploit publicado permite inyectar un javascript dentro de archivos locales del equipo, cuya consecuencia directa es el acceso a archivos críticos de sistema. El exploit es capaz de actuar tanto en Windows como en Linux y, si bien dicho exploit no apunta a sistemas Mac, la vulnerabilidad si está presente y sería solo cuestión de que alguien intente explotarla o de que se lance un exploit similar. En el sistema de Microsoft busca archivos de configuración de varios de los clientes FTP más populares, como también subversion y algunas otras aplicaciones que le permitan subir archivos de manera remota. En linux en cambio, va derecho a buscar el /etc.passwd, que almacena la información de todos los usuarios de sistema y sus carpetas home, entre otras cosas; también busca archivos varios de historial y llaves; configuración de clientes de ftp, remmina(el cliente de escritorio remoto).

El upgrade con el fix apareció ayer 7 de agosto por lo que, si no lo tienen configurado para que actualice automáticamente, o bien si tienen una versión portable, no dejen de actualizar ahora mismo.

Algo más a tener en cuenta. Siendo que el exploit no deja huellas, se recomienda además, que cambien las contraseñas que puedan haber sido expuestas. Se estima que los bloqueadores de publicidad son muy eficientes contra este tipo de amenazas, pero aún así no se puede tener total certeza, ya que su efectividad depende de varios factores, entre ellos de los filtros usados.

---

memoriasdeunsysadmin.tk