

# Apple actualiza su sistema operativo para ordenadores

Apple [ha anunciado](#) una nueva actualización para su sistema operativo de ordenadores portátiles y de escritorio **OS X "Mountain Lion"** que alcanza la versión **10.8.3**.



¿Sus novedades? En primer lugar, incluye **soporte para Windows 8 en Boot Camp**. Esta herramienta de arranque dual también será capaz de trabajar con ordenadores **Mac con discos duro de 3 TB**.

Por otra parte, y aunque no es una característica de dimensiones enormes, el nuevo OS X admite **digitalización de tarjetas de regalo para iTunes utilizando la cámara incorporada del propio ordenador**.

El resto de avances son **mejoras de estabilidad**, incluyendo el parcheo de una URL que entorpecía el buen funcionamiento de las aplicaciones, así como cambios en Logic Pro, 2011 iMacs, las funciones de Contactos y Mensajes.

También se incluyen parches para solucionar errores en Quicktime, Ruby y el propio kernel de la plataforma, susceptibles de ser usados para una escalada de privilegios y robos de información personal, así como un problema de ejecución remota de código a través de archivos PDF y aplicaciones Java Web Start.

Esta es la primera tanda de actualizaciones que se anuncian desde la liberación de OS X 10.8.2 en septiembre pasado.

La nueva versión también trae una revisión de Safari (**Safari 6.0.3**), que mejora el desplazamiento en la página de Facebook y en el momento de realizar zoom, y acelera el rendimiento de sitios web con contenido en forma de plug-in.



Las implementaciones de seguridad en el navegador de Apple se corresponden con una serie de problemas relacionados con la aparición de alertas incorrectas que indicaban que los marcadores no se podían cambiar, con la duplicación de dichos marcadores en iOS tras editarlos en OS X, con el acceso a resultados de búsqueda sin filtrar en Google cuando los controles parentales estaban activados y con el bloqueo del sistema de restauración de la última posición.

El cambio de numeración en Safari soluciona también un **par de fallos que podían ser explotados para llevar a cabo un ataque “cross-site scripting”**.