Published on *Revista .Seguridad* (https://revista.seguridad.unam.mx)

NAVEGANDO AL DÍA

David Eduardo Bernal Michelena

Buenas prácticas

numero-09

Las actualizaciones son porciones de software que distribuye un fabricante de software para corregir errores existentes en los programas, incluyendo a los navegadores, para extender o mejorar su funcionamiento, estabilidad y compatibilidad.

Cada fabricante tiene su propia clasificación de actualizaciones, pero en general podemos dividirlas en actualizaciones de seguridad y de funcionalidad. Las de seguridad tienen el propósito de corregir errores o vulnerabilidades, además se pueden subdividir en varios niveles de importancia según la gravedad de la vulnerabilidad que corrigen. Las más importantes son aquellas que permiten a un atacante remoto ejecutar comandos en el sistema comprometido, así como las que parchan vulnerabilidades de día cero.

Si no se actualiza el navegador, se deja la puerta abierta para que alguna amenaza afecte nuestras computadoras y nuestra información, además de los problemas y limitaciones de funcionalidad, compatibilidad y eficiencia que tendrá nuestro navegador web.

Una de las organizaciones de seguridad más importantes en la investigación de vulnerabilidades de software, Secunia, publica un reporte anual que incluye pruebas y estadísticas de vulnerabilidades en los navegadores web más comunes.

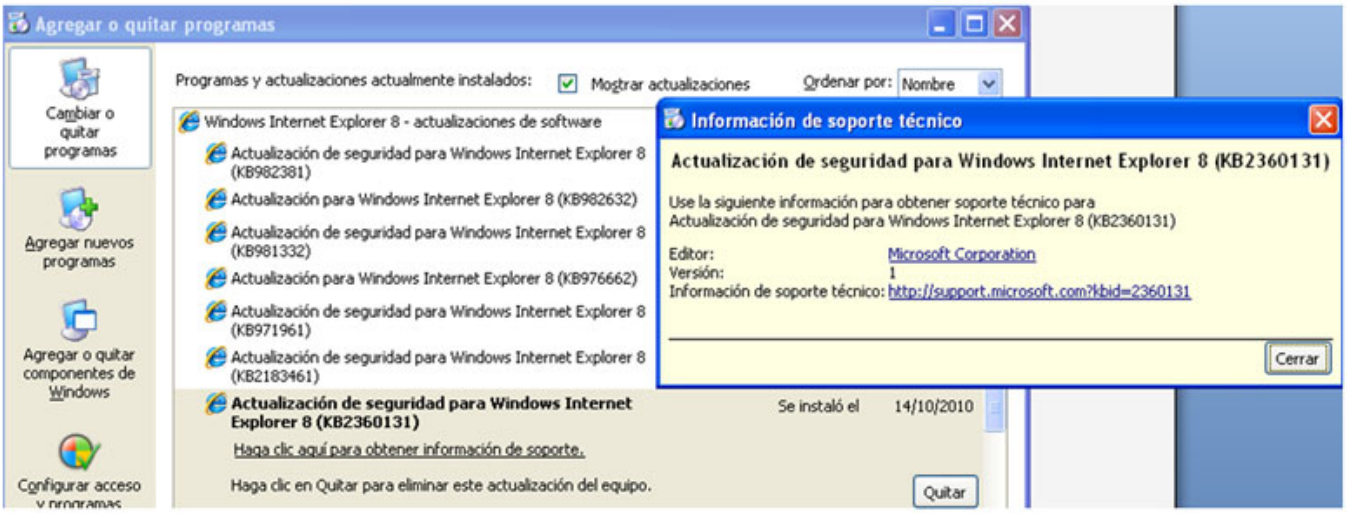
En el reporte del 2009, se indica que la mayor parte de los exploits usados a gran escala, atacan vulnerabilidades viejas, presentes en las versiones desactualizadas de los navegadores. Según el reporte, el porcentaje de navegadores no parchados de Firefox 3.0 fue de 17%, mientras que Firefox 3.5 (la versión más reciente en el 2009) fue de sólo 9.3%. Internet Explorer 6 registró 14.3%, mientras que Internet Explorer 8 sólo presentó 3.6%. La tendencia es clara, un navegador actualizado significa menos vulnerabilidades y por lo tanto, menos probabilidad de que alguien afecte la seguridad de

nuestro navegador.

Algunos fabricantes de software han implementado medidas para que sus programas se actualicen de manera automática, tal es el caso de Microsoft, con Windows Update, Mozilla Firefox, Java, Flash, entre otros. Cuando estos programas se instalan, levantan procesos que se conectan a sus servidores para buscar si hay actualizaciones disponibles, depende de la configuración, algunos las instalan automáticamente y otros presentan un botón de instalación al usuario final. Esto ayuda a que el software esté actualizado, ya que muchos no tienen la iniciativa o los conocimientos para descargar e instalar las actualizaciones manualmente.

Las actualizaciones de seguridad de Internet Explorer se pueden consultar en Agregar o quitar programas. Se selecciona Mostrar actualizaciones y luego se recorre la barra de desplazamiento hasta encontrar “Windows Internet Explorer”. Si se desea ver información más detallada sobre alguna, se selecciona la actualización y el sistema muestra un cuadro de diálogo con una liga en la que podremos ver qué problemas específicos resuelve.

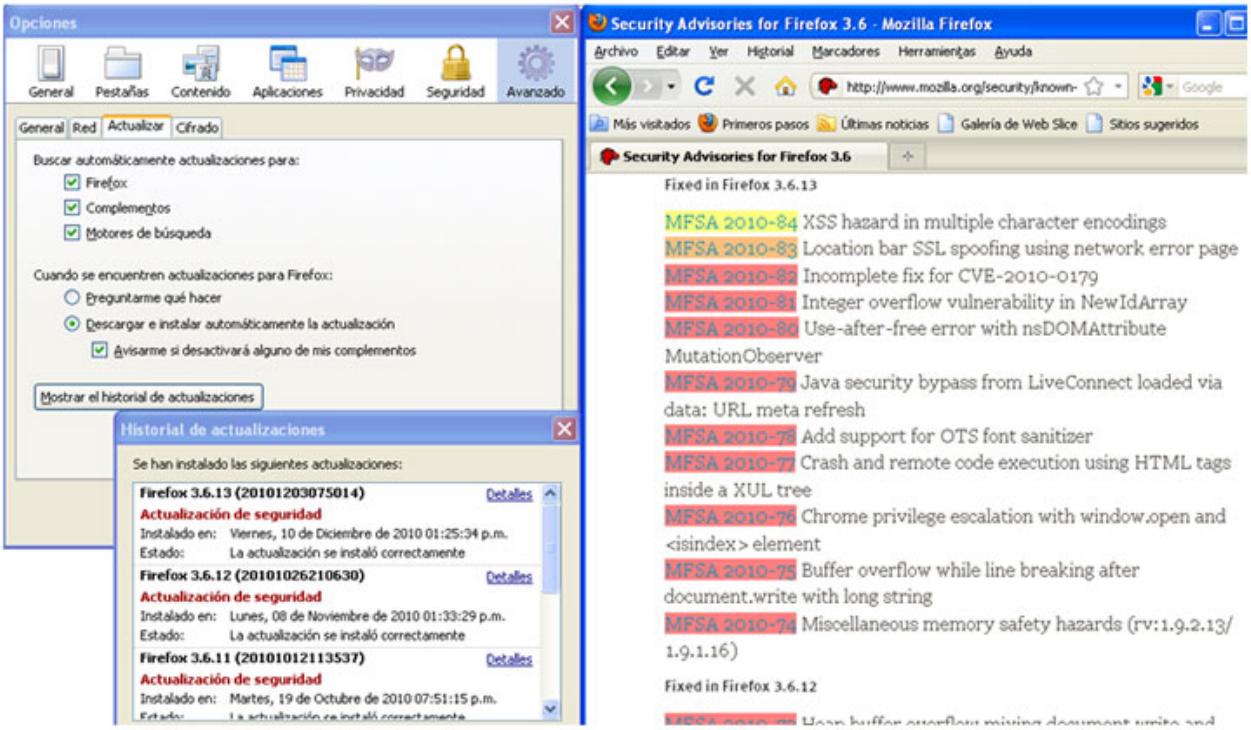
Para Mozilla Firefox, se tienen dos categorías de actualizaciones, las de seguridad y las de estabilidad. Las de seguridad corrigen vulnerabilidades en el software. Esta categoría a su vez se divide en tres:



- **Crítico:** Vulnerabilidad que puede ser utilizada para instalar software sin requerir interacción del usuario.
- **Alto:** Vulnerabilidad que puede ser usada para recopilar datos sensibles en ventanas o inyectando código, sin requerir nada más que acciones normales de navegación.
- **Moderado:** Vulnerabilidad que requiere que la víctima use configuraciones no predeterminadas o que ejecute una serie de pasos complicados o difíciles de realizar.

Estabilidad: Relacionadas con la funcionalidad, compatibilidad y estabilidad del navegador. En general, todos aquellos cambios no relacionados con la seguridad.

En este navegador podemos ver las opciones de actualización que tiene configuradas siguiendo la ruta: Herramientas>Opciones>Avanzado>Actualizar. Podremos ver las actualizaciones instaladas haciendo clic en el botón “Mostrar actualizaciones” que se encuentra en la parte inferior. Si se quieren ver los detalles que se corrigen, hacer clic en el vínculo “Detalles” ubicado en la actualización de interés:



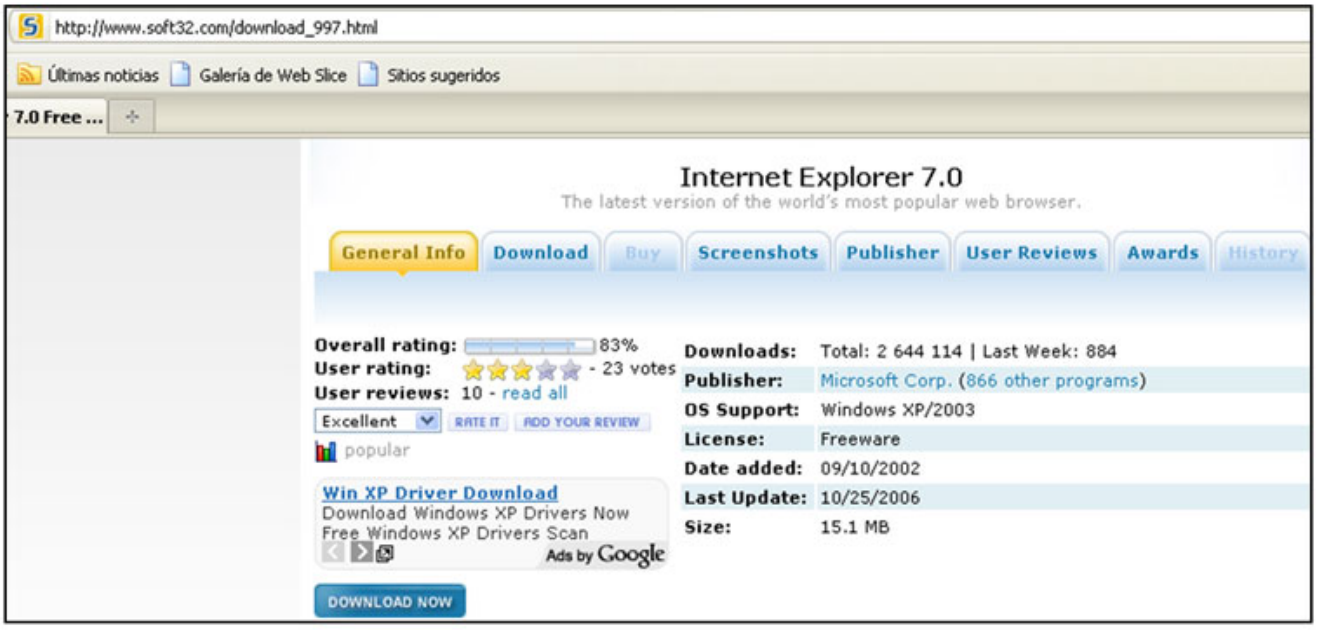
Desgraciadamente la importancia de las actualizaciones es un arma de doble filo si no somos cuidadosos, ya que al instalarlas, en vez de incrementar su seguridad pasa lo contrario, comprometen sus equipos. La pregunta entonces es: ¿cómo distinguir las actualizaciones legítimas de las falsas que son usadas por los usuarios maliciosos para propagar su malware?

Simple, sólo descargar las aplicaciones y sus actualizaciones de los sitios de las organizaciones correspondientes. En algunos casos, como al utilizar Internet Explorer, sólo será necesario que tengamos habilitado Windows Update y la versión estable más actualizada del navegador se actualizará de forma predeterminada. Si se quiere actualizar inmediatamente, se debe descargar el programa de su página. Otros navegadores como Mozilla Firefox, Google Crome y Opera se actualizan automáticamente cuando se detecta una nueva versión, lo que permite que el usuario no se tenga que molestar descargando e instalando la actualización.

Para reducir el riesgo de instalar una aplicación maliciosa, se recomienda que los programas sean descargados directamente de la organización que los desarrolla y no de páginas de terceros, ya que

versiones en otras páginas pueden ser versiones desactualizadas o peor aún, ser programas maliciosos que aparentan ser los navegadores.

A continuación se muestra una página de un tercero que permite descargar Internet Explorer 7, la cual indica incorrectamente que ésta es la versión más reciente del popular navegador web:



En caso de que la funcionalidad de actualización automática esté deshabilitada o por algún motivo no funcione, las actualizaciones también se deben descargar de la página oficial de la organización que las desarrolla. Para descargar los navegadores más populares, se debe hacer desde las siguientes URLs:

Mozilla Firefox:	http://download.mozilla.org/?product=firefox-3.6.13&os=win&lang=es-MX
Google Chrome	http://www.google.com/chrome/eula.html?hl=es
Internet Explorer (versión 8.0 estable)	http://www.microsoft.com/mexico/ie8/

Internet Explorer (versión 9.0 beta)	http://windows.microsoft.com/es-MX/internet-explorer/download/ie-9/worldwide
Opera:	http://www.opera.com/download/get.pl?id=33345&thanks=true&sub=true

Para saber si el navegador que estamos usando está en su versión estable más reciente, debemos consultar la página web del proveedor del navegador, dirigirnos a la sección de descargas y buscar el número de versión más reciente y luego compararlo con la versión de nuestro navegador, esto se puede consultar en Ayuda > Acerca de. Por ejemplo, para Mozilla Firefox haríamos lo siguiente: Entramos a http://www.mozilla.com/es-MX/firefox/ y comprobamos la versión más reciente (3.6.13):

Ahora verificamos cuál es la versión del navegador que estamos utilizando:

Algunos navegadores también permiten buscar actualizaciones en un solo paso, como es el caso de Mozilla por medio de su botón “Buscar actualizaciones” ubicado en el menú de Ayuda, pero el método explicado anteriormente es general para todos los navegadores.

REFERENCIAS:

http://secunia.com/gfx/pdf/Secunia_Annual_Report_2009.pdf
http://secunia.com/gfx/pdf/Secunia_Half_Year_Report_2010.pdf
http://www.zdnet.co.uk/news/security-threats/2010/01/18/french-german-go...
