Comparativa de Seguridad en navegadores de Internet en entornos Windows Vista o Windows 7

Versión: 1.1

19 de Abril de 2010

Informática64

Contenido

Introducción

Hacer un análisis de los mecanismos de seguridad que ofrecen una serie de productos siempre es complicado en su fase de acotación de estudio. Este documento sólo pretende ser un resumen de las características de seguridad que ofrecen los navegadores de Internet más populares en sus últimas versiones sobre las arquitecturas Microsoft Windows Vista y Microsoft Windows 7.

Este estudio se realizó desde el día 20 de Diciembre de 2009 al 20 de Enero de 2010, y revisado el día 12 de Abril de 2010, por lo que si alguna información aparece posterior a la fecha, salvo que se especifique explícitamente, ha quedado fuera del estudio.

Originalmente el artículo está basado en las versiones siguientes, salvo que se cite una versión en concreto:

- Microsoft Internet Explorer 8.0: Publicado en Marzo de 2009.
- Mozilla Firefox 3.5: Salió al mercado 3 de Agosto de 2009.
- Google Chrome 3.0: Lanzado el 12 de Octubre de 2009.
- Apple Safari 4: Lanzado en Junio de 2009.
- Opera Browser 10: Liberado en Septiembre de 2009.

Para la revisión del presente documento a fecha de 12 de Abril de 2010 ha sido necesario actualizar los siguientes navegadores a sus versiones más actuales.

- Mozilla Firefox 3.6.3: Salió al mercado 21 de Enero de 2010.
- Google Chrome 4.1: Lanzado el 17 de Marzo de 2010.
- Opera Browser 10.51: Liberado el 22 de Marzo de 2010.

En el artículo se tendrá en cuenta también el tiempo en el mercado de los navegadores, así como su cuota de mercado y la velocidad del ciclo de versiones de los mismos para evaluarlo en diferentes aspectos de seguridad.

Por supuesto, algunas de las comprobaciones están decididamente orientadas hacia el mundo empresarial en el que el control y la aplicación de directivas de seguridad crucial.

Opciones y características del navegador

Esta primera parte se centra en la configuración y uso del navegador con el sistema operativo. Como se ha dicho anteriormente, está centrado en las características de que hacen uso sobre sistemas operativos Windows Vista y Windows 7.

Arquitectura y modo de ejecución del navegador

Todos los navegadores analizados siguen un modelo de navegación basado en un interfaz divido en pestañas, sin embargo, la manera de ejecutar estas pestañas no es igual en todos. Mientras que Apple Safari, Opera Browser y Mozilla Firefox utilizan una arquitectura monolítica, Microsoft Internet Explorer 8.0 y Google Chrome hacen uso de un proceso único e independiente por cada pestaña, lo cual hace que cualquier problema, de seguridad o no, no afecte al resto de pestañas.

Mandatority Integrity Control y UIPI

Otra característica muy importante a la hora de evaluar el modo de ejecución de los navegadores es cómo interactúan con el sistema operativo haciendo uso de los "Niveles de Integridad" con los que se ejecutan. Este concepto apareció con Microsoft Windows Vista y es un mecanismo que impide que un objeto de un nivel de integridad menos privilegiado pueda acceder a un objeto de un nivel de integridad más privilegiado. Para ello se utilizan dos tecnologías: Mandatory Integrity Control (MIC) y User Interface Privilege Isolation (UIPI).

La idea es que un proceso debe correr, siguiendo el principio de Mínimo Privilegio Posible de la fortificación de sistemas, con el menor nivel de integridad. Así, si se produjera un fallo en un componente corriendo con Nivel de Integridad Bajo, este fallo no expondría los objetos del sistema corriendo en niveles de integridad superiores.

Los navegadores que siguen un modelo monolítico, es decir, que usa un proceso por programa en lugar de un proceso por cada pestaña de navegación, como son Apple Safari, Opera Browser y Mozilla Firefox trabajan con un nivel de integridad "Medio Obligatorio", mientras que Google Chrome y Microsoft Internet Explorer 8.0 levantan las pestañas con un nivel de integridad menor y usan un proceso extra controlador para cargar los componentes que necesitar un nivel de integridad superior.

Esta división hace que se hayan ajustado mucho mejor, y de forma más seguras los privilegios con los que corren cada uno de los componentes del sistema. Es decir, se ha producido una refactorización de los permisos de los componentes más singulares de los navegadores.

DEP, ASLR y Virtual Store

Protecciones adicionales como Address Space Layout Randomization (ASLR) y Data Execution Prevention (DEP) están implementadas en todos los navegadores analizados en sus últimas versiones.

DEP previene contra explotaciones que inyectan código ejecutable en parámetros pasados a procedimientos con el fin de dificultar la generación de exploits. El efecto de esta protección se ha podido ver en la mitigación del exploit denominado Aurora que se utilizó en Internet para vulnerar los navegadores de Microsoft Internet Explorer en versiones antiguas sin DEP activado.

La protección ASLR dificulta a los creadores de exploits el conocer en qué dirección de memoria se carga una determinada librería del sistema. Para ello se utiliza un factor de entropía aleatorio que, en cada ejecución, fuerza a que se cargue la librería en una determinada dirección.

Aunque ambas tecnologías tienen limitaciones en las protecciones que ofrecen resultan ser un modo efectivo de dificultar la creación de exploits en una gran cantidad de situaciones y deben ejecutarse, por seguridad, los navegadores con estas protecciones activadas.

Por último, otra característica de seguridad muy interesante, es el almacenamiento aislado que permite a las aplicaciones almacenar información en un "Virtual Store" del usuario, de modo que se incrementa la seguridad de la aplicación ya que solo ella podrá acceder a esa información y no tendrá acceso directo al registro y las carpetas sensibles del sistema. En el caso de los navegadores analizados solamente Microsoft Internet Explorer 8.0, Apple Safari y Opera Browser lo implementan.

A continuación se presenta una tabla resumen, donde se muestran los resultados obtenidos para cada navegador evaluando dichos valores con la herramienta Process Explorer, disponible en Microsoft Technet en la siguiente URL:

http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx

	DEP	ASLR	Virtual Store	Arquitectura	MIC
IE 8.0	✓	✓	✓	✓	✓
FireFox 3.6.3	✓	✓	×	×	×
Opera 10.51	✓	✓	✓	×	×
Chrome 4.1	✓	✓	×	✓	✓
Safari 4.0	✓	✓	✓	×	×

Extensiones, administración y opciones de configuración

Una de las características habituales y muy utilizadas por los usuarios, es la extensión de la funcionalidad del navegador mediante complementos. La forma de instalar los complementos, las opciones de configuración, y el uso que de ellas hace el navegador pueden suponer un riesgo de seguridad.

Salvo Apple Safari 4.0 el resto de navegadores analizados permiten extender su funcionalidad mediante complementos. Durante el proceso de instalación, todos los navegadores solicitan confirmación para instalar el complemento.

Todos los navegadores permiten visualizar los complementos instalados en el navegador, sin embargo, en el caso de Opera, no es posible la activación y desactivación de complementos de forma individual, siendo la única configuración posible la de desinstalar el complemento.

Para asegurar la procedencia de los complementos y que estos no han sido manipulados por terceros, existe la posibilidad de firmarlos digitalmente. Sólo Microsoft Internet Explorer 8.0 y Mozilla Firefox soportan los complementos firmados. En Internet Explorer esta es una política habitual, estando por defecto permitidos únicamente los complementos firmados. En Mozilla Firefox, aunque está soportado, no es lo habitual, estando la inmensa mayoría de los complementos disponibles sin firmar y no pudiendo configurar el navegador para que solo permita los firmados.

Por último, en un ámbito empresarial, es fundamental poder configurar el uso de complementos según sea el usuario que accede al navegador, permitiendo el uso de complementos a determinados usuarios y a otros no. Solamente Microsoft Internet Explorer 8.0 y Mozilla Firefox permiten este tipo de configuraciones.

	IE 8.0	FireFox 3.6.3	Opera 10.51	Chrome 4.1	Safari 4.0
	✓ Addons ActiveX	✓ Extensiones	✓ Widgets	✓ Gears *Extensiones	✗
	✓	✓	✓	✓	
	✓	✓	✓	✓	
	✓	✓	✓	✓	
	✓	✓	✗	✓	
	✓	✓	✗	✗	
	✓	✓	✗	✗	

En este apartado, una característica muy importante que ha aportado Microsoft Internet Explorer 8.0 respecto al uso que hace de los ActiveX es la posibilidad de realizar un ajuste fino de los privilegios de seguridad para poder ejecutar los componentes. Este ajuste fino permite que en situaciones de riesgo, el navegador se pueda fortificar contra amenazas externas permitiendo que internamente la aplicación no pierda ninguna característica funcional.

Supóngase una amenaza en la que una vulnerabilidad en un plug-in está siendo explotado en Internet por medio de un determinado exploit. Con estas opciones Microsoft Internet Explorer 8.0 permite restringir en que sitios se desea cargar el plug-in y que sitios se restringe su uso mediante listas blancas por sitios y por usuarios. Esta opción es única de Microsoft Internet Explorer 8 y por eso se ha sacado de la tabla comparativa. Las características son:

- Activación de componentes ActiveX por Sitio, de modo que es posible habilitarlos solo para aquellos sitios en los que se confía.

- Es posible activar componentes ActiveX en los perfiles de usuario, sin necesidad de utilizar elevación de privilegios, y ya que solo se realiza en el perfil del usuario, esto no supone un riesgo para la seguridad.

- Sistema de Logs para los ActiveX, de modo que Internet Explorer puede informar de los problemas de instalación y ejecución más comunes, como pueden ser las restricciones de seguridad que impidan la instalación de un ActiveX.

Cabe recordar, que el uso de plug-ins puede resultar un problema para la seguridad tanto por que sean componentes vulnerables como porque sean directamente malware. A pesar de que hace tiempo el primer malware para navegadores se distribuyó para Microsoft Internet Explorer 8.0, hoy en día, tal y como recoge el paper de Symantec de "Firefox y el Malware" existe malware extenso y complejo para Mozilla Firefox.

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/firefox_and_malware.pdf

Esto además hay que completarlo con situaciones en las que los propios plug-ins, aun siendo creados de forma segura, se han visto afectados en su código convirtiéndose en un programa maliciosos. Esto se ha producido por ataques a los servidores de repositorio de código en los que se ha añadido segmento de código malware. Esto, ha pasada en un par de ocasiones directamente con los plug-ins oficiales de Mozilla de Firefox haciendo que equipos actualizados desde los servidores de Mozilla se vean infectados con malware.

http://blog.mozilla.com/addons/2010/02/04/please-read-security-issue-on-amo/

http://blog.mozilla.com/security/2008/05/07/compromised-file-in-vietnamese-language-pack-for-firefox-2/

Administración por GPO y Active Directory

Otra de las características comprobadas en los diferentes navegadores es la posibilidad que oferta en una organización con Microsoft Active Directory desplegado el hacer uso de plantillas de administración de configuren, fortifiquen y administren en tiempo real las opciones de seguridad del navegador.

Mediante políticas de grupo (GPOs) es posible configurar de forma centralizada todos los aspectos del sistema operativo Windows. Es un elemento imprescindible en grandes redes corporativas, y en el caso de Microsoft Internet Explorer también es posible la configuración mediante estas GPOs de absolutamente todas las opciones de seguridad. Así, en caso de necesidad de un cambio en la política de seguridad contra una situación de amenaza activa, se dispone de una herramienta rápida y flexible para la fortificación de los navegadores. La configuración puede ser establecida por usuario y por máquina permitiendo fortificar tanto entornos de ejecución como características de uso en función de las necesidades de los usuarios.

	IE 8.0	FireFox 3.6.3	Opera 10.51	Chrome 4.1	Safari 4.0
Administración mediante GPO	✓	✓1	✘	✘	✘

- Ninguno de los otros navegadores viene preparado de serie para este funcionamiento ni con Microsoft Active Directory ni con ningún otro directorio empresarial, sin embargo, es posible administrar Mozilla Firefox con GPOs mediante el uso de plantillas descargables. Estas plantillas, por tanto, requerirían de administración añadida e instalación aparte.

Servidor Web y Aplicaciones

Este apartado está centrado en las medias de seguridad que añaden los diferentes navegadores contra los ataques que se producen al conectarse a aplicaciones web inseguras o maliciosas que atacan al cliente.

Control de Sesiones y cookies

El servidor Web y el navegador se comunican mediante el Protocolo HTTP, realizándose solicitudes y respuestas HTTP. El protocolo HTTP no mantiene estado, es decir, cada petición y su correspondiente respuesta es manejada como una transacción aislada. Por lo tanto, un servidor Web no es capaz de distinguir si las peticiones vienen o no desde el mismo cliente.

Para ello, en las aplicaciones Web, se hace uso de sesiones, como mecanismo para asociar las diferentes peticiones que provienen de un mismo cliente. Una sesión empieza cuando un

cliente no reconocido por la aplicación realiza la primera petición al Servidor Web y finaliza cuando el cliente la termina o expira el tiempo de vida, debido a que pasa un tiempo determinado sin que el cliente realice una petición.

Existen dos mecanismos para mantener las sesiones, que son la sobre escritura de la URL y las cookies. La sobre escritura de la URL cada vez se utiliza menos debido a que la información queda almacenada en demasiados ficheros de log y permite un acceso mucho más sencillo a ella por terceros por lo que la tendencia global es recurrir al uso de cookies. Además, las cookies permiten al desarrollador de las aplicaciones Web introducir información adicional a la relativa al mantenimiento de la sesión. La responsabilidad en la forma de generar identificadores de sesión y la información almacenada en las cookies recae en los desarrolladores de las aplicaciones. Sin embargo, el navegador es responsable de la gestión y administración de las cookies, así como de impedir que las páginas puedan acceder a cookies que no pertenecen a su dominio entre otras acciones.

Las cookies se establecen y viajan a través de las cabeceras HTTP y además del nombre y valor permiten especificar determinadas características de seguridad, que son la fecha de expiración a partir del cual no deben ser enviadas (expire), el domino para el cual son válidas (domain), la ruta de la aplicación donde es válida (path), y la obligatoriedad de enviarla solo si la conexión es HTTPS.

Para evitar el robo de la sesión (Session Hijacking) mediante ataques de Cross Site Scripting (XSS) se acordó el uso del flag HTTPOnly, que impide el acceso a la cookie desde el navegador, siempre y cuando este lo soporte

Usando la página http://greebo.net/owasp/httponly.php para el test httpOnly y una página propia para el control de los otros atributos de las cookies este es el comportamiento de los diferentes navegadores:

	SECURE	EXPIRES	DOMAIN	PATH	HttpOnly		
					READ	WRITE	AJAX
IE 8.0	✓	✓	✓	✓	✓	✓	✓
FireFox 3.6.3	✓	✓	✓	✓	✓	×	✓
Opera 10.51	✓	✓	✓	✓	✓	×	✓
Chrome 4.1	✓	✓	✓	✓	✓	×	✓
Safari 4.0	✓	✓	✓	✓	✓	×	✓

Como se puede ver en el cuadro anterior, actualmente solo Microsoft Internet Explorer 8.0 ofrece un soporte completo al flag HttpOnly, si bien, el resto de navegadores al impedir su lectura tanto mediante javascript como mediante los objetos AJAX, no es posible realizar el robo de sesión.

Cross Site Scripting (XSS)

Mediante los ataques de Cross Site Scripting (XSS) no sólo es posible tratar de robar la cookie de sesión que mantienen aplicación Web y navegador, también es posible manipular el código HTML que devuelve la aplicación Web para cambiar el aspecto que presenta la página, o añadir funcionalidad "maliciosa" para intentar, por ejemplo, robar credenciales en un formulario de login.

Aunque deben ser los desarrolladores de la aplicación Web quienes controlen que su página no sea vulnerable a XSS, los navegadores pueden incorporar funcionalidad que eviten que una página ejecute scripts que provengan de un dominio distinto al de la página que se visite. De este modo se evita que un atacante inyecte, a través de un enlace malicioso enviado a la víctima, toda una serie de comandos Javascript que desemboquen en el robo de la información que la víctima introduce en esa página manipulada. Actualmente sólo Microsoft Internet Explorer 8.0 incorpora un filtro de este tipo.

	IE 8.0	FireFox 3.6.3	Opera 10.51	Chrome 4.1	Safari 4.0
Filtro XSS	✓	✗	✗	✗	✗

Existe, para Mozilla Firefox, un plug-in llamado NoScript con funciones anti-XSS para Mozilla Firefox. Al igual que en el caso del plug-in de interacción con Microsoft Active Directory, representa un componente extra a añadir a las instalaciones de Mozilla Firefox que no viene por defecto instalado en los navegadores, luego exige de una carga extra de trabajo, administración y control a tener en cuenta.

Clickjacking

Desde hace unos años, una de las vulnerabilidades más explotadas es el clickjacking, el cual puede considerarse una evolución del Cross Site Request Forgey (CSRF), mediante el cual, y

haciendo uso de un Iframe se carga una página que requiere de autenticación (el usuario debe haberse validado antes) y se autoriza la acción mediante un clic (la diferencia con CSRF). A lo largo del año 2009, sitios como Twitter o Facebook han adolecido de estas vulnerabilidades.

Para mitigar esta vulnerabilidad Microsoft propuso una solución, el uso de la cabecera HTTP X-FRAME-OPTIONS, que tomaría los valores DENY y SAMEORIGN, que bloquearían la carga de la página en cualquier frame o en frames de sitios externos.

A continuación se muestra una tabla indicando si los navegadores cuentan, o no, con soporte la cabecera X-FRAME-OPTIONS:

	IE 8.0	FireFox 3.6.3	Opera 10.51	Chrome 4.1	Safari 4.0
Anti-clickjacking	✓	✗	✓	✓	✓
X-FRAME-OPTION					

Cross Domain Request

Una de las desventajas con las que se encuentran los desarrolladores de aplicaciones Web que utilizan AJAX, consiste en que no es posible realizar peticiones AJAX a recursos que se encuentren en otros dominios. Para solventar este inconveniente desde la W3C se extiende el objeto XMLHttpRequest para permitir peticiones a otros dominios (http://www.w3.org/TR/cors/), mientras que por parte de Microsoft en su IE8 se crea el objeto XDomainRequest (http://msdn.microsoft.com/en-us/library/cc288060(VS.85).aspx) cuya funcionalidad es equivalente.

Para evitar ataques XSS que utilicen esta característica para que una página pueda ser llamada mediante uno de estos objetos es necesario que el programador lo permita mediante las cabeceras "Access-Control-*", que permiten definir que dominios pueden llamar a la página, si es necesario usar credenciales, o que métodos HTTP son los permitidos.

Las cabeceras más importantes son Access-Control-Allow-Origin donde se especifican los dominios que pueden llamar mediante AJAX a la página.

En la siguiente tabla se muestra el soporte de los navegadores a Cross Domain Request, y si implementan o no las caberas especificadas.

	IE 8.0	FireFox 3.6.3	Opera 10.51	Chrome 4.1	Safari 4.0
Soporte a Cross Domain Request	✓	✓		✓	✓
Limitación por Sitios de Origen	✓	✓	×	✓	✓

Ingeniería Social

El siguiente grupo de comprobaciones va dedicado a las herramientas que ofrecen los diferentes navegadores frente a los ataques, cada día más comunes, de ingeniería social. Debido al uso intensivo por parte de la sociedad de Internet y la aparición de herramientas de conexión de vida personal, es cada vez más común el uso de tretas de ingeniería social para engañar a los usuarios menos especializados en seguridad.

Resaltado del dominio

Una de las técnicas más extendías para realizar Phishing es intentar engañar al usuario haciendo uso de URLs mal escritas o utilizando subdominios, que hacen creer al usuario que se encuentra en el sitio Web, cuando realmente están en otro.

Para ayudar a los usuarios a identificar rápidamente en que dominio se encuentra, algunos navegadores resaltan de alguna forma el dominio en que se encuentra el usuario, tratando de evitar así la suplantación de un sitio Web.

	IE 8.0	FireFox 3.6.3	Opera 10.51	Chrome 4.1	Safari 4.0
Resaltado del dominio	✓	×	×	✓	×

Solo Internet Explorer 8 resalta el dominio al que navega el usuario, Chrome, por su parte, resalta el nombre del host por completo, pero eso implica que direcciones como "www.facebook.com.it.tk/myperfil.asp" no serían identificadas rápidamente por el usuario como un sitio fraudulento.

Alertas sobre certificados

Mediante el uso de SSL (Secure Socket Layer – Protocolo de conexión segura) se busca garantizar a autenticidad de un sitio Web (y así evitar phising) y la confidencialidad en la comunicación. Para asegurar la identidad del sitio se utiliza un certificado digital de Servidor. En última instancia la autenticidad se basa en la confianza que el usuario y/o máquina tiene en el certificado del servidor, por lo que el certificado debe haber sido generado por una entidad certificadora de confianza, incluida en el sistema operativo y navegadores del cliente

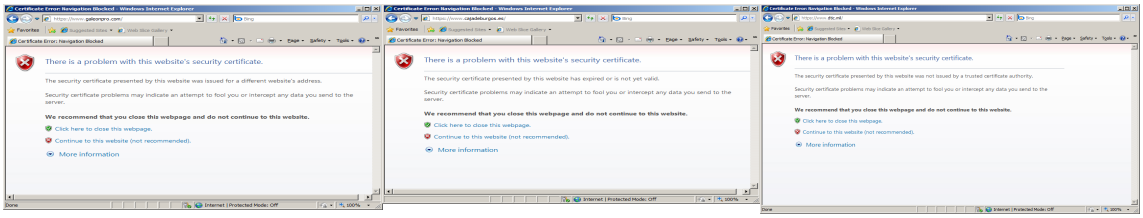
Cuando el usuario está navegando por la red y accede a un sitio con SSL, el navegador debe informar, lo mejor posible, al usuario del certificado que le ofrece el servidor. Indicando si este ha sido generado por una entidad de confianza, si fue generado para el sitio web que está visitando o no, si está caducado, etc. De modo que el usuario pueda decidir si continua o no navegando.

En el siguiente cuadro resumen se indica si los navegadores alertan a los usuarios de estas situaciones:

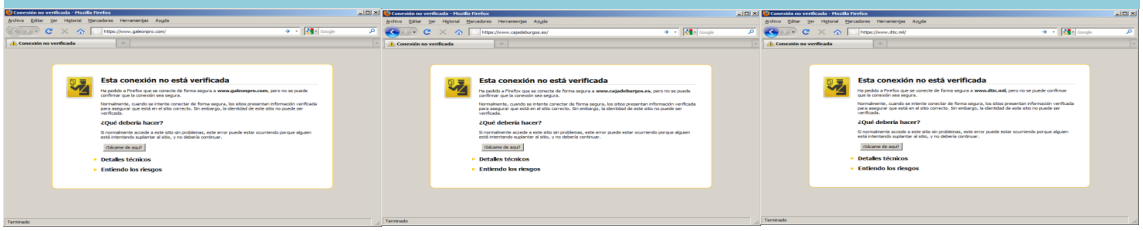
	IE 8.0	FireFox 3.6.3	Opera 10.51	Chrome 4.1	Safari 4.0
Certificado generado para otro dominio	✓	✓	✓	✓	✓
Certificado caducado	✓	✓	✓	✓	✓
Certificado emitido por CA desconocida	✓	✓	✓	✓	✓

Todos los navegadores analizados alertan al usuario de estar circunstancias, además todos lo hacen de semejante modo, mediante un mensaje que ocupa toda la pantalla del navegador, excepto Opera y Safari que genera alertas mediante un dialogo modal. A continuación se muestran las capturas de pantalla de los diferentes navegadores al acceder a sitios cuyos certificados están emitidos para otro dominio, han caducado o han sido emitidos por entidades certificadoras desconocidas.

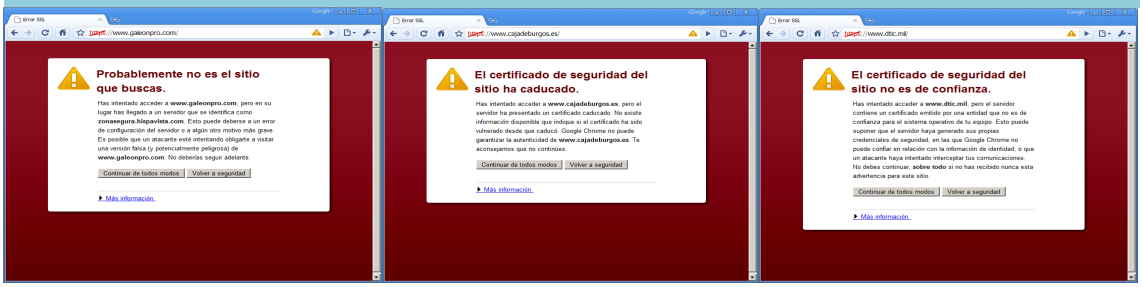
IE 8.0



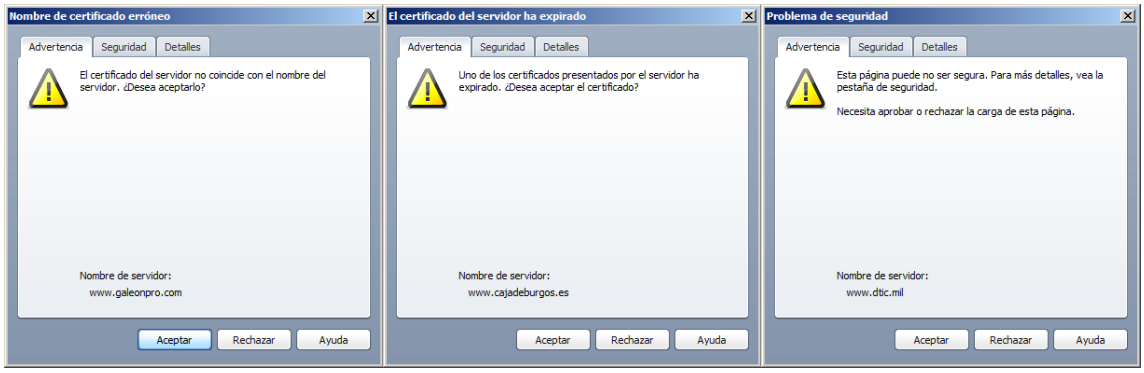
Firefox 3.6



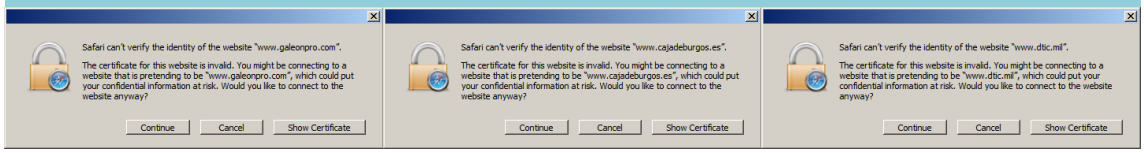
Chrome 4



Opera 10



Safari 4.0



Certificados con validación extendida

La generación de certificados de servidor por parte de las entidades certificadoras (CA) consisten en un proceso automatizado, donde el nivel de verificación de la identidad del solicitante del certificado es bastante bajo. Para subsanar estas deficiencias se han creado los certificados de validación extendida (EV).

Los certificados EV son un tipo especial de certificado X.509 que requieren una investigación más concienzuda de la entidad solicitante por parte de la entidad certificadora antes de generarlo, según se especifica en las “Directrices para los certificados de validación extendida” (http://www.cabforum.org/Guidelines_v1_2.pdf).

Los navegadores deben soportar este tipo de certificados y distinguir si la conexión SSL que se establece a un servidor cuenta con un certificado digital normal o EV, y en consecuencia, informar de ello al usuario de alguna manera.

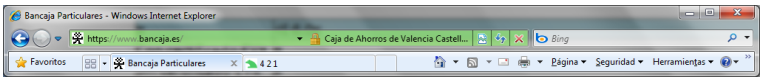
En el siguiente cuadro se indica si los navegadores analizados permiten informar al usuario, de forma visual, si el sitio web al que está conectado mediante SSL utiliza un certificado EV o no.

	IE 8.0	FireFox 3.6.3	Opera 10.51	Chrome 4.1	Safari 4.0
Resaltado de los certificados con VE	✓	✓	✓	!	!

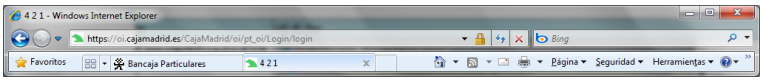
IE coloca la barra de navegación en verde si se trata de un certificado extendido, Firefox y Opera cambian el color del certificado, sin embargo, Chrome y Safari únicamente muestran o no el texto correspondiente a la entidad certificadora, siendo "difícil" averiguar a primera vista si se trata de un certificado EV o no. A continuación se muestran capturas de pantalla de cada uno de los navegadores:

IE 8.0

Con certificado EV



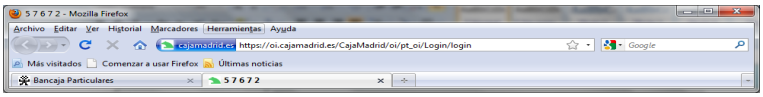
Sin certificado EV



Firefox 3.5

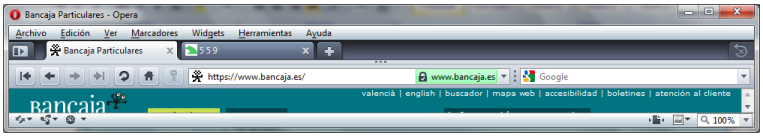
Con certificado EV

Sin certificado EV

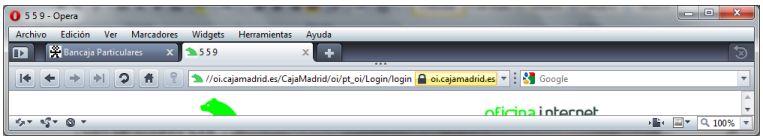


Opera 10

Con certificado EV

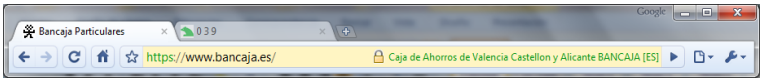


Sin certificado EV

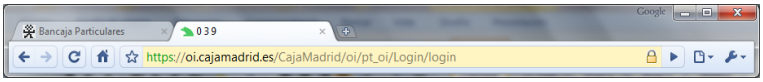


Chrome 3.0

Con certificado EV

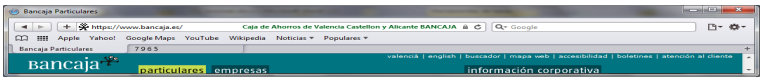


Sin certificado EV

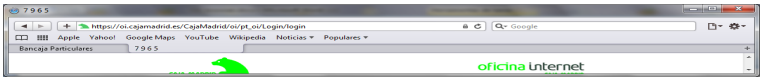


Safari 4.0

Con certificado EV



Sin certificado EV



Como se ha demostrado durante el año 2009 en conferencias de seguridad informática, la aparición de vulnerabilidades en la generación automática de certificados digitales puede provocar ataques de Man In The Middle. Los certificados EV ayudan a mitigar el impacto de estos permitiendo al usuario identificar sitios seguros.

Almacén de certificados

Tanto para certificados “normales” como para los certificados de validación extendida, el navegador los identifica como válidos cuando estos han sido generados a partir de una entidad emisora de certificados de confianza.

Cada navegador, por lo tanto, utiliza un almacén de certificados donde mantiene los certificados de las entidades raíz en los que confían. La pregunta entonces parece obvia, ¿Qué certificados raíz de confianza deben incluir los navegadores?

En el caso de España, bajo las normas de la comisión europea, está obligada a publicar los nombres de todos los prestadores de Servicios de Certificación nacionales acreditados (http://ec.europa.eu/information_society/policy/esignature/eu_legislation/trusted_list/index_en.htm). Por ello, el gobierno español tiene publicada la lista de prestadores de servicios de certificación de firma electrónica (https://www11.mityc.es/prestadores/busquedaPrestadores.jsp)

Para este listado, y recogiendo sólo aquellos prestadores que emiten certificados de servidor seguro, y por lo tanto, certificados válidos para autenticar a un servidor Web, se analiza, para los diferentes navegadores, si consideran o no seguros los sitios web autenticados mediante certificados emitidos por estas entidades.

	IE 8	Firefox 3.6.3	Chrome 4.1	Opera 10.51	Safari 4.0
AC ABOGACÍA	✔	✘	✔	✘	✔
ANCERT	✔	✔	✔	✘	✘
ACCV	✔	✘	✔	✘	✔
CAMERFIRMA	✔	✔	✔	✘	✔
CATCert	✔	✘	✔	✘	✔
FNMT-RCM	✔	✘	✔	✘	✘
Firmaprofesional	✔	✔	✔	✘	✔
HEALTHSIGN	✘	✘	✘	✘	✘
Izenpe, S.A	✔	✘	✔	✔	✔

En este cuadro se puede comprobar, como entidades emisoras de certificados, tan conocidas y utilizadas en España, como la FNMT, no son incluidas en las almacenes de certificados de

Mozilla Firefox, Opera Browser o Apple Safari. Por lo que el acceso a cualquier sitio web cuyo certificado haya sido expedido por ella es considerado no seguro.

Protección ante Phishing y Malware

Hoy en día, una de las formas más comunes de distribuir el Malware es utilizar sitios infectados, de modo que aprovechando las vulnerabilidades de los navegadores o la inocencia de los usuarios, infectan los equipos clientes con la simple visita al sitio o gracias a la descarga de contenido maliciosos.

Para ayudar a proteger a los usuarios del phishing y del malware descargado de sitios maliciosos, los navegadores incorporan características para detectar si la página web que visita el usuario esta notificada como sitio de phishing o si el software que se descarga se considera malintencionado.

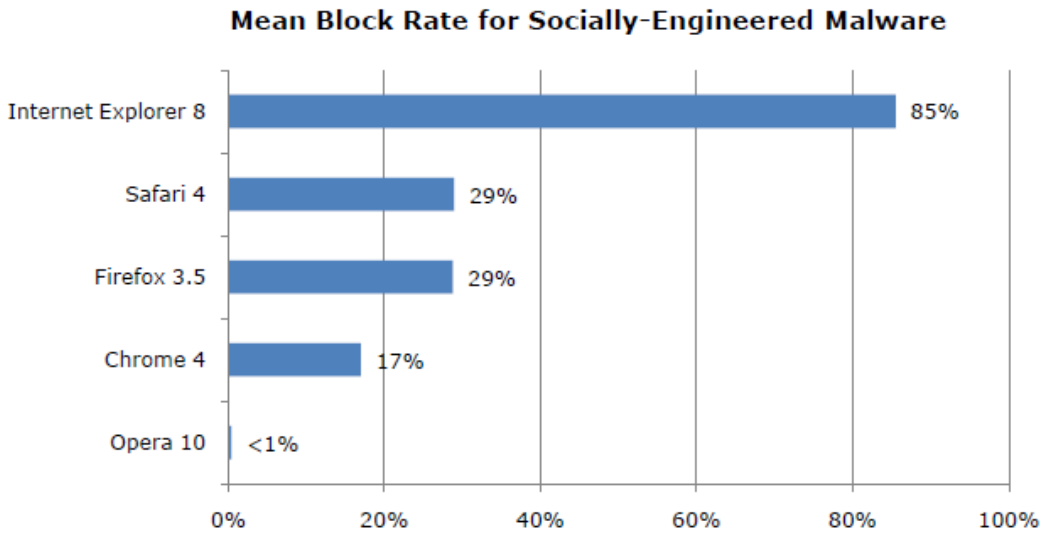
A continuación se muestra una tabla resumen donde se especifica si el navegador incluye estas características y el servicio que utilizan

	IE 8.0	FireFox 3.6.3	Opera 10.51	Chrome 4.1	Safari 4.0
Protección ante Phishing y Malware	✓ Filtro SmartScreen	✓ Google Safe Browsing	✓ PhishTank y GeoTrust	✓ Google Safe Browsing	✓ Google Safe Browsing

Dado que, actualmente, todos los navegadores analizados cuentan con mecanismos de protección ante phishing y malware, es necesario analizar la eficacia de estas medidas. Para ello NSS Labs publicó, en Febrero de 2010, un estudio sobre la detección de malware de los diferentes navegadores, aunque las versiones no corresponden exactamente con las aquí analizadas, se trata del estudio más reciente publicado hasta la fecha y permite ver el esfuerzo que realizan los diferentes laboratorios para proteger a sus usuarios. El estudio es accesible a través de esta dirección:

http://nsslabs.com/test-reports/NSSLabs_Q12010_GTRBrowserSEM_FINAL.pdf

A continuación se muestra un cuadro resumen de los resultados obtenidos por este estudio:



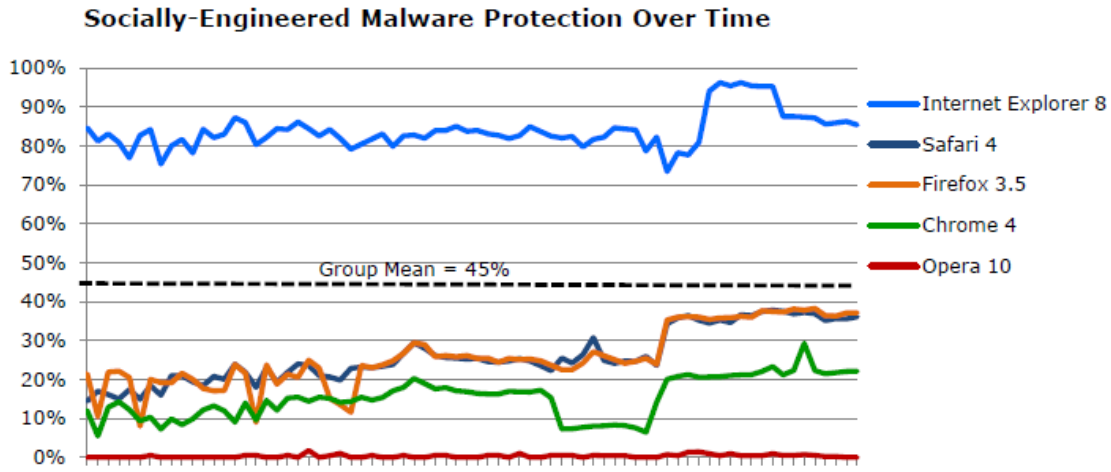
Algo muy importante a tener en cuenta en los Sistemas de detección de malware, es el tiempo, tiempo medio de respuesta de los navegadores a la hora de bloquear el malware.

En este estudio se muestra, por un lado, el tiempo medio que un usuario debe esperar hasta que un navegador añade a su listado de sitios bloqueados una URL maliciosa, una vez que se ha introducido en el conjunto de pruebas:

Browser	Average Add Time (Hours)
Firefox 3.5	5.7
Internet Explorer 8	6.7
Safari 4	9.0
Chrome 4	14.7
Opera 10	82.4
Mean	*23.7*

En la tabla se puede ver, como es Firefox 3.5, el navegador que de media tarda menos en incluir la URL en el listado de sitios maliciosos. Internet Explorer 8 se mantiene un poco por encima, al igual que Safari 4, por su parte Chrome 4 aumenta ya significativamente el tiempo, y por último, Opera 10 tarda excesivo tiempo en incluir las URL de malware en el listado de sitios maliciosos.

En el estudio, se indica como la métrica de bloqueo de URL individuales representa únicamente una perspectiva del problema, por ello, muestran un estudio en el cual analizan un conjunto de direcciones URL vivas durante 18 días, en 74 ciclos de test por cada uno de los cinco navegadores, con el objetivo de evaluar los criterios utilizados para mantener o eliminar las URL maliciosas de los listados de malware. Cada puntuación de la gráfica representa el nivel de protección en un punto dado en el tiempo:



En la gráfica se observa como Internet Explorer 8 mostro un nivel muy alto de protección. Mozilla Firefox y Apple Safari han oscilado entre el 20% y 40%. Google Chrome 4 y Opera Browser 10 obtuvieron resultados más pobres.

Privacidad

El siguiente apartado está dedicado a las opciones de privacidad que tiene un usuario a la hora de utilizar un determinado navegador.

Gestión de la información de navegación

Durante la navegación por Internet los navegadores almacenan una gran cantidad de información, tal como las direcciones visitadas, las cookies utilizadas en las diferentes sesiones, el texto introducido en formularios, etc...

En este apartado se analizan las diferentes opciones que soportan los navegadores en cuanto a la posibilidad de eliminar esta información, de forma conjunta o por separado, en esta tabla se muestra también la posibilidad de navegar en modo privado, es decir, la posibilidad de visitar sitios web de modo que al cerrar el navegador no quede rastro de las actividades realizadas.

Por último, debido a que las compañías que proporcionan contenido a sitios web, a menudo recolectan información sobre la gente que los visita, es posible que si cruzan la información de todos los sitios puedan obtener información valiosa sobre los usuarios que navegan por ellas. Se indica en la tabla si el navegador incorpora algún mecanismo para evitarlo.

	IE 8.0	FireFox 3.6.3	Opera 10.51	Chrome 4.1	Safari 4.0
Borrado individualizado de datos privados	✓	✓	✓	✓	✓
Posibilidad de eliminar al terminar navegación	✓	✓	✓	✓	✘
Políticas de privacidad por zonas			✓ ✘		
[1]	✘			✘	
Navegación en modo privado	✓ InPrivate Browsing	✓ Navegación Privada	✓ Navegación Privada	✓ Modo Incognito	✓ Navegación Privada
Bloqueo de envío de información	✓ InPrivate	✘ Add-on	✘ Add-on	✘ Add-on	✘ Add-on

1 Opera Browser permite personalizar la configuración para cada sitio. Si se desean configurar muchos sitios no es una forma muy cómoda de hacerlo.

	✘			✘	
a terceros	Blocking	AdBlock	AdBlock	AdSweep	AdBlock
Gestor de Cookies	✘	✓	✓	✓	✓
Gestor de Contraseñas	✓	✓	✓	✓	✓

Configuración de JavaScript

JavaScript es el lenguaje utilizado, principalmente, en las aplicaciones web para el desarrollo de interfaces de usuario mejoradas y dotar de mayor dinamismo a las páginas web. Aunque las posibilidades de JavaScripts son limitadas, ya que no tienen acceso a recursos externos al navegador y tiene limitado el acceso a objetos potencialmente peligrosos – y en otras ocasiones con la necesidad de confirmación por parte del usuario como por ejemplo en el acceso al portapapeles -, el uso del Javascript es la fuente de las que se alimentan ataques tales como el Cross Site- Scripting (XSS).

Mediante el uso de JavaScript y aprovechando vulnerabilidades de las aplicaciones, el atacante puede cambiar el aspecto de la aplicación o cambiar su comportamiento. Es por lo tanto, una opción recomendable de seguridad la posibilidad de desactivar el lenguaje JavaScript, y más aun interesante, la posibilidad de controlar exactamente que opciones se permiten y cuáles no. A continuación se muestra un cuadro resumen con las presencia o no de estas opciones en los diferentes navegadores.

	IE 8.0	FireFox 3.6.3	Opera 10.51	Chrome 4.1	Safari 4.0
Deshabilitación de JavaScript	✓	✓	✓	✓	✓
Configuración avanzada de JavaScript	✓	✓	✓	✘	✘

De Google Chrome y Apple Safari destaca la imposibilidad de configurar por diferentes tipos de zonas, sitios o reglas de usuarios.

Vulnerabilidades

Los navegadores, como cualquier otro software, sufren a lo largo de su ciclo de vida, una serie de vulnerabilidades o problemas que pueden permitir a un atacante violar pilares fundamentales de la seguridad, tales como la confidencialidad, integridad, disponibilidad, etc.

En este apartado se recurre a la base de datos de Secunia, donde se publican todas las vulnerabilidades de los diferentes navegadores catalogados por nivel de criticidad. En este repositorio de información se muestra también si existe solución o parche para dichas vulnerabilidades, ya que para un navegador es, tanto o más importante que tener pocas vulnerabilidades, el ser capaz de resolverlas y publicar las actualizaciones adecuadas con la mayor celeridad posible.

El repositorio de Secunia, está organizado en torno a los "Secunia Advisories", donde se indica la fecha de publicación, el nivel de criticidad, el vector de ataque, el impacto, y accediendo al advisory, se pueden comprobar las vulnerabilidades a las que se refiere, incluyendo el código CVE (Common Vulnerabilities and Exposures) de la vulnerabilidad.

Los "Secunia Advisores" están clasificados de acuerdo a 5 niveles de criticidad, que son: Extremely Critical, Highly Critical, Moderately Critical, Less Critical y Not Critical. La diferencia entre ellas es catalogada por Secunia siguiendo el criterio publicado en su web:

http://secunia.com/community/advisories/terminology/

En las tablas de resultado se ha seguido el siguiente código de colores:

Extremely Critical	Highly Critical	Moderately Critical	Less Critical	Not Critical

Comparar vulnerabilidades entre navegadores que han sido publicados en diferentes instantes de tiempo siempre es complicado. Microsoft Internet Explorer 8 fue publicado el 19 de Marzo de 2009 mientras que Mozilla Firefox fue publicado en Junio de 2009 o Google Chrome que fue publicado ya en el año 2010. Contar vulnerabilidades por tiempo puede suponer también una métrica difícil de justificar ya que, elegido el tiempo a priori puede afectar a muchas versiones

del mismo navegador. Debido a ello se ha hecho una contabilidad de vulnerabilidades de compromiso donde se ha escogido un número de versión más o menos similar en arquitectura y que permita realizar un conteo aproximado para tener una estimación del número de vulnerabilidades media.

A continuación se presentan las vulnerabilidades de cada uno de los navegadores según el repositorio de Secunia, ordenados por fechas, y analizando desde las siguientes versiones.

Google Chrome

La siguiente lista recoge el conjunto de advisories publicados para Google Chrome a lo largo del periodo de estudio. Debido al rápido ciclo de versiones, afecta, desde Google Chrome 2.0 a Google Chrome 4.0. Es decir, el número de vulnerabilidades es relativo a 10 meses.

Level	Advisory ID	Version	Impact	Vector Attack	Patched	Vulnerabilities
	SA35411 (10/06/2009)	2.0	System Access Exposure of information	Remote	YES	CVE-2009-1690 CVE-2009-1718
	SA35548 (23/06/2009)	2.0	System Access	Remote	YES	CVE-2009-2121
	SA35844 (17/07/2009)	2.0	System Access	Remote	YES	CVE-2009-2556 CVE-2009-2555
	SA36417 (26/08/2009)	2.0	Spoofing Exposure of information System Access	Remote	YES	CVE-2009-2414 CVE-2009-2416 CVE-2009-2935 CVE-2009-2973
	SA36770 (16/09/2009)	2.0	Security Bypass XSS	Remote	NO	CVE-2009-3263 CVE-2009-3264
	SA36913 (01/10/2009)	3.0	System Access	Remote	YES	CVE-2009-0689
	SA37273 (06/11/2009)	3.0	Exposure of system information Exposure of sensitive information System Access	Remote	YES	CVE-2009-3931 CVE-2009-3932 CVE-2009-3934
	SA37358 (13/11/2009)	3.0	Security Bypass	Remote	YES	CVE-2009-2816
	SA38061 (22/01/2010)	4.0	Exposure of sensitive information	Remote	YES	CVE-2010-0315
	SA37769 (26/01/2010)	3.0	System access Security Bypass Exposure of sensitive information DoS	Remote	NO	fix 10 vulnerabilities
	SA38545	4.0	Manipulation of data Exposure of sensitive information System access	Remote	YES	CVE-2010-0556 CVE-2010-0643 CVE-2010-0644 CVE-2010-0645 CVE-2010-0646 CVE-2010-0647 CVE-2010-0649
	SA39029	4.0	Unknown Security Bypass Spoofing	Remote	YES	CVE-2010-1228 CVE-2010-1229 CVE-2010-1230 CVE-2010-1231 CVE-2010-1232 CVE-2010-1233

CVE-2010-1234
CVE-2010-1235
CVE-2010-1236
CVE-2010-1237

Del navegador Google Chrome hay que notar, en primer lugar, el rápido ciclo de versionados, haciendo que una versión estable dure un periodo menos de 5 meses. Según el sistema de numeración utilizado por Google Chrome se ha pasado de la versión 1.0, publicada el 11 de Diciembre de 2008, a la versión 4.0, publicada el 25 de Enero de 2010, en sólo 15 meses. Además, como se puede ver en la lista de Security Advisories, uno catalogado como Highly Critical en la versión 1.0 no ha sido parcheado.

Microsoft Internet Explorer 8.0

Microsoft Internet Explorer 8.0 fue publicado en Marzo de 2009, por lo que la lista de advisories es, casi completamente, relativa a esta última versión. El periodo abarca 12 meses.

Level	Advisory ID	Version	Impact	Vector Attack	Patched	Vulnerabilities
	SA35362 (09/06/2009)	8.0	System Access Security Bypass	Remote	YES	CVE-2009-1532
	SA35962 (28/07/2009)	8.0	System Access	Remote	YES	CVE-2009-1917 CVE-2009-1918 CVE-2009-1919
	SA36334 (19/08/2009)	8.0	Spoofing	Remote	NO	CVE-2009-3003
	SA36979 (13/10/2009)	8.0	System Access	Remote	YES	CVE-2009-2529 CVE-2009-2530 CVE-2009-2531
	SA37448 (23/11/2009)	8.0	System Access	Remote	YES	CVE-2009-2493 CVE-2009-3671 CVE-2009-3673 CVE-2009-3674
	SA37362 (25/11/2009)	8.0	Exposure of information	Remote	NO	CVE-2009-4073
	SA38209 (15/01/2010)	8.0	System Access Cross Site Scripting	Remote	YES	CVE-2009-4074 CVE-2010-0027 CVE-2010-0244 CVE-2010-0245 CVE-2010-0246 CVE-2010-0248 CVE-2010-0249
	SA38416 (04/02/2010)	8.0	Exposure of system information Exposure of sensitive information	Remote	NO	CVE-2010-0255 CVE-2010-0555
	SA38860 (09/03/2010)	8.0	Exposure of sensitive information System access	Remote	YES	CVE-2010-0490 CVE-2010-0492 CVE-2010-0494

Como se puede apreciar, Microsoft actualiza todas los advisories críticos. Los de menor criticidad tardan más tiempo en ser actualizados debido a que prima la estabilidad de los sistemas, así, estos son parcheados dentro de revisiones cíclicas de código.

Mozilla Firefox

La siguiente lista recoge la lista de advisories de seguridad que afectan, durante el periodo de estudio desde la versión 3.5 hasta 3.6 de Mozilla Firefox. El estudio de vulnerabilidades abarca 9 meses.

Level	Advisory ID	Version	Impact	Vector Attack	Patched	Vulnerabilities
	SA35798 (14/07/2009)	3.5	System Access	Remote	YES	CVE-2009-2467 CVE-2009-2477
	SA36001 (27/07/2009	3.5	System Access Spoofing	Remote	YES	CVE-2009-2470 CVE-2009-2654 CVE-2009-2662 CVE-2009-2663 CVE-2009-2665
	SA36649 (09/09/2009)	3.5	Manipulation of data	Remote	YES	CVE-2009-3274
	SA36671 (10/09/2009)	3.5	Security Bypass Spoofing System Access	Remote	YES	CVE-2009-3069 CVE-2009-3071 CVE-2009-3072 CVE-2009-3073 CVE-2009-3075 CVE-2009-3077 CVE-2009-3078 CVE-2009-3079
	SA36711 (28/10/2009)	3.5	Security Bypass Manipulation of data Exposure of information System Access	Remote	YES	CVE-2009-0689 CVE-2009-3370 CVE-2009-3371 CVE-2009-3372 CVE-2009-3373 CVE-2009-3374 CVE-2009-3375 CVE-2009-3376 CVE-2009-3377 CVE-2009-3378 CVE-2009-3379 CVE-2009-3380 CVE-2009-3381 CVE-2009-3383
	SA37699 (16/12/2009)	3.5	Security Bypass System Access Spoofing Manipulation of data Exposure of information	Remote	YES	CVE-2009-3388 CVE-2009-3389 CVE-2009-3979 CVE-2009-3980 CVE-2009-3982 CVE-2009-3983 CVE-2009-3984 CVE-2009-3985 CVE-2009-3986 CVE-2009-3987
	SA38608 (18/02/2010)	3.6	Security Bypass Manipulation of data Exposure of sensitive information System access	Remote	YES	CVE-2010-0164 CVE-2010-0165 CVE-2010-0166 CVE-2010-0167 CVE-2010-0168 CVE-2010-0169

						CVE-2010-0170 CVE-2010-0171 CVE-2010-0172 CVE-2010-0173 CVE-2010-0174 CVE-2010-0176 CVE-2010-0177 CVE-2010-0178 CVE-2010-0181 CVE-2010-0182 CVE-2010-1028

De Mozilla Firefox llama poderosamente la atención la criticidad de todos los advisories de seguridad, en los que queda de manifiesto la falta de medidas de fortificación interna que mitiguen el impacto de las vulnerabilidades descubiertas.

Opera Browser

La siguiente lista recoge los advisories relativos desde Opera 9.6 hasta 10.x durante el periodo de estudio. El conteo de vulnerabilidades abarca 14 meses.

Level	Advisory ID	Version	Impact	Vector Attack	Patched	Vulnerabilities
	SA36414 (01/09/2009)	9.X	Spoofing	Remote	NO	CVE-2009-3047 CVE-2009-3046 CVE-2009-3045 CVE-2009-3044 CVE-2009-3048 CVE-2009-3049
	SA37182 (28/10/2009)	10.X	Impact: Spoofing Exposure of sensitive information System access	Remote	YES	CVE-2009-3831 CVE-2009-3832
	SA37431 (20/11/2009)	10.x	System Access	Remote	YES	CVE-2009-0689
	SA37479 (23/11/20099	10.X	Unknown Cross Site Scripting Exposure of sensitive information	Remote	YES	CVE-2009-4071 CVE-2009-4072
	SA38546 (11/02/2010)	10.x	Unknown Manipulation of data	Remote	YES	--
	SA38820 (04/03/2010)	10.x	Exposure of sensitive information System access	Remote	YES	--

Como se puede ver, no hay demasiados advisories de Opera durante el periodo de estudio y muchos atribuyen a este resultado tanto a la calidad del software como a la ausencia de interés en la industria del malware que, al igual que no desarrolla de manera constante malware para Opera, tampoco está interesado en las vulnerabilidades y exploits que afecten a este software.

Apple Safari

La lista de advisories desde la versión 4.0 de Safari que fue publicada el 8 de Junio, hasta Abril de 2010, es decir, 9 meses, es la siguiente:

Level	Advisory ID	Version	Impact	Vector Attack	Patched	Vulnerabilities
	SA33495 (03/07/2009)	4.0	DoS	Remote	NO	CVE-2009-2419
	SA35758 (09/07/2009)	4.0	Cross Site Scripting System access	Remote	YES	CVE-2009-1724 CVE-2009-1725
	SA36269 (12/08/2009)	4.0	Spoofing Manipulation of data Exposure of sensitive information System access	Remote	YES	CVE-2009-2188 CVE-2009-2195 CVE-2009-2196 CVE-2009-2199 CVE-2009-2200 CVE-2009-2468
	SA37346 (12/11/2009)	4.0	Security Bypass Exposure of sensitive information System access	Remote	YES	CVE-2009-2414 CVE-2009-2416 CVE-2009-2804 CVE-2009-2816 CVE-2009-2841 CVE-2009-2842 CVE-2009-3384
	SA37931 (22/01/2010)	4.0	Exposure of sensitive information	Remote	NO	CVE-2010-0314
	SA38932 (12/03/2010)	4.0	Security Bypass Exposure of sensitive information System access	Remote	YES	CVE-2009-2285 CVE-2010-0040 CVE-2010-0041 CVE-2010-0042 CVE-2010-0043 CVE-2010-0044 CVE-2010-0045 CVE-2010-0046 CVE-2010-0047 CVE-2010-0048 CVE-2010-0049 CVE-2010-0050 CVE-2010-0051 CVE-2010-0052 CVE-2010-0053 CVE-2010-0054

Análisis de vulnerabilidades

Atendiendo a la información recogida para cada navegador, respecto del número de vulnerabilidades, criticidad, si existe o no parche para su corrección y la distribución de las

mismas a lo largo del tiempo, se presentan una serie de resultados y gráficos que permiten tener una mayor información sobre cómo afectan a cada uno de los navegadores.

Número de vulnerabilidades

Atendiendo exclusivamente al número de vulnerabilidades, se puede observar que es Mozilla Firefox el que más vulnerabilidades ha presentado, seguido de Apple Safari. Por detrás estarían Google Chrome y Microsoft Internet Explorer, mientras que muy por debajo se encuentra Opera.

Llama poderosamente la atención que Mozilla Firefox tiene el doble de las vulnerabilidades que tienen el resto de los navegadores.

Estas cifras deben verse teniendo en cuenta la perspectiva de la cuota de mercado y, por lo tanto, usuarios que utilizan cada uno de los navegadores. A continuación se muestra la cuota de mercado de los navegadores según NETMARKETSHARE en Marzo de 2010.

Como se puede observar, Google Chrome y Apple Safari, pese a tener una cuota y uso muy inferior a Microsoft Internet Explorer, han presentado más o menos las mismas vulnerabilidades que éste. También se puede observar que Opera Browser presenta muy pocas vulnerabilidades.

Si se prorratea el número de vulnerabilidades por el número de meses estudiado en cada familia de producto, el resultado es el siguiente:

Vulnerabilidades según criticidad

Atendiendo a la criticidad de las vulnerabilidades, tomando como dato la criticidad del Advisory al que corresponde, se observa como Microsoft Internet Explorer 8.0 es el único con vulnerabilidades extremadamente críticas, y que el grueso de las vulnerabilidades son clasificadas como altas.

La catalogación de una vulnerabilidad highly critical como extremly critical radica en la existencia de exploits atacando dicha vulnerabilidad. Esto, en la situación actual del mercado del malware y, siendo Microsoft Internet Explorer el navegador con más cuota de mercado, ha hecho de las vulnerabilidades de Microsoft Internet Explorer moneda de cambio entre las mafias de Internet.

En el famoso caso del incidente Aurora, gracias a la aplicación de las medidas de mitigación disponibles Microsoft Internet Explorer 7.0 y Microsoft Internet Explorer 8.0 el exploit que atacó esta vulnerabilidad antes de que fuera parcheada no afectó a los sistemas que tenían activo el Modo Protegido y DEP, tal y como muestra el siguiente tabla:

	Windows 2000	Windows XP	Windows Vista	Windows 7
Internet Explorer 6	Exploitable	Exploitable (current exploit effective for code execution)	N/A (Vista ships with IE7)	N/A (Windows 7 ships with IE 8)
Internet Explorer 7	N/A (IE 7 will not install on Windows 2000)	Potentially exploitable (current exploit does not currently work due to memory layout differences in IE 7)	IE Protected Mode prevents current exploit from working.	N/A (Windows 7 ships with IE 8)
Internet Explorer 8	N/A (IE 8 will not install on Windows 2000)	DEP enabled by default on XP SP3 prevents exploit from working.	IE Protected Mode + DEP enabled by default prevent exploit from working.	IE Protected Mode + DEP enabled by default prevent exploit from working.

Tienes más información de esta vulnerabilidad en el análisis de la misma del equipo de seguridad de Microsoft.

Vulnerabilidades corregidas

En este gráfico se puede observar que, mientras Microsoft Internet Explorer y Mozilla Firefox corrigen prácticamente todas las vulnerabilidades que presentan, los navegadores Google Chrome, Opera Browser y Apple Safari mantienen gran cantidad de vulnerabilidades sin corregir, las cuales, es posible que queden corregidas en versiones posteriores, pero no se generan parches para todas las versiones vulnerables. Este comportamiento, obliga a las empresas que estén utilizando dicho software a forzar un proceso de migración de software no planificado por motivos de seguridad.

Conclusiones finales

A continuación se recogen algunas conclusiones que los autores del presente documento sacan sobre las medidas de seguridad de los diferentes navegadores.

Google Chrome

De este navegador resalta las pocas opciones de configuración que ofrece para los usuarios empresariales, dejando poca o ninguna posibilidad de configuración de seguridad. No permite configurar las opciones de JavaScript, no admite diferentes zonas de seguridad, ni es administrable en remoto por un Active Directory. Saca una nueva versión cada poco tiempo, haciendo difícil la construcción de aplicaciones empresariales sobre ella. En su última versión aplica actualizaciones silenciosas, saltándose todo control que pueda querer un administrador de red sobre el software de sus clientes. Tiene pocos plug-ins pero, como rasgo positivo en seguridad, no existe mucho malware especialmente diseñado para él, salvo el basado directamente en ataques XSS. También hay que resaltar que Google Chrome no tiene filtro Anti XSS ni tan siquiera como plug-ins añadidos.

Mozilla Firefox

El número de vulnerabilidades que muestra durante este año duplica a las de cualquier navegador, lo que obliga a la generación de un gran número de parches que deben ser aplicados con diligencia, ya que la que mayoría son de nivel crítico. Tiene una arquitectura que no saca provecho de las ventajas arquitectónicas que ofrecen los sistemas operativos Windows Vista y Windows 7. Como rasgo positivo hay que destacar que todas las vulnerabilidades son parcheadas aunque ha sufrido bastantes críticas sobre cómo se realiza este proceso debido al gran número de fallos de regresión que generan y que resultan en nuevas vulnerabilidades. Tiene la posibilidad de ser administrado por Active Directory y tener filtro Anti-XSS pero por medio de plug-ins de los que habrá que contabilizar a la hora de vulnerabilidades y parches de seguridad. Además, hay que tener presente que existe mucho malware y muy elaborado técnicamente para Mozilla Firefox y que incluso se ha distribuido por el sitio oficial del producto.

Opera Browser

Este navegador presenta muy pocas opciones empresariales de administración y configuración. No tiene filtro Anti XSS ni en el propio código ni como plug-in añadido y sus opciones de

seguridad son las menos robustas en esta área. Tampoco hace uso de arquitecturas modulares ni saca provecho de las tecnologías MIC y UIPI en Windows Vista y Windows 7. Por otro lado, no se ha descubierto un gran número de vulnerabilidades, tal vez debido al poco interés que demuestra tanto en cuota de mercado de uso, como interés por parte de la industria del malware. También como dato positivo hay que hacer notar que casi no se conoce malware desarrollado para él.

Apple Safari

Este navegador no viene pensado para ser administrado de forma centralizada en una empresa con lo que no tiene buenas herramientas. Al igual que Opera Browser no tiene una arquitectura modular y no hace un uso eficiente de las tecnologías MIC e UIPI. A diferencia de Opera Browser, sí que existe mucho interés en la industria de la seguridad con este navegador, haciendo que sus vulnerabilidades sean altas dejando bastante sin parchear.

Microsoft Internet Explorer

La última versión de Microsoft Internet Explorer 8.0 es el único navegador que ha tenido alguna vulnerabilidad catalogada como extremadamente crítica. Esto se debe a que se conoce, a ciencia cierta, que ha sido utilizada para atacar a los usuarios de este navegador. A pesar de eso, ha demostrado tener las mejores medidas de seguridad aplicadas para fortificar la solución, desde las técnicas de engaño a usuarios, las protecciones Anti XSS, las opciones de fortificación en tecnologías Windows Vista y Windows 7 y, por supuesto, las mejores herramientas de configuración y ajuste de la seguridad, tales como las zonas de seguridad, las listas de permisos en componentes ActiveX por sitio y por usuario, la posibilidad de administrar de forma centralizada da, a los administradores, herramientas eficientes para fortificar sus implantaciones. Como dato negativo hay que resaltar que Internet Explorer, al igual que Firefox, está hoy en día en el punto de mira de la industria del malware y los buscadores de vulnerabilidades.