VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Marzo 2014

Boletín mensual de seguridad para usuarios de computadoras

OUCH!

En esta edición...

- Introducción
- El ciclo de vida de un sistema operativo
- Protégete

Windows XP llega a su fin

Introducción

Windows XP ha demostrado ser uno de los sistemas operativos más populares en la historia de la computación, en su momento, uno de los más usados en todo el mundo. Sin embargo, Windows XP es un sistema antiguo, por lo que Microsoft dejará de dar soporte a este sistema. Su lanzamiento fue hace 12 años, Microsoft tiene programado finalizar su ciclo de soporte el 8 de abril de 2014, lo que significa que no liberará más actualizaciones para los usuarios finales, tampoco parches de seguridad. Aproximadamente un 25% de equipos de escritorio en el mundo aún usan Windows XP (sólo Windows 7 es más popular), lo que propicia que millones de usuarios se encuentren en gran riesgo. Hay que tomar en cuenta que los hogares no serán los únicos afectados, es decir, XP todavía es utilizado en oficinas, sistemas de control industrial, cajeros automáticos, sistemas médicos, terminales de venta y otros dispositivos. En el siguiente apartado se describe el riesgo en el que se encontrará Windows XP al no tener soporte y las precauciones que deben tomarse para proteger el sistema.

Editor Invitado

Jason Fossen, especialista en seguridad de Microsoft Windows en Enclave Consulting LLC, es autor del sexto día del curso Asegurando Windows con Controles de Seguridad Crítica (Securing Windows with the Critical Security Controls, SEC505) del SANS y también ofrece scripts de seguridad en PowerShell en el sitio **http://cyber-defense.sans.org/blog/**.

El ciclo de vida de un sistema operativo

Es posible que desconozcas esto, pero el sistema operativo de tu computadora tiene un límite de vida útil. El proveedor que lo crea genera actualizaciones y parches que añaden nuevas características, que mejoran la estabilidad y rendimiento, además de que lo mantienen seguro. Eventualmente el proveedor dejará de darle soporte, para centrar su atención y recursos en las nuevas tecnologías que promociona, es decir, dejará de proporcionar recursos a ese sistema aun a sabiendas de conocer que es vulnerable y que los criminales cibernéticos pueden aprovechar dicha situación para comprometerlo. En abril, Windows XP quedará bajo esta situación. Incluso quizás, por medio de Microsoft se conocerán las vulnerabilidades de los equipos que tienen Windows XP y un criminal cibernético podría explotarlas, sin embargo, Microsoft no arreglará más estos problemas.

Protégete

En caso de no poder adquirir un nuevo equipo, puedes protegerte con un sistema actualizado que cuente con soporte activo. Algunas organizaciones no se verán tan perjudicadas al migrar a Windows 7 en lugar de Windows 8, ya que la interfaz gráfica de Windows 7 es similar a la de Windows XP. Sin embargo, Windows 8 es más seguro pues, en comparación

Windows XP llega a su fin

con versiones anteriores, ha tenido significantes mejoras. También existen otros proveedores de sistemas operativos que puedes considerar, como Mac OS X de Apple. De cualquier manera, es momento de actualizarse y no cuentas con mucho tiempo para hacerlo. Si simplemente no puedes cambiar el sistema Windows XP antes de abril, considera lo siguiente:

Una vez que Windows XP deje de recibir soporte, la mejor manera de protegerse es migrar a un nuevo sistema operativo que cuente con soporte activo y asegurarse de que esté actualizado.

- Usa la computadora con Windows XP solamente para las funcionalidades o aplicaciones que sean absolutamente necesarias. Por ejemplo, quizás tú y tu organización ejecuten un viejo programa que solamente sea compatible en XP y por esta razón no puede ser actualizado. Si este es el caso, entonces no utilices la computadora para otro propósito, como correo electrónico o navegar a través de Internet.

- Si tienes que usar tu equipo para navegar, deja de utilizar Internet Explorer y cambia a otro navegador, como Mozilla Firefox, Google Chrome u Opera. Asegúrate de mantener siempre actualizado el navegador y que el proveedor continúe dando soporte para quienes usan Windows XP.

- Evita usar aplicaciones nativas de Windows XP para abrir archivos descargados de Internet (como Windows Media Player). En su lugar utiliza aplicaciones de otros proveedores que aún cuenten con soporte para sus versiones de Windows XP.

- Considera utilizar servicios de seguridad de red gratuitos como OpenDNS. Servicios como estos protegen su sistema de visitantes desconocidos y sitios maliciosos. Además, algunos servicios pueden detectar si tu equipo intenta conectarse a botnets conocidas, lo que indica que el sistema se encuentra infectado.

- Asegúrate de tener instalado un programa de seguridad, como un antivirus, éste debe tener soporte y mantenimiento activo para Windows XP.

- Si no es primordial que tu equipo tenga conexión a Internet (por ejemplo si lo usas sólo para crear documentos) entonces desconecta el equipo de la red. Si necesita estar conectado, asegúrate de que se encuentre protegido por un firewall y que esté bloqueando cualquier tráfico hacia el equipo. Las organizaciones quizás puedan aislar

Windows XP llega a su fin

todos los equipos con Windows XP en una red separada, de esta manera, si alguno de los equipos se infecta, el resto de los equipos de la organización no se verán afectados.

- Realiza regularmente respaldos de los datos de tus equipos con Windows XP, como prevención en caso de que se infecten. Guarda al menos uno de los respaldos en un dispositivo externo, como un dispositivo USB. Si te encuentras forzado a recuperar el sistema, considera seriamente recuperarlo en un nuevo equipo. Si recuperas de nuevo un sistema con Windows XP, será muy probable que se vuelva a infectar.

- Si utilizas Windows XP en tu organización, tal vez la compañía tenga medidas adicionales que deberás tomar en cuenta. Recuerda que éstas son solamente medidas preventivas a corto plazo, no son el sustituto de una actualización que permita que el sistema sea seguro. Tarde o temprano tendrás que migrar a un nuevo sistema.

Conoce más

Suscríbete al boletín mensual de conciencia sobre seguridad OUCH!, consulta los archivos OUCH! y aprende más acerca de las soluciones de seguridad SANS visitando: http://www.securingthehuman.org

Versión en español

UNAM-CERT, Equipo de Respuesta a Incidentes de Seguridad de la Información en México reconocido ante FIRST, es una referencia en la materia en este país.
Sitio web: http://www.seguridad.unam.mx
Síguelo en Twitter @unamcert

Recursos

Anuncios Microsoft EOL:
http://www.microsoft.com/es-es/windows/endofsupport.aspx
OpenDNS:
www.opendns.org
Guía de migración:
http://bitelia.com/2014/01/fin-soporte-windows-xp-migracion
Copias de seguridad y recuperación personal:
http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201309_sp.pdf

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducción al español por: Erika Ródriguez e Israel Rubí