Informe de Amenazas CCN-CERT IA-02/14

Riesgos de uso de Windows XP tras el fin de soporte

22 de enero de 2014

ÍNDICE

1. SOBRE CCN-CERT

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es). Este servicio se creó a finales del año 2006 como el CERT gubernamental/nacional, y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad. De acuerdo a todas ellas, el CCN-CERT tiene responsabilidad en ciberataques sobre sistemas clasificados y sobre sistemas de la Administración y de empresas pertenecientes a sectores designados como estratégicos.

La misión del CCN-CERT es, por tanto, contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a las Administraciones Públicas y a las empresas estratégicas, y afrontar de forma activa las nuevas ciberamenazas.

2. RIESGOS DE FIN DE SOPORTE DE XP

En 2002 Microsoft presentó su política de Ciclo de Vida de Soporte con el fin de ofrecer una mayor transparencia y previsibilidad a la hora de explicar las opciones de soporte para sus productos. Cada producto de Windows tiene un ciclo de vida que comienza cuando se lanza un producto y termina cuando ya no se vende o no tiene soporte.

Siguiendo esta política, los productos para empresa y desarrolladores, entre los cuales se incluyen los sistemas operativos Windows y Microsoft Office, disponen de un mínimo de 10 años de soporte (5 de soporte estándar y 5 más de soporte extendido) en el soporte a nivel de service pack.

Por otro lado, hay que tener en cuenta que a partir de 2012 la mayoría de los fabricantes de hardware OEM (*Original Equipment Manufacturer*) dejaron de dar soporte a Windows XP en la mayor parte de sus nuevos modelos de PC.

El uso de Windows XP supone **no recibir** soporte de ningún tipo desde Microsoft, ni **actualizaciones de seguridad** ni parches de resolución de incidencias. Por todo ello, los sistemas corporativos se hacen vulnerables y pueden exponer a un Organismo a graves amenazas para la seguridad de la información. Además será más difícil adquirir o actualizar software que ofrezca nuevas funcionalidades, debido a incompatibilidades con Windows XP.

2.1 Riesgos inherentes a permanecer fuera del soporte oficial de Microsoft

Los riesgos a los que se exponen las plataformas son:

- Windows XP se convertirá en un "blanco fácil" para explotar vulnerabilidades una vez dejen de publicarse actualizaciones de seguridad por parte de Microsoft. Los atacantes y creadores de código dañino se centrarán especialmente en sistemas XP, con la certeza de que a partir del 8 de abril de 2014 ninguna vulnerabilidad será parcheada y sus ataques tendrán siempre éxito.
- Tras la publicación por parte de Microsoft de actualizaciones de seguridad para Windows 8 y Windows 7, los atacantes podrían realizar ingeniería inversa de los mismos para comprobar qué vulnerabilidades son parcheadas y comprobar si las mismas están presentes en Windows XP. En caso de ser así, el atacante tendría garantizado el éxito de una posible intrusión a un sistema con Windows XP.
- Cualquier red corporativa con un solo PC con el sistema operativo Windows XP estará en riesgo. Una vez comprometido ese equipo podrá ser utilizado como trampolín para infectar al resto de equipos independientemente de la tecnología de su sistema operativo.

- Existe un gran número de vulnerabilidades conocidas no parcheadas. Se estima que existe también un importante número de vulnerabilidades que aún no son conocidas (día cero).
- Es muy probable que algunos atacantes mantengan a la espera programas para ataques remotos que se sirvan de fallos de seguridad no publicados y los utilicen cuando haya finalizado el ciclo de vida de Windows XP. Esto implica que cualquier Organismo estaría desprotegido indefinidamente ante este tipo de ataques.
- El mero hecho de mantener actualizados los antivirus comerciales no será suficiente. Las tasas de infección, publicadas por Microsoft en el año 2012, son el doble en sistemas Windows XP que en sistemas Windows 7. Cabe mencionar la posibilidad de que los fabricantes de software antivirus dejen de actualizar sus soluciones para Windows XP.
- A día de hoy, siguen apareciendo nuevas vulnerabilidades que permiten al atacante tomar control de los sistemas de forma remota. A modo de ejemplo, el NIST estadounidense ha publicado 28 de estas vulnerabilidades tan sólo en los 3 primeros meses de 2013.
- Un usuario interno malintencionado podría saltarse las protecciones implementadas por los administradores de la red y tomar control de la misma ante la falta de soluciones de seguridad apropiadas por desactualización.

Adicionalmente, las nuevas capacidades de los ordenadores no son aprovechadas por Windows XP. La mayoría de los nuevos equipos tienen características que no existían, o estaban sin madurar, cuando se interrumpieron las mejoras de los *service packs* para Windows XP.

Además, hoy en día, la mayoría de los equipos vienen con un mínimo de 4 GB de memoria, que un sistema operativo normal Windows XP de 32 bits no puede gestionar.

3. CONCLUSIONES

Queda patente el riesgo que supone **no migrar a una versión más actualizada de Windows** ya que el uso de software sin soporte **supone limitar seriamente la capacidad de uso seguro de las TIC por parte de una Organización**.

Con la migración se rebajaría sustancialmente el impacto de las potenciales amenazas y se consolidaría una infraestructura de sistemas más eficiente, más segura, con mejoras en su administración y con una menor tasa de fallos.

4. RECOMENDACIÓN

Se recomienda por tanto la elaboración de un plan de migración del parque de equipos con sistema operativo Windows XP a versiones más actualizadas a la

mayor brevedad posible para reducir en la medida de lo posible el impacto de ausencia de soporte.

ANEXO A. REFERENCIAS

[Ref – 1]	**Microsoft Security Blog** The Risk of Running Windows XP after support ends April 2014 Agosto de 2013 http://blogs.technet.com/b/security/archive/2013/08/15/the-risk-of-running-windows-xp-after-support-ends.aspx