



Los errores del software y su solución, una asignatura pendiente

No hace mucho, Microsoft anunció la existencia de una grave vulnerabilidad de seguridad en su librería Microsoft ASN.1 y, como ya es clásico, este nuevo error está provocado por un desbordamiento de búfer¹. La Abstract Syntax Notation 1 (ASN.1) es un estándar de datos empleado desde hace años en muchas aplicaciones y dispositivos para la normalización e intercambio de datos. Este problema concreto afecta a los sistemas corriendo con Windows 2000, Server 2003, XP y NT 4.0. Al igual que todos los desbordamientos de *buffer*, el problema es grave ya que permite la entrada de virus, claudicación de sistemas, usurpación de identidades, etc., puesto que el ASN1 es un componente bastante común de los sistemas operativos. Aunque la publicación de parches por parte de Microsoft es algo del todo habitual, la publicación de estos parches en concreto ha estado rodeada de muchos amargos comentarios dentro del mundillo de la seguridad informática.

Los descubridores de esta anomalía, eEye², afirman que informaron a Microsoft de la existencia de estos problemas 200 días antes de la publicación de la correspondiente corrección (parche), lo que supone un tiempo excesivo a todas luces. Según Microsoft esta sorprendente demora se debe a que ciertas respuestas que afectan a la seguridad de los sistemas requieren un delicado equilibrio entre velocidad y calidad de la resolución y, en este caso, Microsoft ha necesitado evaluar múltiples aspectos y casos particulares para la creación de un parche de "gran calidad", según ellos declaran. La pregunta que queda en el aire es si Microsoft se hubiera sentido más presionada para la publicación de esta actualización en el caso de que eEye no le hubiese otorgado esos 200 días de ventaja.

Microsoft ha cambiado su política de publicación de parches para sus aplicaciones y sistemas operativos y esto ha causado cierto revuelo además de abrir el triste tema de las continuas "actualizaciones" del software y su correspondiente planificación. Los comunicados de Microsoft han venido a echar más sal en la herida y exhiben un paternalismo difícil de entender si nos olvidamos de que el gigante de Redmond es una empresa "genuinamente americana"

Lo que sí sabemos es que eEye ya se ha cansado de esperar indefinidamente la respuesta de Microsoft a los problemas que va descubriendo y acaba de publicar una página de «próximos avisos³», indicando la fecha de la notificación y el número de días que han transcurrido sin que Microsoft aporte una solución. En esa relación lo que hay son vulnerabilidades existentes y no solucionadas, por lo que cualquier intruso que conozca su existencia puede sacar provecho de las mismas.

La publicación de este parche se inscribe dentro de la nueva política de publicación de "enmiendas" de Microsoft en la que todos los parches desarrollados desde la última actualización se publican juntos como un todo. A título de ejemplo de este nuevo estilo, en su publicación de febrero de este año, Microsoft ha distribuido tres

correcciones que hacen. Algunas veces, los parches que se publican conducen a la necesidad de nuevos parches. Por ejemplo, el 15 de octubre de 2003 Microsoft publicó siete parches para corregir vulnerabilidades conocidas en Windows y Exchange, y fue éste el primer ejemplo de sus nuevas actualizaciones mensuales. Pasados siete días, el 22 de octubre, Microsoft confirmó la existencia, en los parches anteriores, de problemas en sus versiones «extranjeras», incluida la española, y proporcionó una corrección de los mismos. De nuevo, siete días después, el 29 de octubre, Microsoft «reparchea» algunas de sus entregas anteriores. Durante los 5 últimos años no ha existido un sólo mes en que Microsoft no haya distribuido parches de seguridad.

El problema de las actualizaciones

El problema de las actualizaciones de software para corregir errores previos en aplicaciones y sistemas operativos es propio de cualquier empresa que se dedique al desarrollo de software; independientemente de si se trata del gigante Microsoft o de la más pequeña *spin-up* del mundillo universitario. La corrección de distribuciones previas es un problema común a todos los fabricantes: distribuciones Linux, Sun, IBM, HP, etc.

La actualización del software por parte del usuario final requiere, en todos los casos, pasar evaluaciones y controles de calidad previos en sistemas de pruebas, para luego distribuirlos en los sistemas de producción.

nuevos parches: el primero está relacionado con una vulnerabilidad (MS04-006) en los servidores que gestionan el servicio WINS⁴ y que ha sido catalogado como de baja importancia a importante, dependiendo de los casos. Por otra parte, en esa misma entrega se corrige la vulnerabilidad, ya comentada, en la implementación ASN.1 en Windows NT, 2000, XP y Server 2003 (MS04-007), y también se incluye un parche ya publi-

Según datos publicados por Hispasec, para sistemas como el HP-UX y el Solaris de Sun se llegan a publicar más de 15 parches y actualizaciones en una misma semana; productos como HP OpenView, Sun ONE, Sun Cluster, etc. superan a los anteriores en este siniestro *ranking*. En el caso del sistema operativo AIX de IBM el número de parches publicados semanalmente puede llegar a superar el número 30. A la vista de los datos del servicio SANA (Hispasec), en un mismo mes se llegaron a publicar 202 alertas referidas a los sistemas y aplicaciones de IBM, mientras que para los sistemas Sun sólo hubo 117, HP llegó hasta 109 publicaciones y Microsoft sólo contó con 41 alertas, luego Microsoft no es la compañía que mas

correcciones tiene que hacer.

Un problema asociado con la necesidad de corregir lo previamente publicado es el tiempo que se tarda en hacerlo. Por ejemplo, las vulnerabilidades de desbordamiento de búfer anunciadas en junio de 2002 y ubicadas en las librerías del DNS (CERT CA-2002-19), fueron resueltas de forma inmediata en la mayoría de las distribuciones Linux, mientras que HP lo hizo en septiembre de ese año y aún siguió después publicando parches para corregir el mismo problema en sus sistemas HP-UX donde el problema no era tan crítico.

En lo que se refiere a los tiempos de reacción frente al descubrimiento de vulnerabilidades, los sistemas Linux resaltan elogiosamente en cuanto a su celeridad en la resolución de este tipo de problemas. Además de coexistir en ese entorno varios procedimientos para corregir problemas, las ideas del Open Source aportan la solución en forma de código fuente. Este nuevo código se puede compilar de forma inmediata y antes de disponer de los paquetes específicos publicados por el creador del software afectado, por lo que la solución puede ser muy rápida. Si no se necesita tanta celeridad, el usuario también se puede esperar unos pocos días para disponer de los paquetes es-

¹ Un atacante por desbordamiento de búfer permite ejecutar código con los privilegios de la aplicación afectada, y el atacante podrá realizar cualquier acción en el sistema como instalar otros programas, visualizar, modificar o eliminar datos, o crear nuevas cuentas de usuario con plenos privilegios, etc.

² Ver <http://www.eeye.com/>

³ Ver eEye Upcoming Advisories <http://www.eeye.com/html/Research/Upcoming/index.html>

⁴ WINS = Windows Internet Naming Service

pecíficos de la distribución que se tenga instalada.

En todo esto hay que tener en cuenta que la actualización del software por parte del usuario final requiere, en todos los casos, pasar evaluaciones y controles de calidad previos en sistemas de pruebas, para luego distribuirlos en los sistemas de producción. Prácticamente todo el mundo tiene experiencia directa de que la instalación inmediata de algunos parches les ha ocasionado problemas de incompatibilidad, mal funcionamiento, o regresión de antiguas vulnerabilidades.

Está claro que «en todas partes cuecen habas» y que nadie puede «lanzar la primera piedra» ante el fenómeno que nos ocupa. Aunque, en teoría, los «modelos formales de desarrollo de programas» definen los pasos a seguir para asegurar, en lo posible, la calidad de los programas desarrollados, la aplicación estricta de estos modelos siempre hace «no competitivo» el tiempo de desarrollo de un producto medianamente complejo.

A pesar de esto, como usuarios no debemos disculpar la existencia de fallos informáticos y debemos desterrar la fatalista tendencia a asumir que los fallos existen y debemos convivir con ellos. No hay razón alguna para no exigir de las compañías suministradoras de software o hardware un compromiso real y firme sobre el correcto funcionamiento y la calidad de los productos que ellas desarrollan y, además, esos proveedores están obligados a realizar el esfuerzo que sea necesario para enmendar sus errores previos.

Otro elemento a tener muy en cuenta en esto de parchear sistemas y aplicaciones es la calidad de los boletines que publica cada fabricante y que, en este caso y aspectos, los mejor publicados son los del Microsoft. La razón de ello posiblemente esté en tener que abarcar niveles muy heterogéneos de clientes que van desde los usuarios noveles hasta administradores profesionales. En general, los boletines de Microsoft son claros, sencillos y contienen toda la información necesaria para entender en qué consisten los problemas. Por otra parte, los boletines de otros fabricantes, como IBM o Sun, son bastante difíciles de digerir y están dirigidos a un público especializado que, se supone, no requiere grandes detalles.

En este último grupo uno se encuentra con la secretaria actua-

ción de algunos fabricantes al impedir el acceso a la información publicada mediante el control de accesos reservándolo a usuarios registrados de sus productos y no suelen emitir alertas por correo-e u otros mecanismos proactivos.

A finales del pasado año, Microsoft Ibérica publicó una nota de prensa que ha venido a empeorar las cosas y en la que se mostraba ligeramente enojada por las críticas que había recibido su nueva política de publicación de parches de seguridad.

En esa nota, Microsoft reconoce que debe continuar haciendo un esfuerzo para comunicar los motivos que justifican sus decisiones, lo cual es muy loable y de agradecer, y nos informa de:

– Que Microsoft cambia su política de comunicación de actualizaciones de seguridad, que se producirán de forma predecible en el segundo martes de cada mes, y que existirán excepciones cuando la situación lo requiera.

Pensar que un problema, en términos prácticos, no existe porque no se ha descubierto, es una soberbia falacia ya que equivale a pensar que lo que yo desconozco lo desconoce todo el mundo.

– Que el objetivo de este proceder es permitir la «Planificación» de la actualización de software en las empresas de forma adecuada y ordenada.

Esta nueva política da paso a preguntas del tipo: ¿cómo voy a mantener mi sistema vulnerable durante un mes hasta que llegue ese día de actualización? Un hecho con el que podríamos estar todos de acuerdo es que las vulnerabilidades en un sistema software representan un aumento exponencial del riesgo desde el momento en que son descubiertas ya que, a partir de ahí, además de los riesgos que representan por sí mismas para el sistema, se le suma la posibilidad de que sean explotadas por atacantes humanos.

En la nota de Microsoft se mencionan varios ejemplos de vulnerabilidades que han estado «durmientes» durante muchos años (Kerberos, SNMP y las 187 y 100 vulnerabilidades de seguridad detectadas en Debian y Redhat durante el año 2003), y como ejemplo más reciente se menciona el caso del virus Blaster, cuya vulnerabilidad clave ha estado latente durante bastante tiempo y no ha causado problemas conocidos hasta que alguien la ha descubierto y ha hecho uso de ella.

Aún siendo cierto lo anterior, de lo que no podemos nunca estar seguros es de cuándo y quién descubre una vulnerabilidad, por lo que no se puede inferir que el riesgo sea nulo por el hecho de que la existencia de la vulnerabilidad no haya sido anunciada.

Todos los comentarios que se han leído respecto a la mencionada nota de prensa de Microsoft están dirigidas a resaltar que 1) las vulnerabilidades existen y se explotan antes de ser publicadas, recordando que existen grupos de investigación dedicados a descubrir vulnerabilidades y a explotárselas en beneficio propio, 2) que una vulnerabilidad no se publica, no quiere decir que no existan ataques que las usen y pasan desapercibidos, 3) que los sistemas deben ser seguros «per se» y no porque se oculten sus fallos, 4) que Microsoft no suele ser quien descubre los fallos, sino terceras personas ajenas a la compañía, y que las vulnerabilidades se cono-

cen antes de cualquier posible reacción, por lo que Microsoft no debe decidir sobre el descubrimiento y publicación de vulnerabilidades, 5) que las empresas son las que planifican sus propias políticas de actualizaciones, y que éstas no deben estar condicionadas porque dichas actualizaciones estén o no disponibles en una determinada fecha, 6) que hay una dificultad añadida para usuarios sin banda ancha si lo que tienen que descargar son actualizaciones voluminosas.

Si se reúnen todos los parches en una misma entrega, la validación e instalación de las mismas se convierte en una operación de mayor envergadura, que termina acarreado retrasos en el despliegue final. En general, el parchado de un sistema no es de complejidad acumulativa, sino combinatoria.

Además de esto hay que recordar que la filosofía de diseño de los productos Microsoft es la de integrar aplicaciones y funcionalidades en el propio sistema operativo, lo que supone un amplificador de vulnerabilidades ya que, cuando están presentes, afectan a todo lo que se ejecute en sus sistemas operativos; un ejemplo dramático y pertinaz de ello es el

Internet Explorer.

Está claro que Microsoft sigue imbuida de grandes dosis de paternalismo y se siente llamada a enseñar a «planificar» las actualizaciones de sus usuarios. Ya es triste tener que estar corrigiendo el software que tanto dinero nos ha costado, pero más triste es ver que los creadores de ese software nos consideran incapaces, por no decir otra cosa. La nueva política de parches de Microsoft es una metedura de pata que destruye lo mucho bueno que tenía su joven sistema de actualizaciones on-line, construido a la sombra de lo que ya era habitual en distribuciones de código abierto.

Microsoft debe bautizarse en humildad y tener muy presente que sus errores casi siempre son descubiertos por «los otros», algunos de los cuales tienen la amabilidad de informarles y hacerlo en exclusiva. Que yo sepa, Microsoft no «gratifica» a los que descubren sus fallos y, tal y como están las cosas, debería hacerlo.

La necesidad de corregir cualquier software es un hecho y cuantas más personas colaboren en ello mejor será. Las actualizaciones deberían estar disponibles tan pronto como sea posible y deberán difundirse con máxima celeridad. Los fabricantes de software deberían fomentar y recompensar la identificación de sus fallos ya que, el mismo hecho de su descubrimiento ya supone una mejora neta en el producto que comercializan. Desde este punto de vista, deberíamos erradicar de la informática el secretismo y propugnar escenarios más abiertos y colaborativos.

Pensar que un problema, en términos prácticos, no existe porque no se ha descubierto, es una soberbia falacia ya que equivale a pensar que lo que yo desconozco lo desconoce todo el mundo. En realidad nadie sabe a ciencia cierta qué es lo que conocen los demás, por lo que nunca podemos estar seguros de que un error informático está realmente latente para todos. Siempre que hay un error en un software, la espada de Damocles está izada y lo único que no sabemos es cuándo caerá sobre nuestras cabezas. ■

JORGE DÁVILA MUÑOZ
Director
Laboratorio de Criptografía
**LSSI - Facultad
de Informática - UPM**
jdavila@fi.upm.es