NOTA INFORMATIVA CSIRT. #3546 19/09/2011

El riesgo del uso de Extensiones de terceros en los portales desarrollados mediante el CMS Joomla!

DOCUMENTO PÚBLICO

La presente nota recoge la información sobre el riesgo que conlleva el uso de **Extensiones de terceros** en portales desarrollados mediante el CMS Joomla! y recomendaciones sobre cómo usarlas de manera segura.

Análisis

Las llamadas **Extensiones** en Joomla! son pequeñas piezas de software que se pueden agregar sobre el CMS y que permiten expandir las funcionalidades de Joomla! agregando capacidades al mismo que no existen en el paquete estándar de instalación. Las Extensiones se clasifican según Joomla! como Módulos, Plugins, Componentes, Idiomas o Plantillas. Joomla! incluye diversas Extensiones por defecto. Así por ejemplo, en el caso de los Módulos, se incluyen los módulos por defecto como "Menú Principal", "Menú Superior", "Selector de Plantilla", "Encuestas", "Noticias Externas","Contador de Accesos", etc. Pero también es posible agregar Extensiones creadas por terceros, es decir Extensiones sobre las que Joomla! no tiene ningún tipo de control. En el apartado Extensiones > Instalar/ Desinstalar, en panel de administración, se pueden ver que Extensiones hay instaladas en un sitio web Joomla!

Instalar Extesiones de terceros conlleva el riesgo de que estén infectadas por malware y por tanto causen daños en nuestro servidor e incluso pudiendo llegar a convertirlo en un distribuidor de malware infectando a quienes lo visiten. También pueden ser extensiones vulnerables y hacer que nuestro sitio sea vulnerable comprometiendo nuestro sitio a posibles ataques, por este motivo, se recomienda usar solo las Extensiones que realmente se necesiten, seguir ciertas pautas de seguridad que enumeraremos a continuación, así como probarlas siempre en un entorno de preproducción antes de pasarlas a producción.

Desde el propio grupo de editores del Directorio de Extensiones (http://extensions.joomla.org/) y desde http://comunidadjoomla.org recomiendan algunas pautas para comprobar si una extensión es segura o no:

1. No instalar directamente las extensiones en nuestros sitios sin comprobar PRIMERO qué contienen.
   Tras descomprimir los paquetes de la extensión comprobar que todos los directorios de la misma tengan un fichero index.html. El archivo index.html controla que no se pueda acceder directamente a la carpeta.
2. Recomendable buscar en el código comandos que cambien los permisos de los directorios, como por ejemplo el comando chmod ("directorio", 777).
3. Asegurarse que los ficheros con la extensión .php contienen todos una línea al comienzo del mismo con el comando die: defined('_JEXEC') or die('Restricted access'); comprueba si está definida la variable "_JEXEC", y si no lo está muestra un mensaje de error mediante la función "die". Esto es una medida de seguridad que incluye el marco de trabajo Joomla! y que es recomendable usar en los archivos .php que tengamos en el sitio, evitara que los usuarios accedan a las páginas directamente sin hacer antes las comprobaciones de seguridad incluidas en Joomla!
4. Evitar instalar extensiones que modifiquen el núcleo de Joomla!
5. Comprobar que la extensión no se encuentra dentro de la lista de extensiones vulnerables http://docs.joomla.org/Vulnerable_Extensions_List
6. Se recomienda no instalar extensiones descargadas desde sitios "Warez" ya que podrían estar infectadas de malware.
7. Cuando se instalen extensiones nuevas es más recomendable, generalmente, que se use el método "Subir un paquete" o "Instalar desde un directorio" ya que instalar desde una URL remota puede ser peligroso

Recordemos que el mayor riesgo para que nuestro sitio Joomla! se vea comprometido es que NO esté actualizado, por tanto para mitigar dicho riesgo, el sitio Joomla! deberá estar actualizado cada vez que hay una nueva actualización y si se usan extensiones de terceros también deberemos estar al tanto de las actualizaciones de las mismas.

Para finalizar comentar que, desde la propia documentación oficial de Joomla! podemos extraer una serie de enlaces interesantes acorde a la securización de nuestro sitio y que recomendamos leer:

1. Recomendaciones de seguridad que engloban desde el comienzo de la instalación hasta que hacer si nuestro sitio ha sido comprometido. http://docs.joomla.org/Security

2. Securizando extensiones Joomla!
   http://docs.joomla.org/Securing_Joomla_extensions

Conclusiones

Las extensiones proporcionan a nuestros sitios Joomla! una mayor funcionalidad. Sin embargo el uso de las extensiones de terceros conlleva cierto riesgo añadido, ya que no están bajo el control de Joomla! y podrían hacer que nuestro sitio o nuestro servidor se viera comprometido. Por tanto, se recomienda actuar con precaución y mesura a la hora de instalarlas; usar las estrictamente necesarias, seguir las pautas de seguridad recomendadas a la hora de instalarlas así como mantener siempre actualizado nuestro Joomla! y nuestras extensiones.

Referencias destacables:

Para la realización de esta nota informativa se han consultado y extraído información de las siguientes referencias:

http://forum.joomla.org/

http://extensions.joomla.org/

http://docs.joomla.org/Vulnerable_Extensions_List

http://www.gnumla.com/articulos/jandbeyond-2010/pagina-6.html

http://comunidadjoomla.org/

http://docs.joomla.org/Securing_Joomla_extensions

http://ayudajoomla.com

Fecha de redacción: 19 de septiembre de 2011