Vulnerabilidad en el Servicio de Servidor de Windows

El martes 8 de Agosto de 2003 Microsoft liberó su emisión mensual de Boletines de Seguridad, la cual consistió de 12 boletines. Dentro de ellos existe uno que soluciona una vulnerabilidad en el Servicio de Servidor que podría permitir que nuestro sistema esté en riesgo y pueda ser utilizado por un intruso/hacker.

- ¿Qué sistemas Windows son afectados?
- ¿Por qué estamos alertando sobre la vulnerabilidad?

¿Por qué estamos alertando sobre la vulnerabilidad?

Ha comenzado a circular en el Internet código que explota la vulnerabilidad en el Servicio de Servidor. Esto significa que si no hemos instalado en el equipo las actualizaciones de seguridad liberadas el pasado martes 8 de Agosto de 2006, entre las que se encuentra la que soluciona la vulnerabilidad en el Servicio de Servidor, nuestro equipo podría estar en riesgo.

Una vez que el sistema es comprometido por un intruso o hacker podría ser utilizado para distintos fines, uno de los más comunes por ejemplo es utilizar al equipo como un zombi que forme parte de una botnet (red de equipos controlada por un intruso) que realice ataques de negación de servicio. Si el código de exploit se convierte en un tipo de gusano de Internet, podríamos ser infectados por él.

¿Qué hago para estar protegido?

Lo único que tienes que realizar a la brevedad posible es actualizar tu sistema Windows con los parches de seguridad liberados el pasado martes 8 de Agosto de 2006 por Microsoft Corp., entre las cuales se encuentra el que soluciona la vulnerabilidad en el servicio de Servidor.

Existen distintas formas para poder actualizar tu sistema a continuación te mencionamos algunas de ellas:

- Microsoft Update
- Windows Update
- Actualizaciones Automáticas

Existe un documento en éste mismo portal que te puede guiar paso a paso para que puedas realizar éste procedimiento de forma sencilla.

El documento lo puedes encontrar en

Métodos y herramientas de actualización:
http://www.seguridad.unam.mx/usuario-casero/secciones/herramientas.dsc

No olvides que existen otras herramientas que te pueden ayudar a mantenerte protegido cuando estas conectado a Internet mientras actualizas tu equipo. Estas herramientas son un firewall personal, un software antivirus y un software antispyware.

Puedes consultar otros documentos que pueden ayudarte con información relacionada con estas herramientas:

Firewall
http://www.seguridad.unam.mx/usuario-casero/secciones/firewall.dsc
Instalación y configuración de ZoneAlarm
http://www.seguridad.unam.mx/doc/?ap=tutorial&id=186
Sofware antivirus
http://www.seguridad.unam.mx/usuario-casero/secciones/antivirus.dsc
Spyware
http://www.seguridad.unam.mx/usuario-casero/secciones/spyware.dsc