

COMUNICADO VITI TI022-SI-26abr04

Abril 26, 2004

DE:

Dirección de Seguridad de la Información

DIRIGIDO A:

Directores VITI

Directores de Informática

ASUNTO:

Confirmación de Microsoft de ataques a vulnerabilidades en servicios de SSL (SMTP, IMAPS, POP3S y NNTPS)

El viernes 23 de abril, Microsoft confirmó que existe un ataque disponible en Internet que afecta a una de las vulnerabilidades corregidas en la actualización de seguridad MS04-011 (liberada el pasado 13 de abril). Este ataque afecta principalmente a equipos que estén corriendo IIS con SSL habilitado. (HTTPS)

El día de hoy, lunes 26 de abril, Symantec confirma que existen ya disponibles ataques similares para otros servicios diferentes a SSL, tales como SMTP, IMAPS, POP3S y NNTPS.

Como medidas preventivas, Symantec recomienda:

1. Instalar la actualización de seguridad recomendada por el Boletín de Seguridad de Microsoft MS04-011 (<http://www.microsoft.com/technet/security/bulletin/MS04-011.msp>)
2. Si no se requieren y no afecta su operación, deshabilitar los servicios que utilizan SSL. <http://support.microsoft.com/default.aspx?scid=kb:en-us;187498>
3. De ser posible y si no afecta su operación, filtrar los siguientes puertos:
UDP: 135-139, 445, 25, 563, 993 y 995.
TCP: 138-139, 445, 593, 25, 563, 993 y 995.

Es importante recordarles que es necesario que estas actualizaciones sean instaladas de manera prioritaria, ya que es posible ejecutar código remoto en los equipos comprometidos. Se espera que un worm que ataque esta vulnerabilidad, aparezca en los próximos días o semanas.

Rodrigo Hernández Burad (rhernand@itesm.mx)

Dirección de Seguridad de la Información

Vicerrectoría de Tecnologías de Información