

Windows XP y Vista también podrían ser vulnerables al ataque al generador de números aleatorios

Actualización (22-Nov, 10:05): Microsoft [acaba de confirmar](#) que **XP también está afectado**, aunque el bug será resuelto en el futuro Service Pack 3. También afirma que Vista y 2003 **no** están afectados.

Como algunos de nuestros lectores anticipaban, el ataque divisado tras el [criptoanálisis](#) recientemente aplicado al generador de números aleatorios de Windows 2000 podría ser extrapolable también al utilizado en Windows XP, 2003 y Vista, por cuanto las anunciadas mejoras parecen no haber sido nunca finalmente implementadas y Microsoft [responde con evasivas](#) cuando se le pregunta.

En todo caso, Microsoft niega la mayor, porque reconoce que se trata de una vulnerabilidad, pero no de una vulnerabilidad *de seguridad*, por cuanto la información sólo se muestra al usuario. Por su parte, los creadores del trabajo afirman que el peligro radica precisamente en que el usuario accede a una información que nunca debería mostrarse. Symantec coincide con Microsoft, pero lo califica como un "error de diseño".

Fuente: www.kriptopolis.org