

Tuesday, December 18, 2007

### **Dual\_EC\_DRBG added to Vista SP1**

Do you remember the article linking to Bruce Schneiers article about the possible backdoor in the NIST-endorsed Dual\_EC\_DRBG random number generator. Well exactly this algorithm was added to Microsoft Vista SP1.. As Bruce writes it in his blog:t's not enabled by default, and my advice is to never enable it. Ever.

Posted by Joerg Moellenkamp in English, Security at 14:20

HeHe, thank for the link... it's amazing know this kind of news  
Anonymous on Dec 18 2007, 22:26