

Debian Flaw Allows SSL Keys to be Cracked

Contributed by Administrator
Friday, 23 May 2008
Last Updated Friday, 23 May 2008

According to an announcement on the [debian.org](http://www.debian.org) security lists, a flaw in the random number generator of debian's openssl package has the potential to make any cryptographic key material generated by it guessable. This flaw, which according to the site was introduced in September of 2006, affects all major debian distributions including the very popular Ubuntu operating system. One of the most troubling aspects of this vulnerability is that it makes any SSL key generated by using OpenSSL on Debian potentially vulnerable. This flaw has the potential to lead to multiple security breaches, given the wide distribution of Debian based operating systems in the web hosting world and the large number of e-commerce sites that utilize SSL certificates for securing customer transactions. Any hosts that run Debian, or any webmasters whose sites are running a Debian server should immediately update their version of OpenSSL and re-issue all SSL certificates created with the old version. Instruction for rolling over keys can be found here <http://www.debian.org/security/key-rollover/> For more information, please visit www.debian.org .