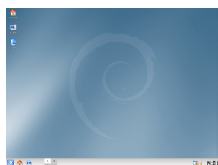


14 May 2008

By: Daniel Voicu, Linux Editor

Debian Desktop
Gnebu

Weakness in OpenSSL on Debian and Ubuntu Discovered

Immediate update is advised

If you are using Debian or any other distro that's based on it (such as Ubuntu), you are advised to update, because [a weakness was discovered](#) in the random number generator used by OpenSSL. To fix the problem, you will have to update the OpenSSL packages and regenerate any private keys made on Debian (Etch or newer) or Ubuntu 7.04 and higher. Because of this issue, some encryption keys are much simpler than they should be. An attacker could find the key through a brute-force attack. The encryption keys used in OpenSSH, OpenVPN and SSL certificates are the most affected by the weakness. Those generated with GnuPG or GNUTLS do not suffer from this vulnerability. OpenSSL version 0.98c-1 was the first vulnerable version and was uploaded in the unstable distribution on September 17, 2006. Since then, the data propagated to the testing and current stable (Etch) distributions. Sarge, the old distribution, is not vulnerable. The problem was caused by a patch to OpenSSL. Although the vulnerability affects operating systems based on Debian, it could indirectly affect other systems if a weak encryption key is imported into them. OpenSSL is an open-source implementation of the TLS and SSL protocols, and is based on SSLeay, a project by Eric Young and Tim Hudson, who stopped the development of their software at the end of 1998. The core library of OpenSSL is written in C, implementing the basic cryptographic functions. OpenSSL supports cryptographic algorithms like Blowfish, DES, RC2, IDEA, MD5, RSA and more. So, if you are using any of the following Linux distributions, you are advised to update immediately: Debian Etch; Ubuntu Feisty Fawn; Ubuntu Gutsy Gibbon; Ubuntu Hardy Heron. After you update the packages, regenerate all the private keys you've made on these systems.