

Re: OpenSSH affected by recent OpenSSL security problems?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2003-03/0302.html>

From: Nico Kadel-Garcia (nkadel@verizon.net)

Date: 03/23/03

From: Nico Kadel-Garcia <nkadel@verizon.net>

Date: Sun, 23 Mar 2003 22:25:31 GMT

Dimitri Maziuk wrote:

> *Neil W Rickert sez:*

>

>> iglesias@draco.acs.uci.edu (Mike Iglesias) writes:

>>

>>

>>> *There have been a couple of security problems with OpenSSL recently (timing based attack and the Klima-Pokorny-Rosa attack, see <http://www.openssl.org/> for more information). I was wondering if these issues affect OpenSSH, and how serious is this for OpenSSH. Basically I want to know how soon I need to rebuild OpenSSH with a new OpenSSL library for all the architectures we build it for.*

>>

>

>

>

>

>> *If you are using dynamic openssl libraries, then you should only need to rebuild those without recompiling openssh.*

>

>

> *That's what I thought. And then I found out that libcrypto's soname is 0.9.7 (old one had 0.9.6). So you can't upgrade from 0.9.6x to 0.9.7y without rebuilding openssh and everything else linked with openssl's so's.*

>

> *Dima*

Yes, you can. You have to build a spare set of compatibility libraries for old software you're not ready to replace: take a look at the RedHat RPM's for how such things can be done.