

comp.security.ssh: OpenSSH affected by recent OpenSSL security problems?

OpenSSH affected by recent OpenSSL security problems?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2003-03/0279.html>

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

Date: 03/21/03

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

Date: 21 Mar 2003 22:26:33 GMT

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.

Thanks,

--

Mike Iglesias

University of California, Irvine

Network & Academic Computing Services

Internet:

iglesias@draco.acs.uci.edu

phone:

949-824-6926

FAX:

949-824-2069