

Re: FreeBSD Security Advisory FreeBSD-SA-06:22.openssh

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2006-10/msg00006.html>

- *From:* Colin Percival <cperciva@xxxxxxxxxxx>
 - *Date:* Mon, 02 Oct 2006 14:25:05 -0700
-

Theo de Raadt wrote:

The OpenSSH project believe that the race condition can lead to a Denial of Service or potentially remote code execution

^^

Bullshit. Where did anyone say this?

The OpenSSH 4.4 release announcement says that, actually:

* Fix an unsafe signal handler reported by Mark Dowd. The signal handler was vulnerable to a race condition that could be exploited to perform a pre-authentication denial of service. On portable OpenSSH, this vulnerability could theoretically lead to
^^
pre-authentication remote code execution if GSSAPI authentication
^^
is enabled, but the likelihood of successful exploitation appears remote.

Colin Percival

freebsd-security@xxxxxxxxxxx mailing list
<http://lists.freebsd.org/mailman/listinfo/freebsd-security>
To unsubscribe, send any mail to "freebsd-security-unsubscribe@xxxxxxxxxxx"