

Re: [Full-Disclosure] IETF Draft – Fix for TCP vulnerability (fwd)

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-04/0150.html>

From: Mike Silbersack (*silby_at_silby.com*)

Date: 04/22/04

Date: Thu, 22 Apr 2004 01:28:20 -0500 (CDT)

To: Don Lewis <truckman@FreeBSD.org>

On Wed, 21 Apr 2004, Don Lewis wrote:

> *On 21 Apr, Mike Silbersack wrote:*
> > *Do you have access to a system that exhibits the "RST at end of window"*
> > *syndrome so that you could code up and test out this part of the patch?*
>
> *Nope. The only report of this that I saw was from jayanth. Judging by*
> *the tcpdump timestamps, it looks like whatever this wierd piece of*
> *hardware was, it was nearby.*

Something just occurred to me... we can just lump the "RST at end of window" case into the whole "RST somewhere in the window case". In that way, we only need two cases:

1. RSTs exactly at last_ack_sent (always accepted)
2. Everything else in the window (only accepted if "not under attack".)

I could code up and test this over the weekend, if it sounds like a solution we're willing to go with.

Mike "Silby" Silbersack

freebsd-security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"