

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

**Source:** <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-04/0148.html>

---

**From:** Don Lewis ([truckman\\_at\\_FreeBSD.org](mailto:truckman_at_FreeBSD.org))

**Date:** 04/22/04

Date: Wed, 21 Apr 2004 16:31:14 -0700 (PDT)

To: [silby@silby.com](mailto:silby@silby.com), [jayanth@yahoo-inc.com](mailto:jayanth@yahoo-inc.com)

On 21 Apr, Mike Silbersack wrote:

>

> *On Wed, 21 Apr 2004, Don Lewis wrote:*

>

>> > *1. Accept all RSTs meeting the criteria you just listed above.*

>>

>> *At this step, it would be better if we used the window size that was*

>> *advertised in the last packet sent, since that is what the sequence*

>> *number of the RST packet will be calculated from, while the window size*

>> *could have increased if data was consumed from the receive queue between*

>> *the time we sent the last packet and when we received the RST.*

>>

>> *It doesn't look like we keep the necessary data for this. Probably the*

>> *easiest thing to do would be to calculate the expected sequence number*

>> *in tcp\_output() and stash it in the pcb.*

>

> *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.

---

[freebsd-security@freebsd.org](mailto: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](mailto:freebsd-security-unsubscribe@freebsd.org)"