

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

*Source:* <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-04/0115.html>

---

**From:** Don Lewis (*truckman\_at\_FreeBSD.org*)

**Date:** 04/21/04

Date: Tue, 20 Apr 2004 20:11:55 -0700 (PDT)

To: avalon@caligula.anu.edu.au

On 21 Apr, Darren Reed wrote:

> *Forwarded message:*

>> *From full-disclosure-admin@lists.netsys.com Wed Apr 21 11:49:12 2004*

>> *To: full-disclosure@lists.netsys.com*

>> *From: Darren Bounds <dbounds@intrusense.com>*

>> *Subject: [Full-Disclosure] IETF Draft – Fix for TCP vulnerability*

>> *Date: Tue, 20 Apr 2004 18:19:58 -0400*

>>

>> -----BEGIN PGP SIGNED MESSAGE-----

>> *Hash: SHA1*

>>

>> <http://www.ietf.org/internet-drafts/draft-ietf-tcpm-tcpsecure-00.txt>

I saw this draft earlier today.

RFC793 [1] currently requires handling of a segment with the RST bit when in a synchronized state to be processed as follows:

- 1) If the RST bit is set and the sequence number is outside the expected window, silently drop the segment.
- 2) If the RST bit is set and the sequence number is acceptable i.e.:  
(RCV.NXT <= SEG.SEQ <= RCV.NXT+RCV.WND) then reset the connection.

Instead, the following changes should be made to provide some protection against such an attack.

- A) If the RST bit is set and the sequence number is outside the expected window, silently drop the segment.
- B) If the RST bit is exactly the next expected sequence number, reset the connection.
- C) If the RST bit is set and the sequence number does not exactly match the next expected sequence value, yet is within the acceptable window (RCV.NXT < SEG.SEQ <= RCV.NXT+RCV.WND) send an acknowledgment.

Our original implementation of the RST sequence number checking was much more permissive than RFC 793. I submitted a patch, which was included

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

in tcp\_input.c version 1.81 that implemented steps A and B above. It was discovered that this is incompatible with certain peers, so the code was changed to match RFC 793 in tcp\_input.c 1.98.

I don't know if adding step C will fix the problem. There may further info in the list archives.

---

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"