

## Re: Any status on timestamp vulnerability fix for 4.X?

**Source:** <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-06/0030.html>

---

**From:** Uwe Doering ([gemini\\_at\\_geminix.org](mailto:gemini_at_geminix.org))

**Date:** 06/29/05

Date: Wed, 29 Jun 2005 23:51:24 +0200

To: Richard Coleman <[rcoleman@criticalmagic.com](mailto:rcoleman@criticalmagic.com)>

Richard Coleman wrote:

> *Uwe Doering wrote:*

>

>> *Richard Coleman wrote:*

>>

>>> *Any information on when (or if) the following timestamp vulnerability  
>>> will be fixed for 4.X? Any information would be appreciated.*

>>>

>>> <http://www.kb.cert.org/vuls/id/637934>

>>

>> *FYI, the fix for RELENG\_5 applies to RELENG\_4 as is (apart from the  
>> CVS version header, of course):*

>>

>>

[http://www.freebsd.org/cgi/cvsweb.cgi/src/sys/netinet/tcp\\_input.c.diff?r1=1.252.2.15&r2=1.252.2.16&f=u](http://www.freebsd.org/cgi/cvsweb.cgi/src/sys/netinet/tcp_input.c.diff?r1=1.252.2.15&r2=1.252.2.16&f=u)

>>

>> *After verifying its semantic correctness for RELENG\_4 we've been  
>> running the patch for a couple of weeks now with no ill effects.*

>>

>> *I'm posting this also as an encouragement for committers to go ahead  
>> and do the MFC. It's low hanging fruit.*

>>

>> *Uwe*

>

> *We tried applying that diff to 4.10, but compilation failed with*

>

> *tcp\_input.o: In function 'tcp\_dooptions':*

> *tcp\_input.o(.text+0x21d8): undefined reference to 'TSTMP\_GT'*

>

> *Did you just define that macro? Or was something else required?*

Well, this MFC affected two files, actually. I didn't mention it explicitly because I considered it obvious from the accompanying CVS comment:

FreeBSD-Security: Re: Any status on timestamp vulnerability fix for 4.X?

----- cut here -----  
MFC: rev 1.270 of tcp\_input.c, rev 1.25 of tcp\_seq.h  
- Tighten up the Timestamp checks to prevent a spoofed segment from  
 setting ts\_recent to an arbitrary value, stopping further  
 communication between the two hosts.  
- If the Echoed Timestamp is greater than the current time,  
 fall back to the non RFC 1323 RTT calculation.  
----- cut here -----

So 'tcp\_seq.h' needs to be patched, too. Here's the direct link to that  
diff:

[http://www.freebsd.org/cgi/cvsweb.cgi/src/sys/netinet/tcp\\_seq.h.diff?r1=1.22.2.1&r2=1.22.2.2&f=u](http://www.freebsd.org/cgi/cvsweb.cgi/src/sys/netinet/tcp_seq.h.diff?r1=1.22.2.1&r2=1.22.2.2&f=u)

With both patches in place the kernel ought to compile correctly. Hope  
it works for you now.

Uwe

--  
Uwe Doering | EscapeBox - Managed On-Demand UNIX Servers  
geminix@geminix.org | <http://www.escapebox.net>

---

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"