

Re: OpenSSL buffer overflow

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2007-10/msg00005.html>

- *From:* Stefan Esser <se@xxxxxxxxxxx>
 - *Date:* Thu, 04 Oct 2007 15:39:08 +0200
-

Mike Tanca schrieb:

At 05:43 PM 9/28/2007, Stefan Esser wrote:

I did not see any commits to the OpenSSL code, recently; is anybody going to commit the fix?

See <http://www.securityfocus.com/archive/1/480855/30/0> for details ...

How serious is this particular issue ? Is it easily exploitable, or difficult to do ? Are some apps more at risk of exploitation than others ? e.g. ssh, apache ?

Seems that the following URL (from the FreeBSD Security Advisory) has a better formatted version of the same information as can be found at the location I had given:

<http://marc.info/?l=bugtraq&m=119091888624735>

A trailing '\0' can be written on the position following a buffer, with little effort. The BugTraq entry describes it in detail ...
But (AFAIK) no further analysis has been performed.

Regards, STefan

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