Tutorial: <https://www.youtube.com/watch?v=EECB9LLmPvc>

2.1) As the length decreases, so does the length of the output.

2.2) The boundary length of 22 results in a packet without any extra data.

3.1) Now that we updated the OpenSSL library, the attack is useless. Nothing is returned even with the –length option.

3.2) The problem is with this line:

*memcpy(bp, pl, payload);*

There is no check to determine if pl is valid or not. Therefore, a memory breach can occur.

Patches:

* Bounds checking before memcpy() is executed
* Server calculates packet size at runtime which requires additional overhead