

Heartbleed Bug

openssl / t1_lib.c

```
2584 tls1_process_heartbeat(SSL *s)
:
2610  buffer = OPENSSL_malloc(1 + 2 + payload + padding)
2611  bp = buffer;
2612
2613  /* Enter response type, length and copy payload */
2614  *bp++ = TLS1_HB_RESPONSE;
2615  s2n(payload, bp);
2616  memcpy(bp, pl, payload);
2617  bp += payload;
2618  /* Random padding */
2619  RAND_pseudo_bytes(bp, padding);
:
```