Heartbleed 취약점 소스코드 분석

```
2435    #ifndef OPENSSL_NO_HEARTBEATS
2436    int
2437    tls1_process_heartbeat(SSL *s)
2438        {
2439        unsigned char *p = &s->s3->rrec.data[0], *pl;
2440        unsigned short hbtype;
2441        unsigned int payload;
2442        unsigned int padding = 16;
2443
2444        hbtype = *p++;
2445        n2s(p, payload);
2446        pl = p;
```

Figure 1 Read Heartbeat Request Message

● Line 2439 실행 후: *p=1, p 위치=Request 메시지 1번째 바이트

직역	*p에 rrec.data[0] 대입, *p, *pl의 자료형은 unsigned char (1byte)
기능	p는 Heartbeat Request 메시지가 저장된 메모리의 첫 주소 지정
맥락	포인터 p로 Heartbeat Request 메시지를 다룰 예정

● Line 2444 실행 후: hbtype=1, p 위치= Request 메시지 2번째 바이트

직역	hbtype에 *p(1byte)를 자동 형변환하여 대입 후, p를 상위주소로 1byte 이동
기능	hbtype에 요청 타입값 0x01 저장, p는 2번째 byte 지정
맥락	Request 메시지에 대한 Response 메시지를 생성하게 함 (line 2453)

● Line 2445 실행 후: payload=페이로드 길이, p 위치=Request 메시지 4번째 바이트

직역	p부터 2바이트를 읽어 payload에 대입 후, p를 상위주소로 2byte 이동
기능	payload에 Request 메시지의 Payload Length 값 저장
맥락	Response 메시지에 쓰일 Payload Length 값 저장

● Line 2446 실행 후: pl 위치=Request 메시지 4번째 바이트

직역	pl에 p를 대입
기능	pl은 Request 메시지 4번째 바이트(payload 필드 시작주소) 지정
맥락	Response 메시지 구성할 때 사용

```
2453        if (hbtype == TLS1_HB_REQUEST)
2454            {
2455            unsigned char *buffer, *bp;
2456            int r;
2457
2458            buffer = OPENSSL_malloc(1 + 2 + payload + padding);
2459            bp = buffer;
2460
2461            *bp++ = TLS1_HB_RESPONSE;
2462            s2n(payload, bp);
2463            memcpy(bp, pl, payload);
2464
2465            bp += payload;
2466            RAND_pseudo_bytes(bp, padding);
2467
2468            r = ssl3_write_bytes(s, TLS1_RT_HEARTBEAT, buffer,\
2469                                    3 + payload + padding);
```

Figure 2 Write Heartbeat Response Message

● Line 2458 실행 후: buffer=Heartbeat Response 메시지 버퍼 시작 주소

직역	bp에 buffer 값 대입
기능	bp는 포인터이므로 하위주소에서 상위주소로 저장 가능
맥락	bp로 Response 메시지 다룰 예정

● Line 2459 실행 후: bp=Heartbeat Response 메시지 버퍼 시작 주소

직역	bp에 buffer 값 대입
기능	bp는 포인터이므로 하위주소에서 상위주소로 저장 가능
맥락	bp로 Response 메시지 다룰 예정

● Line 2461 실행 후: *bp=2, bp=Heartbeat Response 메시지 2번째 바이트

직역	*bp에 TLS1_HB_RESPONSE(2) 저장 후, bp를 상위주소로 2byte 이동
기능	Response 메시지 Type 필드 값 저장 후, bp는 메시지 2번째 byte 지정
맥락	Response 메시지에 Type 필드값 저장

● Line 2462 실행 후: bp=Heartbeat Response 메시지 4번째 바이트

직역	변수 payload(2byte)를 읽어 빅 엔디안으로 변환 후, bp에 저장 후 bp를 상위주소로 2byte 이동
기능	bp에 Payload Length값 저장
맥락	Response 메시지에 Payload Length 빅 엔디안 방식으로 저장

● Line 2463 실행 후:

직역	pl부터 변수 payload 값만큼 읽어 bp에 쭉 저장
기능	pl이 가리키는 주소부터 payload(Reqeust 메시지 Payload Legth값) 값만큼 bp에 복사
맥락	조작된 경우 버퍼 Out-of-bound Read 발생

● Line 2468 실행 후:

직역	*buffer(Response 메시지 전체)를 ssl3_write_bytes() 함수에서 처리
기능	*buffer를 암호화 후 전송
맥락	Response 메시지 전송