

3.4 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 3 Read Heartbeat Request Message (출처: OpenSSL_1_0_1/ssl/t1_lib.c)

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

직역	*p 에 rrec.data[0] 대입, *p, *pl 의 자료형은 unsigned char (1byte)
기능	p 는 Heartbeat Request 메시지가 저장된 메모리의 첫 주소 지정
맥락	포인터 p 로 Heartbeat Request 메시지를 다룰 예정

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

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

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

직역	p 부터 2 바이트를 읽어 payload 에 대입 후, p 를 상위주소로 2byte 이동
기능	payload 에 Request 메시지의 Payload Length 값 저장
맥락	Response 메시지에 쓰일 Payload Length 값 저장

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

직역	pl 에 p 를 대입
기능	pl 은 Request 메시지 4 번째 바이트(payload 필드 시작 주소) 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 4 Write Heartbeat Response Message (출처: OpenSSL_1_0_1/ssl/t1_lib.c)

- Line 2453 실행 후:

직역	Hbtype 이 TLS1_HB_REQUEST(1) 이라면
기능	Response 메시지 작성 기능으로 분기
맥락	Response 메시지 작성

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

직역	buffer 에 동적할당한 메모리 주소 대입
기능	Response 메시지 구성 시 필요한 저장공간 확보
맥락	Response 메시지 구성에 필요한 메모리 동적할당

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

지역	bp 에 buffer 값 대입
기능	bp 는 포인터이므로 하위주소에서 상위주소로 저장 가능
맥락	bp 로 Response 메시지 다룰 예정

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

지역	*bp 에 TLS1_HB_RESPONSE(2) 저장 후, bp 를 상위주소로 2byte 이동
기능	Response 메시지 Type 필드 값 저장 후, bp 는 메시지 2 번째 byte 지정
맥락	Response 메시지에 Type 필드값 저장

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

지역	변수 payload(2byte)를 읽어 빅 엔디안으로 변환 후, bp 에 저장 후 bp 를 상위주소로 2byte 이동
기능	bp 에 Payload Length 값 저장
맥락	Response 메시지에 Payload Length 빅 엔디안 방식으로 저장

- Line 2463 실행 후:

지역	pl 부터 변수 payload 값만큼 읽어 bp 에 쪽 저장
기능	pl 이 가리키는 주소부터 payload(Request 메시지 Payload Length 값) 값만큼 bp 에 복사
맥락	조작된 경우 버퍼 Out-of-bound Read 발생

- Line 2468 실행 후:

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