Remote Heap-Based Buffer Underflow Vulnerability at BuptLab dns relay server

Written by : Antonius (w1sdom)
Web : www.bluedragonsec.com
Github : https://github.com/bluedragonsecurity
Vulnerability discovered by : Antonius
Date of Discovery : March 6 2026

On March 6 2026 I discovered a buffer underflow vulnerability at BuptLab dns relay server.

BuptLab dns relay server is a dns relay server developed by Agicy from Beijing University. Here is the repository of BuptLab dns relay server : https://github.com/agicy/buptLab-dns_relay_server

The vulnerability occurs when the dns relay server processed a 5 bytes of truncated dns packet. Here is the the packet that triggers the vulnerability at BuptLab dns relay server :

```
# xxd poc_dns_packet.bin
00000000: a77e 0014 a6
# wc -c poc_dns_packet.bin
5 poc_dns_packet.bin
```

The packet doesn't have a completed dns header, it's a truncated dns packet.

Source Code Analysis

The asan log indicates a write of 1 byte outside the boundary of buffer :

==22332==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7b96a5d245ef at pc

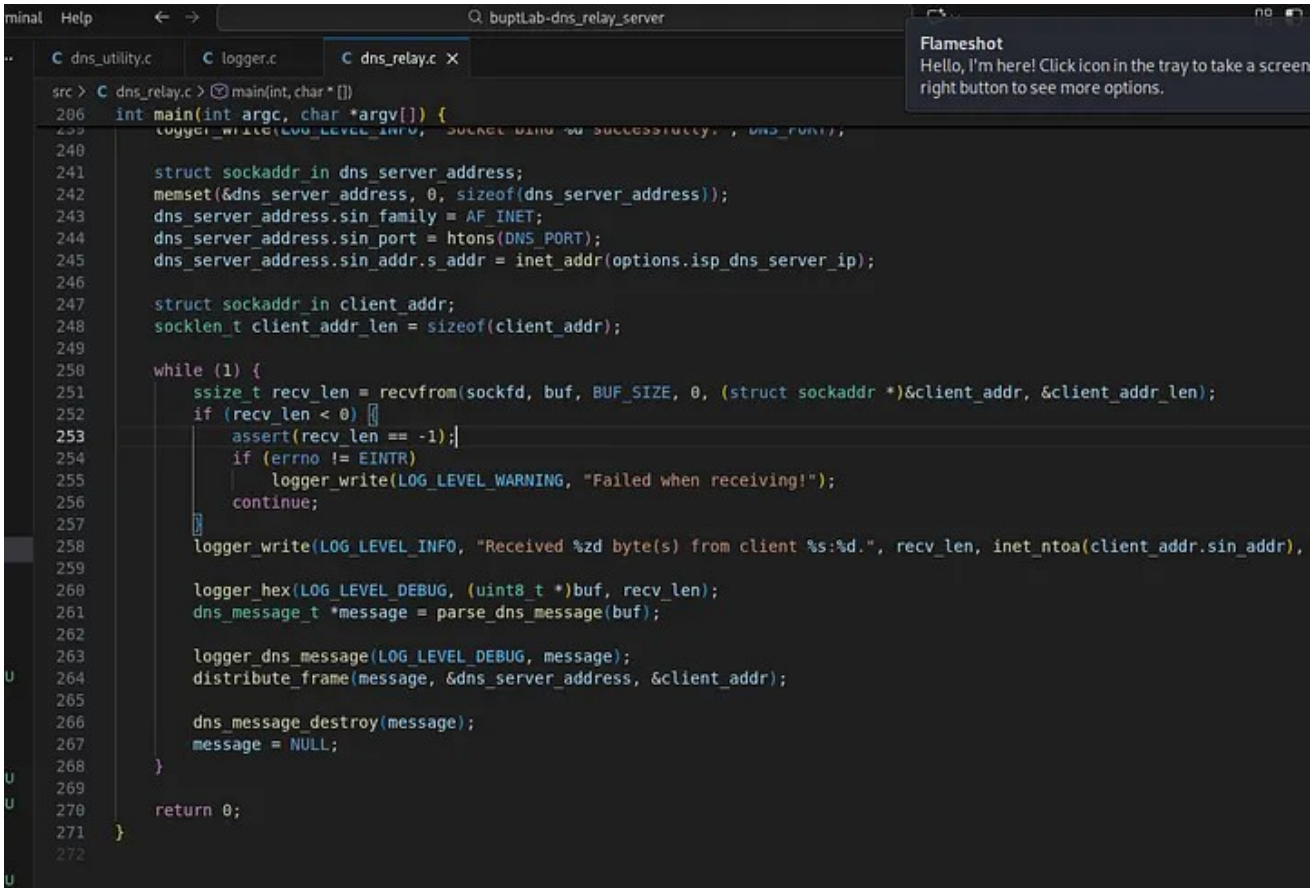
0x55d5fd9b3604 bp 0x7fffcbf8a090 sp 0x7fffcbf8a088

WRITE of size 1 at 0x7b96a5d245ef thread T0
#0 0x55d5fd9b3603 in get_name_from_name_field src/network/dns_utility.c:41
#1 0x55d5fd9bd123 in logger_dns_message src/module/logger.c:153
#2 0x55d5fd9af98e in main src/dns_relay.c:263
#3 0x7f76a6a29f67 in __libc_start_call_main ../sysdeps/nptl/libc_start_call_main.h:58
#4 0x7f76a6a2a024 in __libc_start_main_impl ../csu/libc-start.c:360
#5 0x55d5fd9af3c0 in _start
(/home/robohax/Desktop/fuzz/dns/buptLab-dns_relay_server/dns_relay+0x1f3c0) (BuildId:
c5699f255c9870f6ad7559482666aea647197291)

More specifically it's a write of 1 byte before the allocated buffer region

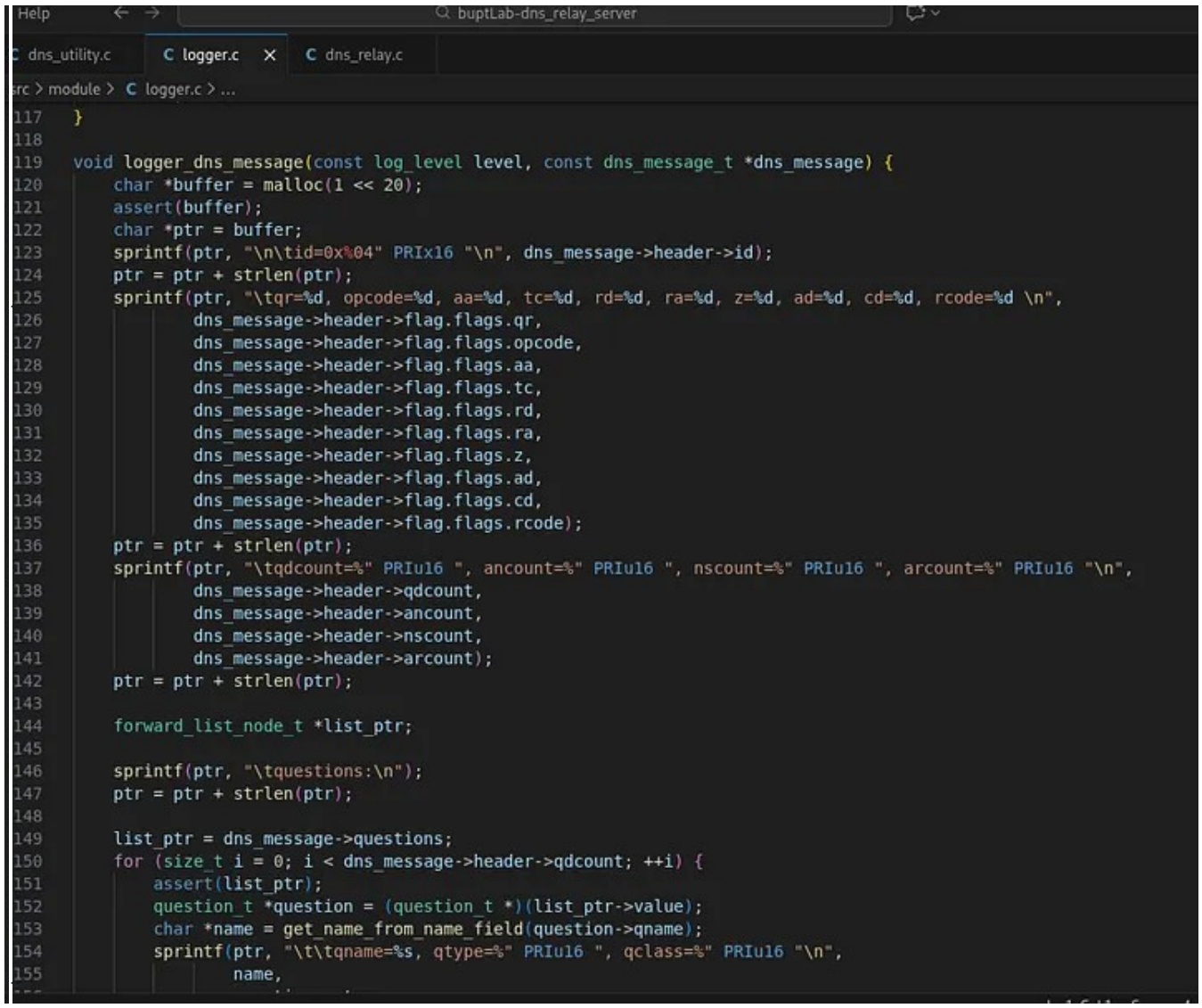
0x7b96a5d245ef is located 1 bytes before 1-byte region [0x7b96a5d245f0,0x7b96a5d245f1)
allocated by thread T0 here:
#0 0x7f76a771a0ab in malloc ../../../../src/libsanitizer/asan/asan_malloc_linux.cpp:67
#1 0x55d5fd9b3281 in get_name_from_name_field src/network/dns_utility.c:31
#2 0x55d5fd9bd123 in logger_dns_message src/module/logger.c:153
#3 0x55d5fd9af98e in main src/dns_relay.c:263
#4 0x7f76a6a29f67 in __libc_start_call_main ../sysdeps/nptl/libc_start_call_main.h:58

Based on the error message only we can determine that there is a buffer underflow vulnerability that triggered because of the truncated dns packet.



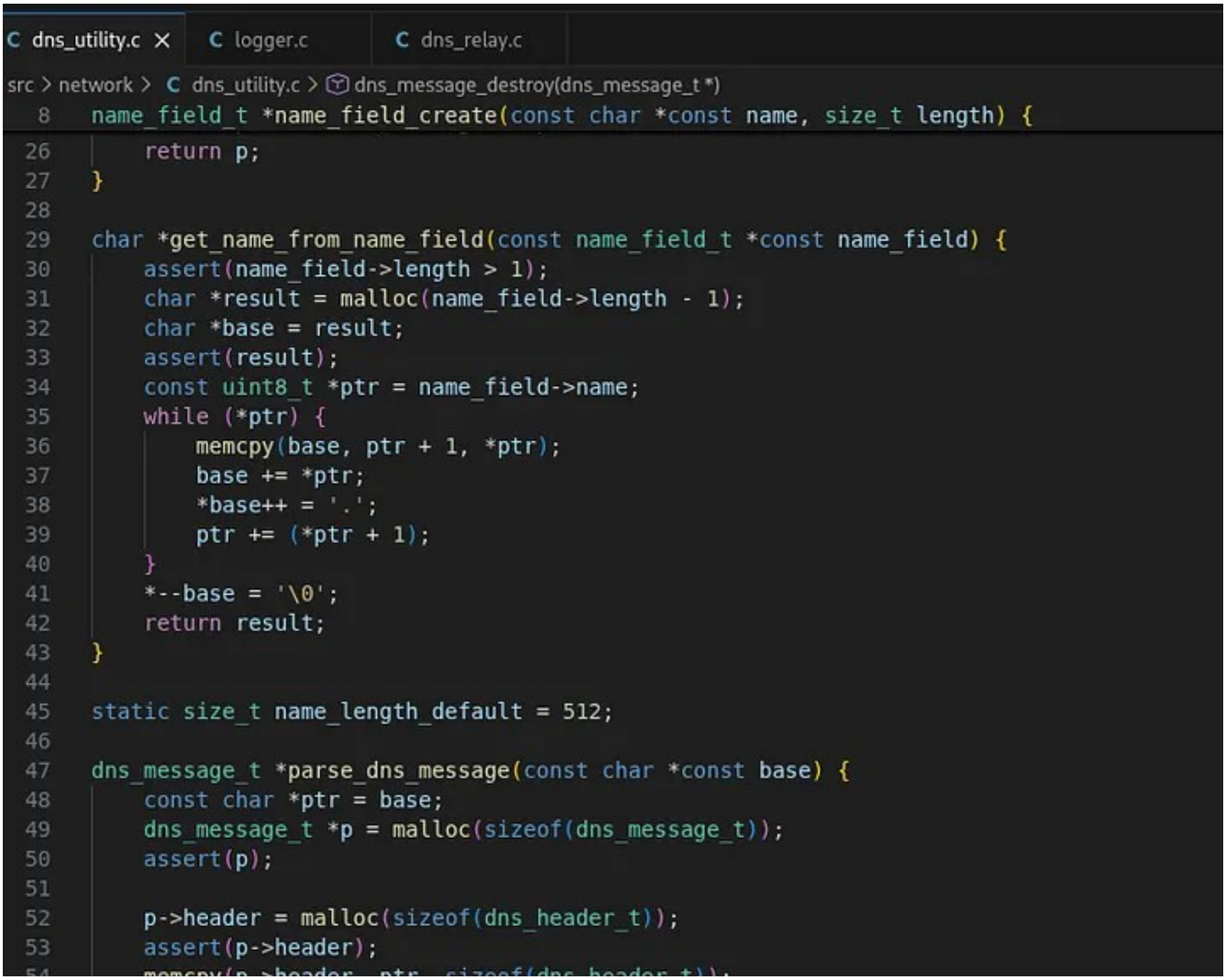
in dns_relay.c line 263, we can see the bug triggered by logger_dns_message(LOG_LEVEL_DEBUG, message) function call.

Let’s check the logger_dns_message function at modules/logger.c :



in line 153 the vulnerability triggered by a call to get_name_from_name_field :

char *name = get_name_from_name_field(question->qname);



The vulnerability occurs since this loop never occurs :

```
while (*ptr) {
    memcpy(base, ptr + 1, *ptr);
    base += *ptr;
    *base++ = '.';
    ptr += (*ptr + 1);
}
```

The loop won’t run since name_field->name[0] == 0

```
*--base = '\0';
```

This code will shift the pointer position 1 step backward and fill the last character with null terminated string.

Since the name_field->name is Null, the base[-1] will be overwritten by null terminated string, hence a buffer underflow occurs !

POC

https://github.com/bluedragonsecurity/buptLab-dns_relay_server_remote_heap_based_buffer_underflow/blob/main/poc.c

References

https://medium.com/@w1sdom/remote-heap-based-buffer-underflow-vulnerability-at-buptlab-dns-relay-server-bac6505070a9

https://github.com/bluedragonsecurity/buptLab-dns_relay_server_remote_heap_based_buffer_underflow