FRRouting / frr Public

Code Issues 407 Pull requests 143 Discussions Actions ···

New issue

Jump to bottom

Miss a check on length in Babel #10487

Closed whichbug opened this issue on Feb 2 · 3 comments · Fixed by #10494

whichbug commented on Feb 2 • edited

The code below misses a check on the relationship between `packetlen` and `bodylen` before Line 298, which may lead to buffer overflows when accessing the memory at Line 300 and Line 309.

frr/babeld/message.c
Lines 289 to 309 in `3d1ff4b`

```
289    babel_packet_examin(const unsigned char *packet, int packetlen)
290    {
291        unsigned i = 0, bodylen;
292        const unsigned char *message;
293        unsigned char type, len;
294
295        if(packetlen < 4 || packet[0] != 42 || packet[1] != 2)
296            return 1;
297        DO_NTOHS(bodylen, packet + 2);
298        while (i < bodylen){
299            message = packet + 4 + i;
300            type = message[0];
```

To fix, we may put the code below before the while loop:

```
if (packetlen < bodylen + 4) {
    debugf(BABEL_DEBUG_COMMON,"Received truncated message.");
    return 1;
}
```

The output of the address sanitizer:

```
==271648==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x603000000114 at pc
0x00000059301a bp 0x7fff3f7301f0 sp 0x7fff3f7301e8
READ of size 1 at 0x603000000114 thread T0
    #0 0x593019 in babel_packet_examin /home/parallels/myfrr/babeld/message.c:300:16
    #1 0x593019 in parse_packet /home/parallels/myfrr/babeld/message.c:354:9
```

whichbug pushed a commit to whichbug/frr that referenced this issue on Feb 3

`babeld: fix FRRouting#10487 by adding a check on packet length` ff0f99d

qlyoung commented on Feb 3 Member

Awesome! Since you already have a fix, would you be willing to submit the patch as a PR? That would be super helpful.

whichbug mentioned this issue on Feb 3

babeld: add a check for truncated packets #10494

Merged

whichbug pushed a commit to whichbug/frr that referenced this issue on Feb 3

`babeld: fix FRRouting#10487 by adding a check on packet length` … 32d3742

whichbug commented on Feb 3 Author

> Awesome! Since you already have a fix, would you be willing to submit the patch as a PR? That would be super helpful.

Thanks for your reply. I have created the pull request.

whichbug pushed a commit to whichbug/frr that referenced this issue on Feb 4

`babeld: fix FRRouting#10487 by adding a check on packet length` … 6a0b68a

whichbug pushed a commit to whichbug/frr that referenced this issue on Feb 4

`babeld: fix FRRouting#10487 by adding a check on packet length` … 50044ec

idryzhov closed this as completed in #10494 on Feb 6

plsaranya pushed a commit to plsaranya/frr that referenced this issue on Feb 28

```
babeld: fix FRRouting#10487 by adding a check on packet length …                                   02d7418
```

qlyoung commented on Mar 28 • edited ▾ Member

This has been assigned CVE-2022-26127 with a severity score of 7.8.

No assessment of exploitability has been made.

Please see my comment here

patrasar pushed a commit to patrasar/frr that referenced this issue on Apr 28

```
babeld: fix FRRouting#10487 by adding a check on packet length …                                   805b4d5
```

gpnaveen pushed a commit to gpnaveen/frr that referenced this issue on Jun 7

```
babeld: fix FRRouting#10487 by adding a check on packet length …                                   8645122
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

babeld: add a check for truncated packets
whichbug/frr

2 participants