Incorrect checks on length in babeld #10502

Closed db-sca opened this issue on Feb 4 · 2 comments · Fixed by #10504

db-sca commented on Feb 4 • edited

The check at Line 310 is not correct. It should be `i + len + 2 > bodylen` rather than `i + len > bodylen`, because `len` does not include the first two bytes, i.e., `message[0]` and `message[1]`

frr/babeld/message.c
Lines 300 to 312 in `ab68283`

```
300       type = message[0];
301       if(type == MESSAGE_PAD1) {
302           i++;
303           continue;
304       }
305       if(i + 1 > bodylen) {
306           debugf(BABEL_DEBUG_COMMON,"Received truncated message.");
307           return 1;
308       }
309       len = message[1];
310       if(i + len > bodylen) {
311           debugf(BABEL_DEBUG_COMMON,"Received truncated message.");
```

db-sca commented on Feb 4 • edited Author

The check at Line 305 is also incorrect. It should be `i + 2 > bodylen` rather than `i + 1 > bodylen`.

You may feed the packet "2a:02:00:01:02" to the function to reproduce an overflow at Line 309.

db-sca changed the title ~~An incorrect check on length in babeld~~ Incorrect checks on length in babeld on Feb 4

qingkaishi added a commit to qingkaishi/frr that referenced this issue on Feb 4

`babeld: fix FRRouting#10502 FRRouting#10503 by repairing the checks o…` … 05a1985

qingkaishi mentioned this issue on Feb 4

babeld: fix the checks for truncated packets #10504

Merged

qingkaishi added a commit to qingkaishi/frr that referenced this issue on Feb 4

`babeld: fix FRRouting#10502 FRRouting#10503 by repairing the checks o…` … c379335

donaldsharp closed this as completed in #10504 on Feb 8

mergify bot pushed a commit that referenced this issue on Feb 8

`babeld: fix #10502 #10503 by repairing the checks on length` … ✕ 8d45143

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

`babeld: fix FRRouting#10502 FRRouting#10503 by repairing the checks o…` … ac79863

qlyoung commented on Mar 28 Member

Assigned CVE-2022-26128 with a 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#10502 FRRouting#10503 by repairing the checks o…` … 5916eb6

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

`babeld: fix FRRouting#10502 FRRouting#10503 by repairing the checks o…` … 8876609

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

babeld: fix the checks for truncated packets
qingkaishi/frr

2 participants