

New issue

[Jump to bottom](#)

babeld: bugs in parse_hello_subtlv, parse_ihu_subtlv, and parse_update_subtlv #10503

✓ Closed

qingkaishi opened this issue on Feb 4 · 6 comments · Fixed by [#10504](#)

Labels

triage

qingkaishi commented on Feb 4

Contributor

[frr/babeld/message.c](#)

Lines 131 to 151 in e743c1b

```
131     parse_update_subtlv(const unsigned char *a, int alen,
132                        unsigned char *channels)
133     {
134         int type, len, i = 0;
135
136         while(i < alen) {
137             type = a[i];
138             if(type == SUBTLV_PAD1) {
139                 i++;
140                 continue;
141             }
142
```

Line 143: the condition should be `i + 1 >= alen` instead of `i + 1 > alen`. Otherwise, overflows will happen at 147.

Line 148: the condition should be `i + len + 2 > alen` instead of `i + len > alen`. We need include extra two bytes, `a[i]` and `a[i + 1]` in this check.

 qingkaishi added the **triage** label on Feb 4

qingkaishi commented on Feb 4

Contributor

Author

[frr/babeld/message.c](#)

Lines 179 to 201 in e743c1b

```
179     parse_hello_subtlv(const unsigned char *a, int alen,
180                        unsigned int *hello_send_us)
181     {
182         int type, len, i = 0, ret = 0;
183
184         while(i < alen) {
185             type = a[0];
186             if(type == SUBTLV_PAD1) {
187                 i++;
188                 continue;
189             }
190
```

Line 185: it should be `a[i]` instead of `a[0]` .

Line 191: the condition should be `i + 1 >= alen` instead of `i + 1 > alen`

Line 197: the condition should be `i + len + 2 > alen` instead of `i + len > alen`

qingkaishi commented on Feb 4 • edited ▼

Contributor

Author

[frr/babeld/message.c](#)

Lines 224 to 247 in e743c1b

```
224     parse_ihu_subtlv(const unsigned char *a, int alen,
225                     unsigned int *hello_send_us,
226                     unsigned int *hello_rtt_receive_time)
227     {
228         int type, len, i = 0, ret = 0;
229
230         while(i < alen) {
231             type = a[0];
232             if(type == SUBTLV_PAD1) {
233                 i++;
234                 continue;
235             }

```

Line 231: it should be `a[i]` instead of `a[0]` .

Line 237: the condition should be `i + 1 >= alen` instead of `i + 1 > alen` .

Line 243: the condition should be `i + len + 2 > alen` instead of `i + len > alen` .

idryzhov commented on Feb 4

Contributor

Hi @qingkaishi, thanks for letting everyone know about the issues.
But as you already know how to fix all of them, it would be much easier for us if you provide a PR with the fixes instead.

qingkaishi commented on Feb 4

Contributor

Author

Hi @qingkaishi, thanks for letting everyone know about the issues. But as you already know how to fix all of them, it would be much easier for us if you provide a PR with the fixes instead.

Sure. I will do that soon.

idryzhov commented on Feb 4

Contributor

Thanks!

 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  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

This has been assigned [CVE-2022-26129](#) 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#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

triage

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

3 participants

