

FRRouting / frr Public

<> Code Issues 375 Pull requests 363 Discussions Actions Projects

Commit 693a2e0

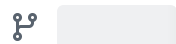


ton31337 committed on Mar 10

bgpd: Check if the NHC length is enough to fill TLV value + TLV header
BGP_NHC_TLV_MIN_LEN is 4 bytes (TLV code + TLV length), and when we parse TLVs, we subtract BGP_NHC_TLV_MIN_LEN as well, so we should include BGP_NHC_TLV_MIN_LEN when checking the remaining length too.

Reported-by: Jiahao Lei

Signed-off-by: Donatas Abraitis <donatas@opensourcerouting.org>



1 parent [d6671d4](#) commit 693a2e0

1 file changed

+1 -1

Top



▼ bgpd

bgp_attr.c



▼ bgpd/bgp_attr.c

```

@@ -3887,7 +3887,7 @@ static int bgp_attr_nhc(struct bgp_attr_parser_args
 *args)
3887 3887         tlv_code = stream_getw(s);
3888 3888         tlv_length = stream_getw(s);
3889 3889
3890 -         if (length < tlv_length) {
3890 +         if (length < tlv_length + BGP_NHC_TLV_MIN_LEN) {

```

```
3891 3891         zlog_err("%pBP rcvd BGP NHC TLV length %d exceeds remaining
length %d",
3892 3892         peer, tlv_length, length);
3893 3893         bgp_nhc_free(nhc);
```



Comments 0



Please [sign in](#) to comment.