

FRRouting / frr Public

<> Code Issues 374 Pull requests 361 Discussions Actions Projects

Commit 0e6882b



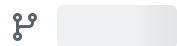
Jafaral committed on Mar 9 · ✓ 20 / 21

bgpd: fix off-by-one error in FlowSpec operator array bounds check

Change loop > BGP_PBR_MATCH_VAL_MAX to loop >= BGP_PBR_MATCH_VAL_MAX in bgp_flowspec_op_decode() and bgp_flowspec_bitmask_decode() to prevent writing one element past the end of the mval[] array when more than 5 chained operators are present in a FlowSpec component.

Reported-by: Jiahao Lei

Signed-off-by: Jafar Al-Gharaibeh <jafar@atcorp.com>



1 parent [dab7ac7](#) commit 0e6882b

1 file changed

+4 -2

↑ Top ⚙️

Filter files...

bgpd

bgp_flowspec_util.c

Search within code ⚙️

bgpd/bgp_flowspec_util.c

```

@@ -274,8 +274,10 @@ int bgp_flowspec_op_decode(enum
    bgp_flowspec_util_nlri_t type,
274 274     }
275 275
276 276     do {
277 -         if (loop > BGP_PBR_MATCH_VAL_MAX)
277 +         if (loop >= BGP_PBR_MATCH_VAL_MAX) {

```

```
278 278          *error = -2;
279 +          return offset;
280 +      }
279 281
280 282          if (offset >= max_len) {
281 283          *error = -1;
@@ -397,7 +399,7 @@ int bgp_flowspec_bitmask_decode(enum
bgp_flowspec_util_nlri_t type,
397 399      }
398 400
399 401      do {
400 -          if (loop > BGP_PBR_MATCH_VAL_MAX) {
402 +          if (loop >= BGP_PBR_MATCH_VAL_MAX) {
401 403          *error = -2;
402 404          return offset;
403 405      }

```

Comments 0



Please [sign in](#) to comment.