osrg / **gobgp** Public

Code | Issues 198 | Pull requests 26 | Actions | Security and quality 3

Commit `76d9110`

fujita committed on Apr 1 · 80 / 80

```
packet/mrt: fix uint16 underflow in parseRibEntry path attribute loop

Add a bounds check on totalLen before entering the loop, and check
that each path attribute length does not exceed the remaining
attribute length to prevent uint16 underflow on subtraction.

Signed-off-by: FUJITA Tomonori <fujita.tomonori@gmail.com>
```

`master` (#3357) · v4.5.0 v4.4.0

1 parent bc77597 commit 76d9110

1 file changed +7 -3

Top

Filter files...

pkg/packet/mrt

mrt.go

Search within code

pkg/packet/mrt/mrt.go

```
@@ -413,6 +413,9 @@ func parseRibEntry(data []byte, family bgp.Family,
isAddPath bool, prefix ...bgp
413 413         }
414 414         totalLen := binary.BigEndian.Uint16(data[:2])
415 415         data = data[2:]
    416 +       if len(data) < int(totalLen) {
    417 +           return nil, nil, errNotAllRibEntryBytesAvailable
    418 +       }
```

```
416  419          options := &bgp.MarshallingOption{
417  420              MRT: true,
418  421          }
     @@ -441,10 +444,11 @@ func parseRibEntry(data []byte, family bgp.Family,
     isAddPath bool, prefix ...bgp
441  444              mp.Value = []bgp.PathNLRI{{NLRI: prefix[0], ID: e.PathIdentifier}}
442  445          }
443  446
444       -          attrLen -= uint16(p.Len())
445       -          if len(data) < p.Len() {
446       -              return nil, nil, errNotAllRibEntryBytesAvailable
     447  +          pLen := uint16(p.Len())
     448  +          if pLen > attrLen {
     449  +              return nil, nil, fmt.Errorf("path attribute length %d exceeds
     remaining attribute length %d", pLen, attrLen)
447  450          }
     451  +          attrLen -= pLen
448  452          data = data[p.Len():]
449  453          e.PathAttributes = append(e.PathAttributes, p)
450  454      }
```

Comments 0

Please sign in to comment.