

[New issue](#)[Jump to bottom](#)

# [Bug] Format string vulnerability in fix\_ipv6\_checksums() function #723

✓ Closed

tin-z opened this issue on Mar 28 · 1 comment

Projects

 4.4.2

tin-z commented on Mar 28

## Describe the bug

Tcpreplay version 4.4.1 contains a memory leakage flaw, CWE-134 vulnerability in fix\_ipv6\_checksums() function. The highest threat from this vulnerability is to data confidentiality. The inputs required to exploit the vulnerability is unknown.


[tcpreplay/src/tcpedit/edit\\_packet.c](#)

Lines 160 to 166 in 09f0774

```
160     if (pkthdr->caplen == pkthdr->len) {
161         int ip6_len = ipv6_header_length(ip6_hdr, pkthdr->len, l2len);
162         if (ip6_hdr->ip_len < ip6_len) {
163             tcpedit_setwarn(tcpedit, "Unable to checksum IPv6 packet with invalid: pkt=" COUNTED);
164             tcpedit->runtime.packetnum, ip6_hdr->ip_len);
165             return TCPEDIT_WARN;
166         }
```

## Additional context

A patch was proposed in the following pull request: [#720](#)

  fklassen added this to **To do** in 4.4.2 on Apr 22  fklassen moved this from **To do** to **In progress** in 4.4.2 on Aug 1

fklassen commented on Aug 1

Member

Fixed in PR [#720](#)



fklassen closed this as completed on Aug 1



4.4.2 [automation](#) moved this from In progress to Done on Aug 1

#### Assignees

No one assigned

#### Labels

None yet

#### Projects



4.4.2

Done

#### Milestone

No milestone

#### Development

No branches or pull requests

2 participants

