Closed Issue created 2 months ago by **Jason Cohen**

f5ethtrailer: Infinite loop in legacy style dissector

Summary

Under certain circumstances the dissector will enter an infinite loop trying to dissect a trailer.

Steps to reproduce

f5ethtrailer.pref_walk_trailer: TRUE Malformed / corrupt packet such that heuristic signature matches possible legacy trailer, but a would be length field is larger than remaining bytes in TLV.

```
» tshark-git -o f5ethtrailer.pref_walk_trailer:TRUE -r trailer_walk_hang.pcap
    1   0.000000 00:00:00_00:00:00  00:00:00_00:00:00   FILEINFO  296 tcpdump -vv -s0 -ni 0.0:nnn -w
    2  93.541785 10.178.128.52 51289 160.254.173.245 10133 35 UDP  1338 51289 → 10133 Len=205
^C^Z
[2]  + 1076 suspended  tshark-git -o f5ethtrailer.pref_walk_trailer:TRUE -r trailer_walk_hang.pcap
```

Can't SIGINT, must SIGKILL

What is the current bug behavior?

*shark fails to move past subject frame and spins in loop.

What is the expected correct behavior?

Dissector should bail out of dissection and reject the data.

Sample capture file

(If possible attach a sample capture file, not screenshot of dissection, showing this issue)

trailer_walk_hang.pcap

Build information

```
» tshark-git -v
TShark (Wireshark) 4.1.0 (v4.1.0rc0-138-gdba3c64d6e74).

Copyright 1998-2022 Gerald Combs <gerald@wireshark.org> and contributors.
Licensed under the terms of the GNU General Public License (version 2 or later).
This is free software; see the file named COPYING in the distribution. There is
NO WARRANTY; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

Compiled (64-bit) using GCC 10.2.1 20210110, with GLib 2.66.8, with PCRE2, with
zlib 1.2.11, with libpcap, with POSIX capabilities (Linux), with libnl 3, with
Lua 5.2.4, without GnuTLS, with Gcrypt 1.8.8, with Kerberos (MIT), without
MaxMind, without nghttp2, without brotli, with LZ4, with Zstandard, with Snappy,
with libxml2 2.9.10, with libsmi 0.4.8, with binary plugins.

Running on Linux 5.10.102.1-microsoft-standard-WSL2, with Intel(R) Core(TM)
i7-9850H CPU @ 2.60GHz (with SSE4.2), with 25436 MB of physical memory, with
GLib 2.66.8, with PCRE2 10.36 2020-12-04, with zlib 1.2.11, with libpcap 1.10.0
(with TPACKET_V3), with c-ares 1.17.1, with Gcrypt 1.8.8, with LZ4 1.9.3, with
Zstandard 1.4.8, with libsmi 0.4.8, with LC_TYPE=en_US.UTF-8, binary plugins
supported.
```

Edited 2 months ago by Gerald Combs

Tasks 0

No tasks are currently assigned. Use tasks to break down this issue into smaller parts.

Linked items 0

Link issues together to show that they're related or that one is blocking others. Learn more.

Related merge requests 1

f5ethtrailer: Fix possible infinite loop in legacy trailer heuristic

!7981

When this merge request is accepted, this issue will be closed automatically.

Activity

Jason Cohen mentioned in merge request !7981 (merged) 2 months ago

Gerald Combs closed via merge request !7981 (merged) 2 months ago

Gerald Combs changed title from **f5ethtrailer: infinite loop in legacy style dissector** to **f5ethtrailer: Infinite loop in legacy style dissector** 2 months ago

Gerald Combs @geraldcombs · 2 months ago Owner

CVE-2022-3190

Please register or sign in to reply