Suricata - Bug #3846
Infinite loop if the sniffing interface temporarily goes down
07/27/2020 03:10 PM - Dan Moinescu

Status: New
Priority: Normal
Assignee:
Category:
Target version:
Affected Versions:
Effort:
Difficulty:
Label:

Description
How to reproduce: start suricata in live-pcap mode. Bring the sniffing interface down with ip link set(interface_name) down, then bring it up again.

Suricata doesn't exit, but it no longer produces events either.

The problem appears to be that function ReceivePcapLoop keeps calling PcapTryReopen in a loop, which in turn keeps returning PCAP_ERROR_ACTIVATED, resulting in an infinite loop.

The following patch fixes it:

```c
--- a/src/source-pcap.c
+++ b/src/source-pcap.c
@@ -250,6 +250,7 @@ TmEcode ReceivePcapLoop(ThreadVars *tv, void *data, void *slot)
     ptv->cb_result = TM_ECODE_OK;
+    TmEcode retval = TM_ECODE_OK;
     while (1) {
         if (suricata_ctl_flags & SURICATA_STOP) {
@@ -278,7 +279,16 @@ TmEcode ReceivePcapLoop(ThreadVars *tv, void *data, void *slot)
             returnInt(TM_ECODE_OK);
         } while (r < 0);
     }
```

```c
+    switch(r) {
+        case PCAP_ERROR_ACTIVATED:
+            /* "the operation can't be performed on already activated captures" - permanent error, exit
+             */
+            dbreak = 1;
+            retval = TM_ECODE_FAILED;
+            break;
+        }
+    } while (r < 0 && dbreak == 0);
+    if (dbreak) {
+        break;
+    }
```

```c
@@ -292,7 +302,7 @@ TmEcode ReceivePcapLoop(ThreadVars *tv, void *data, void *slot)
     StatsSyncCountersIfSignalled(tv);
+    SCReturnInt(retval);
 }
**History**

**#1 - 07/28/2020 06:21 PM - Roland Fischer**

The proposed patch is one way of fixing it but it'll exit Suricata.

The question is whether Suricata should try to recover in this use case, or if it should exit and leave it up to some external process control, e.g. systemd if you fancy that, to restart the whole thing. Each solution has its pros and cons.

From what I can tell, retry behaviour was added in [https://github.com/OISF/suricata/commit/fb36c0af126883f9117bd45ad162323a9efaf031](https://github.com/OISF/suricata/commit/fb36c0af126883f9117bd45ad162323a9efaf031) quite a bit ago with the goal of "Prior to this patch, a suricata listening to an interface was leaving when the interface goes down. This patch modifies the behaviour to automatically reconnect.".

This probably points more towards fixing up PcapTryReopen() to handle this use case as well, but the suricata devs would better know their preference.

**#2 - 07/28/2020 06:24 PM - Roland Fischer**

Fixing PcapTryReopen() would probably require to pcap_close() the pcap handle in this case and re-create it similar to what is done in ReceivePcapThreadInit().

---

09/07/2020