Suricata - Bug #5436

Infinite loop if the sniffing interface temporarily goes down (6.0.x backports)

07/04/2022 02:12 PM - Juliana Fajardini Reichow

<table>
<thead>
<tr>
<th>Status:</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Juliana Fajardini Reichow</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>6.0.7</td>
</tr>
<tr>
<td>Affected Versions:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Effort:</td>
<td></td>
</tr>
<tr>
<td>Label:</td>
<td></td>
</tr>
</tbody>
</table>

**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;
 +    retval = TM_ECODE_OK;
     while (1) {
@@ -278,7 +279,16 @@ TmEcode ReceivePcapLoop(ThreadVars *tv, void *data, void *slot)
   } while (r < 0 && dbreak == 0);
 if (dbreak) {
   break;
@@ -292,7 +302,7 @@ TmEcode ReceivePcapLoop(ThreadVars *tv, void *data, void *slot)
     StatsSyncCountersIfSignalled(tv);
 +    SCReturnInt(retval);
 }
```

07/16/2022 1/2
/**
Related issues:
Copied from Bug #3846: Infinite loop if the sniffing interface temporarily go...  Closed

History
#1 - 07/04/2022 02:12 PM - Juliana Fajardini Reichow
- Copied from Bug #3846: Infinite loop if the sniffing interface temporarily goes down added