Suricata - Bug #3888
6.0.0-dev - heap-buffer-overflow /opt/suricata/src/flow-manager.c:472:34 in FlowTimeoutHash with AFPv3
8/23/2020 09:39 AM - Peter Manev

Status: Closed
Priority: Normal
Assignee: Victor Julien
Category: 
Target version: 6.0.0rc1
Affected Versions: 
Difficulty: 
Label: 

Description
Stable is not affected.

This does not affect stable versions - 5.0.x
Only 6.0.0-dev/git master is affected.

After running for a while the following can be triggered/observed:

```
==16264==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x7f47cc5f0038 at pc 0x00000093f1d1 bp 0x7f47531ffdf0 sp 0x7f47531ffde8
READ of size 4 at 0x7f47cc5f0038 thread T71 (FM#07)
#0 0x93f1d0 in FlowTimeoutHash /opt/suricata/src/flow-manager.c:472:34
#1 0x93ffd8 in FlowTimeoutHashInChunks /opt/suricata/src/flow-manager.c:552:26
#2 0x93b84c in FlowManager /opt/suricata/src/flow-manager.c:897:21
#3 0xb7487b in TmThreadsManagement /opt/suricata/src/tm-threads.c:541:9
#4 0x7f47e1228fa2 in start_thread (/lib/x86_64-linux-gnu/libpthread.so.0+0x7fa2)
#5 0x7f47e017c4ce in clone (/lib/x86_64-linux-gnu/libc.so.6+0x9f4ce)
```


allocated by thread T0 (Suricata-Main) here:
```
#0 0x556149 in posix_memalign (/usr/local/bin/suricata+0x556149)
#1 0x82add9 in SCMallocAlignedFunc /opt/suricata/src/util-mem.c:116:13
#2 0x921cae in FlowInitConfig /opt/suricata/src/flow.c:606:17
#3 0xb4aa32 in PreRunInit /opt/suricata/src/suricata.c:2026:5
#4 0x84c409 in PostConfLoadedSetup /opt/suricata/src/suricata.c:2625:5
#5 0xb4ec45 in SuricataMain /opt/suricata/src/suricata.c:2782:9
#6 0x58464e in main /opt/suricata/src/main.c:22:12
#7 0x7f47e00a709a in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2409a)
```

Thread T71 (FM#07) created by T0 (Suricata-Main) here:
```
#0 0x556149 in posix_memalign (/usr/local/bin/suricata+0x556149)
#1 0x82add9 in SCMallocAlignedFunc /opt/suricata/src/util-mem.c:116:13
#2 0x921cae in FlowInitConfig /opt/suricata/src/flow.c:606:17
#3 0xb4aa32 in PreRunInit /opt/suricata/src/suricata.c:2026:5
#4 0x84c409 in PostConfLoadedSetup /opt/suricata/src/suricata.c:2625:5
#5 0xb4ec45 in SuricataMain /opt/suricata/src/suricata.c:2782:9
#6 0x58464e in main /opt/suricata/src/main.c:22:12
```


Shadow bytes around the buggy address:
```
0x0f9798b5f2b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0f9798b5fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0f9798b5fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```
Compile build-info and other extra information can be found in the attached.

### History

**#1 - 08/23/2020 09:41 AM - Peter Manev**
- File overflow-extrainfo added

Extra info attached.
Seems related to - [https://redmine.openinfosecfoundation.org/issues/3885](https://redmine.openinfosecfoundation.org/issues/3885)

**#2 - 08/24/2020 03:08 PM - Victor Julien**
- Status changed from New to Assigned
- Assignee set to Victor Julien
- Target version set to 6.0.0rc1

**#3 - 08/31/2020 03:01 PM - Victor Julien**
- Priority changed from Normal to High

**#4 - 09/04/2020 05:08 AM - Victor Julien**
- Status changed from Assigned to Closed
- Priority changed from High to Normal

[https://github.com/OISF/suricata/pull/5356/commits/703de670963c33e63357ac04934c02648e9ea086](https://github.com/OISF/suricata/pull/5356/commits/703de670963c33e63357ac04934c02648e9ea086)

### Files

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>overflow-extrainfo</td>
<td>19.4 KB</td>
<td>08/23/2020</td>
<td>Peter Manev</td>
</tr>
</tbody>
</table>