## Suricata - Bug #3745
### rules: memory leak on bad rule
06/03/2020 11:42 AM - Jeff Lucovsky

<table>
<thead>
<tr>
<th>Status:</th>
<th>Assigned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Jeff Lucovsky</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>5.0.4</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

```
==1==ERROR: LeakSanitizer: detected memory leaks
Direct leak of 16 byte(s) in 1 object(s) allocated from:
 #0 0x536742 in calloc /src/llvm-project/compiler-rt/lib/asan/asan_malloc_linux.cpp:154:3
 #1 0x8bc643 in SCCallocFunc suricata/src/util-mem.c:57:20
 #2 0x721a3b in SigMatchList2DataArray suricata/src/detect-parse.c:1602:41
 #3 0x67bfcc in DetectEngineAppInspectionEngine2Signature suricata/src/detect-engine.c:484:19
 #4 0x6a7986 in SigMatchPrepare suricata/src/detect-engine-build.c:1830:9
 #5 0x6a77e3 in SigGroupBuild suricata/src/detect-engine-build.c:1924:9
 #6 0x6b6721 in SigLoadSignatures suricata/src/detect-engine-loader.c:370:9
 #7 0x687d3d in DetectEngineReload suricata/src/detect-engine.c:4052:9
 #8 0x5691c9 in LLVMFuzzerTestOneInput suricata/src/tests/fuzz/fuzz_sigpcap.c:178:9
 #9 0x46ea31 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerLoop.cpp:556:15
 #10 0x459551 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) /src/llvm-project/compiler-rt/lib/fuzzer/FuzzerDriver.cpp:292:6
```

Testcase for the fuzz_sigpcap target attached.


Rule is:
```
alert tcp any any -> any 6 file_data;content:" ";dns.query;content:" ";
```

### Related issues:
- Copied from Bug #3683: rules: memory leak on bad rule [Closed]

### History

**#1 - 06/03/2020 11:42 AM - Jeff Lucovsky**

- Copied from Bug #3683: rules: memory leak on bad rule added

### Files

| clusterfuzz-testcase-minimized-fuzz_sigpcap-5069729246216192 | 71 Bytes | 04/29/2020 | Victor Julien |

06/13/2020