Suricata - Bug #3683
rules: memory leak on bad rule
04/29/2020 06:38 PM - Victor Julien

Status: Closed
Priority: Normal
Assignee: Philippe Antoine
Category:
Target version: 6.0.0rc1
Affected Versions:
Effort:
Difficulty:
Label: Needs backport

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.
https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=21911

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

Related issues:
Copied to Bug #3744: rules: memory leak on bad rule
Copied to Bug #3745: rules: memory leak on bad rule

History
#1 - 05/01/2020 08:26 AM - Victor Julien
https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=21911

#2 - 05/01/2020 12:14 PM - Philippe Antoine
- Status changed from New to In Review
- Assignee set to Philippe Antoine

https://github.com/OISF/suricata/pull/4905

#3 - 06/03/2020 11:42 AM - Jeff Lucovsky
- Copied to Bug #3744: rules: memory leak on bad rule added

#4 - 06/03/2020 11:42 AM - Jeff Lucovsky
- Copied to Bug #3745: rules: memory leak on bad rule added

#5 - 06/10/2020 08:37 PM - Philippe Antoine
- Status changed from In Review to Closed
<table>
<thead>
<tr>
<th>Files</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>clusterfuzz-testcase-minimized-fuzzSigcap-5069729246216192</td>
<td>71 B</td>
<td>04/29/2020</td>
<td>Victor Julien</td>
</tr>
</tbody>
</table>

[https://github.com/OISF/suricata/pull/5043](https://github.com/OISF/suricata/pull/5043)