Suricata - Bug #3682
bsize needs to err upon non possible matching conditions
04/27/2020 09:01 PM - Peter Manev

<table>
<thead>
<tr>
<th>Status:</th>
<th>In Review</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>7.0rc1</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>Needs backport to 6.0</td>
</tr>
</tbody>
</table>

Description
The following does not err (but it should)

cat bsize.rules

alert http any -> any (msg:"bsize test TEST"; http.uri; content:"abcdefgh123456"; bsize:2; sid:111; rev:1;)

/opt/suritest/bin/suricata -l log/ -S bsize.rules --engine-analysis ; cat log/rules_analysis.txt
[693058] 27/4/2020 -- 22:19:00 - (suricata.c:1056) <Notice> (LogVersion) -- This is Suricata version 6.0.0-dev (eef776087 2020-04-27) running in USER mode
-------------------------------------------------------------------
Date: 27/4/2020 -- 22:19:00
-------------------------------------------------------------------
== Sid: 111 ==
alert http any -> any (msg:"bsize test TEST"; http.uri; content:"abcdefgh123456"; bsize:2; sid:111; rev:1;)
  Rule matches on http uri buffer.
  App layer protocol is http.
  Rule contains 0 content options, 1 http content options, 0 pcre options, and 0 pcre options with http modifiers.
  Fast Pattern "abcdefgh123456" on "http request uri (http_uri)" buffer.
  Warning: TCP rule without a flow or flags option.
  -Consider adding flow or flags to improve performance of this rule.

/opt/suritest/bin/suricata -l log/ -S bsize.rules -T

If urilen:2 is added it errors properly

[693684] 27/4/2020 -- 22:38:21 - (detect-engine-loader.c:347) <Warning> (SigLoadSignatures) -- [ERRCODE: SC_ERR_NO_RULES_LOADED(43)] - 1 rule files specified, but no rules were loaded!
[693684] 27/4/2020 -- 22:38:21 - (suricata.c:2154) <Error> (LoadSignatures) -- [ERRCODE: SC_ERR_NO_RULES_LOADED(43)] - 1 rule files specified, but no rules were loaded!
_RULES.Loaded(43) – Loading signatures failed.

Related issues:
Copied to Bug #3746: bsize needs to err upon non possible matching conditions...   Rejected
Copied to Bug #3747: bsize needs to err upon non possible matching conditions...   Rejected

History
#1 - 04/27/2020 09:01 PM - Peter Manev
Originally reported by Jae Williams.

#2 - 05/12/2020 09:05 AM - Victor Julien
- Status changed from New to Assigned
- Assignee set to Jeff Lucovsky
- Target version set to 6.0.0beta1
- Label Needs backport added

#3 - 05/18/2020 02:41 PM - Jeff Lucovsky
- Status changed from Assigned to In Review

https://github.com/OISF/suricata/pull/4949

#4 - 06/03/2020 11:43 AM - Jeff Lucovsky
- Copied to Bug #3746: bsize needs to err upon non possible matching conditions (4.1.x) added

#5 - 06/03/2020 11:43 AM - Jeff Lucovsky
- Copied to Bug #3747: bsize needs to err upon non possible matching conditions (5.0.x) added

#6 - 08/05/2020 12:03 PM - Victor Julien
- Target version changed from 6.0.0beta1 to 6.0.0rc1

#7 - 09/04/2020 02:13 PM - Victor Julien
- Target version changed from 6.0.0rc1 to 7.0rc1

#8 - 06/02/2022 08:30 PM - Victor Julien
- Label Needs backport to 6.0 added
- Label deleted (Needs backport)

Is https://github.com/OISF/suricata/pull/5980 the latest PR on this?