Suricata - Bug #3747

bsize needs to err upon non possible matching conditions (5.0.x)

06/03/2020 11:43 AM - Jeff Lucovsky

Status: Assigned
Priority: Normal
Assignee: Jeff Lucovsky
Category: TBD
Affected Versions: TBD

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.

If urilen:2 is added it errors properly


If urilen:2 is added it errors properly

  from file bsize.rules at line 3
[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!
RULES_LOADED(43) - Loading signatures failed.

Related issues:
Copied from Bug #3682: bsize needs to err upon non possible matching conditions

In Review

History

#1 - 06/03/2020 11:43 AM - Jeff Lucovsky
- Copied from Bug #3682: bsize needs to err upon non possible matching conditions added

#2 - 06/21/2020 06:09 PM - Nick Price
Pretty new to this part of the codebase but I have a quick fix in place at
https://github.com/DominoTree/suricata/commit/80eae4b98c61bde0f20b052b1ab07738235859

I'm sure I've done several things the wrong way here and I wasn't sure if we need to change things here to use callbacks or not. Let me know of any changes I should make or different approaches I should use and I'll get them sorted ASAP.

#3 - 10/07/2020 06:00 AM - Victor Julien
- Subject changed from bsize needs to err upon non possible matching conditions to bsize needs to err upon non possible matching conditions (5.0.x)
- Target version changed from 5.0.4 to TBD

Not yet fixed in master, so backport will wait for that.