Suricata - Bug #317
Invalid Rules
08/19/2011 06:26 AM - Peter Manev

Status: Assigned
Priority: Normal
Assignee: Jason Taylor
Category: 
Target version: TBD
Affected Versions: medium
Difficulty: low
Effort: medium
Label: 

Please find attached some tests with invalid rule keywords combinations (bad "grammar") that should not be loaded by the engine, nevertheless they are getting loaded.

modifiers and rule keywords - distance,within, depth, offset...

Snort corrected some of the issues they had - "Improved error checking for invalid combinations of "depth", "offset", "distance", and "within" modifiers in rules. Rules that mix relative and non-relative options on the same content will now cause errors." - http://blog.snort.org/2010/12/snort-2903-is-coming-soon.html dated back in Dec 2010, some of them are still not addressed, I believe.

Please find a comparison of invalid rules and if they load or not. I have tested all the bad rules with Sur 1.0.4/1.0.5/git master, Snort 2.8.5.1/2.9.0.5/current beta, the results are in the spreadsheet attached.

Thanks

Related issues:
Related to Bug #2982: invalid dsize distance rule being loaded by suricata

History
#1 - 10/26/2011 09:28 AM - Victor Julien
- Assignee set to Eileen Donlon

Peter Pan, can you update this to include our 1.1beta3 release and the 2.9.1.2 Snort release?

#2 - 10/26/2011 09:35 AM - Peter Manev
Sure. Will update.

#3 - 10/31/2011 09:27 AM - Peter Manev
- File InvalidRulesUpdated.xls added

Updated file attached
Updates include current git master and Snort 2.9.1.2

#4 - 11/04/2011 11:53 AM - Eileen Donlon
- File InvalidRulesUpdatedwithCategories.xls added

I've added a sheet to Peter's workbook which lists categories of invalid or bad rules, and color-coded the rules in Peter's list to show the category. The point of listing the categories is that it makes it easier to develop a comprehensive set of rules for testing. Let me know if you have done this already! A lot of these checks have already been implemented but I don't know if they've all been tested.

The "bad" rule checks would be part of the rule analyzer.

#5 - 11/04/2011 01:11 PM - Peter Manev
I like the idea.
I think it would be good if we can number the categorizations as well i.e.
01 - Semantics Err
02 - Syntax Err
...
We could rewrite the "msg" in the alerts to reflect the categorization. Then it shouldn’t be difficult to write a script that would test all the rules and reflect the results in one go for every git update/release update. Other opinions?

#6 - 07/04/2012 03:46 AM - Victor Julien
- Target version set to TBD

#7 - 12/22/2015 03:45 PM - Andreas Herz
- Assignee changed from Eileen Donlon to Andreas Herz

#8 - 02/07/2016 03:46 PM - Andreas Herz
Quite old ; But tested the rules again against 3.0 and the only rules left are Content-Greater-Than-Dsize.rule and the other Dsiz-*.rule files.

#9 - 05/29/2016 05:06 PM - Andreas Herz
To resolve all the examples we would need to include several checks when parsing dsize rules since the checks depend on several other keywords. Do we want to add this or are we just fine with loading those rules since they shouldn't hurt but also not match?

#10 - 05/30/2016 01:34 AM - Peter Manev
Ideally - the checks should be there.

#11 - 05/31/2016 04:56 AM - Victor Julien
Agreed. If a rule can't match due to internal inconsistencies then we should reject it.

#12 - 06/03/2016 07:09 AM - Peter Manev
As an addition: this rule below -

```
alert tcp any any -> any any (msg: "la di da"; content: "0a:23:bf hu-ha");
```

loads with 3.1dev (rev d39e575) without err but it shouldn't load since it is missing a sid#.

#13 - 07/17/2018 08:18 AM - Victor Julien
- Assignee changed from Andreas Herz to Anonymous
- Effort set to medium
- Difficulty set to low

Think it would be nice to refresh this and open tickets for individual issues.

#14 - 02/23/2019 10:07 PM - Andreas Herz
- Assignee set to Community Ticket

#15 - 04/15/2019 11:51 PM - Jason Taylor
- Status changed from New to Assigned
- Assignee changed from Community Ticket to Jason Taylor

#16 - 05/15/2019 05:22 PM - Jason Taylor
suricata-verify tests have been submitted for the invalid rules.
https://github.com/OISF/suricata-verify/pull/57

there is still one rule that is successfully loading in current suricata master branch:
```
alert udp any any -> any any (msg:"TEST SUCCESFULL - dsize/distance INVALID combination "; dsize:10; content:"boom"; content:"foom"; distance:10; sid:66666663; rev:1;)
```

#2982 has been created to track the invalid rule loading

#17 - 05/15/2019 05:23 PM - Jason Taylor
- Related to Bug #2982: invalid dsize distance rule being loaded by suricata added

#18 - 07/27/2019 09:58 PM - Andreas Herz
Jason Taylor are you also interested in working on the parsing?

#19 - 07/29/2019 01:54 PM - Jason Taylor
Sure, I can certainly take a look, which parsing items are you referring to?

As a side note I am working on https://redmine.openinfosecfoundation.org/issues/2982 which I think is the only outstanding issue related to this ticket?

#20 - 07/29/2019 08:05 PM - Andreas Herz
yep, when it's merged we can close it. Thanks!

#21 - 07/30/2019 12:07 AM - Jason Taylor
Ideally I will have some time to work on this in the near future, if it's something time sensitive then by all means someone else can take it. This is all educational so I am stumbling my way through learning :)

#22 - 08/08/2019 10:17 PM - Andreas Herz
That's an ongoing issue for quite some time, so we're happy for every contribution :)

Files
<table>
<thead>
<tr>
<th>File Name</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>InvalidRules.tar.bz2</td>
<td>14.9 KB</td>
<td>08/19/2011</td>
<td>Peter Manev</td>
</tr>
<tr>
<td>InvalidRules.xls</td>
<td>13 KB</td>
<td>08/19/2011</td>
<td>Peter Manev</td>
</tr>
<tr>
<td>InvalidRulesUpdated.xls</td>
<td>14 KB</td>
<td>10/31/2011</td>
<td>Peter Manev</td>
</tr>
<tr>
<td>InvalidRulesUpdatedwithCategories.xls</td>
<td>18.5 KB</td>
<td>11/04/2011</td>
<td>Eileen Donlon</td>
</tr>
</tbody>
</table>