Suricata - Bug #1488

stream_size <= and >= modifiers function as < and > (equality is not functional)

06/16/2015 11:19 AM - Charles Smutz

Status: Closed
Priority: Normal
Assignee: Alexandre Macabies
Category: 
Target version: 3.0RC1
Affected Versions: 
Effort: 
Difficulty: 
Label: 

Description

for the stream_size keyword, the <= and >= modifiers function the same as the < and > modifiers respectively. When the = modifier matches, the <= and >= modifiers do not match.

When the following rules are applied to the specified pcap:

```#rules intended to be applied to https://csmutz.com/smsec_files/alice_full.pcap

alert tcp any any -> any any (msg:="=137"; stream_size:client,=,137; content:"GET "; sid:517301; rev:1;)
aalert tcp any any -> any any (msg:="!=137"; stream_size:client,!=,137; content:"GET "; sid:517302; rev:1;)
aalert tcp any any -> any any (msg:=">137"; stream_size:client,>,137; content:"GET "; sid:517303; rev:1;)
aalert tcp any any -> any any (msg:="<137"; stream_size:client,<,137; content:"GET "; sid:517304; rev:1;)
aalert tcp any any -> any any (msg:=">=137"; stream_size:client,>=,137; content:"GET "; sid:517305; rev:1;)
aalert tcp any any -> any any (msg:="<=137"; stream_size:client,<=,137; content:"GET "; sid:517306; rev:1;)
aalert tcp any any -> any any (msg:="=138"; stream_size:client,=,138; content:"GET "; sid:517311; rev:1;)
aalert tcp any any -> any any (msg:="!=138"; stream_size:client,!=,138; content:"GET "; sid:517312; rev:1;)
aalert tcp any any -> any any (msg:=">138"; stream_size:client,>,138; content:"GET "; sid:517313; rev:1;)
aalert tcp any any -> any any (msg:="<138"; stream_size:client,<,138; content:"GET "; sid:517314; rev:1;)
aalert tcp any any -> any any (msg:=">=138"; stream_size:client,>=,138; content:"GET "; sid:517315; rev:1;)
aalert tcp any any -> any any (msg:="<=138"; stream_size:client,<=,138; content:"GET "; sid:517316; rev:1;)
aalert tcp any any -> any any (msg:="=139"; stream_size:client,=,139; content:"GET "; sid:517321; rev:1;)
aalert tcp any any -> any any (msg:="!=139"; stream_size:client,!=,139; content:"GET "; sid:517322; rev:1;)
aalert tcp any any -> any any (msg:=">139"; stream_size:client,>,139; content:"GET "; sid:517323; rev:1;)
aalert tcp any any -> any any (msg:="<139"; stream_size:client,<,139; content:"GET "; sid:517324; rev:1;)
aalert tcp any any -> any any (msg:=">=139"; stream_size:client,>=,139; content:"GET "; sid:517325; rev:1;)
aalert tcp any any -> any any (msg:="<=139"; stream_size:client,<=,139; content:"GET "; sid:517326; rev:1;)
```
Alerts for >=138 (517315) and <=138 (517316) should occur as =138(517311) does.

The following alerts were generated on 2.1beta4 but the same issue exists in previous issues.

History

#1 - 06/18/2015 10:28 AM - Alexandre Macabies
Should be fixed by PR #1560.

#2 - 07/23/2015 04:41 AM - Victor Julien
- Status changed from New to Closed
- Assignee set to Alexandre Macabies
- Priority changed from Low to Normal
- Target version set to 3.0RC1
- % Done changed from 0 to 100

https://github.com/inliniac/suricata/pull/1560