Suricata - Feature #3887

yaml: Increase maximum size for address vars

08/21/2020 03:40 PM - Duane Howard

Status: Closed
Priority: Normal
Assignee: Jeff Lucovsky
Category: 
Target version: 7.0rc1
Effort: 
Difficulty: 

Label: 

Description

It appears the maximum length for an address var is 8192 bytes when dynamically generating lists for vars in large networks, it is easy to exceed this limit (especially with IPv6 network ranges). Can this be increased?

The only current workaround I'm aware of is to try to dynamically split lists and generate multiple vars which is... a bit unruly

[0] https://github.com/OISF/suricata/blob/master/src/detect-engine-address.c#L746

Related issues:

- Related to Bug #2190: apparent 1000 character limit in threshold.conf IP lists
- Related to Task #4097: Suricon 2020 brainstorm

History

#1 - 09/16/2020 07:16 AM - Victor Julien
- Status changed from New to Assigned
- Assignee set to Jeff Lucovsky
- Target version set to 7.0rc1

It would be nice if it can be made dynamic so there is no hardcoded limit.

Target is 7 for now. We can consider backporting if its not intrusive.

#2 - 10/17/2020 02:58 PM - Jeff Lucovsky
I suggest we cap the size allowed when permitting larger sizes.

The current (hard coded) limit is around 8k.

Suggestions for a reasonable upper bound?

#3 - 10/19/2020 11:46 AM - Jeff Lucovsky
- Status changed from Assigned to In Review

https://github.com/OISF/suricata/pull/5498 (draft)
https://github.com/OISF/suricata/pull/5598

#4 - 11/19/2020 05:01 PM - Jason Ish
- Related to Bug #2190: apparent 1000 character limit in threshold.conf IP lists added

#5 - 11/19/2020 05:02 PM - Jason Ish
- Related to Task #4097: Suricon 2020 brainstorm added

#6 - 11/24/2020 09:36 AM - Victor Julien
- Subject changed from Increase maximum size for address vars to yaml: Increase maximum size for address vars
- Status changed from In Review to Closed