Suricata - Bug #4414

threshold: slow startup on threshold.config with many addresses in suppression

04/06/2021 12:22 PM - Jeff Lucovsky

Status:	Closed		
Priority:	Normal		
Assignee:	Jeff Lucovsky		
Category:			
Target version:	5.0.7		
Affected Versions:		**Difficulty:**	
Effort:		**Label:**	

Description

A threshold config like

```
suppress gen_id 0, sig_id 0, track by_src, ip $SUPPRESS
suppress gen_id 1, sig_id 0, track by_src, ip $SUPPRESS
```

Combined with a large number of addresses in $SUPPRESS causes Suricata to load really slowly when using many rules.

```
  21,40%  Suricata-Main  suricata             [.] DetectAddressCmpIPv4
  20,53%  Suricata-Main  suricata             [.] DetectAddressCmp
  12,61%  Suricata-Main  suricata             [.] DetectAddressInsert
```

This appears to be caused by parsing the complex address string over and over again.

In per rule address parsing we cache. In threshold address parsing it appears this is not done, or is broken.

Steps to reproduce:

Create a config with many addresses:

```
#!/usr/bin/env python
# python cidr.py 192.168.1.1/24

import sys, struct, socket

(ip, cidr) = sys.argv[1].split('/')
cidr = int(cidr)
host_bits = 32 - cidr
i = struct.unpack('>I', socket.inet_aton(ip))[0] # note the endianness
start = (i >> host_bits) << host_bits # clear the host bits
end = start | ((1 << host_bits) - 1)

header = "%YAML 1.1\n---\n"
print(header)

final = ""
cnt = 0
i = 0
s = ""
# excludes the first and last address in the subnet
for r in range(start, end):
    x = socket.inet_ntoa(struct.pack('>I',r))
    if i == 0 or i % 100 == 0:
        if i != 0:
            s = s + "]\""
            final = final + "," + "$MYVAR" + str(cnt)
        else:
            final = "SUPPRESS: \"[$MYVAR" + str(cnt)
```

```
        print(s)
        s = "MYVAR" + str(cnt) + ": \"[" + x
        cnt += 1
    else:
        s = s + "," + x
    i += 1
s = s + "]\""
final = final + "]\""
print(s)
print(final)
```

(taken from https://stackoverflow.com/a/44043448)

Run: python ipaddresses.py 1.0.0.0/22 > suppress.yaml

In your suricata.yaml add:

```
vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"

    EXTERNAL_NET: "!$HOME_NET"
    #EXTERNAL_NET: "any"

    HTTP_SERVERS: "$HOME_NET"
    SMTP_SERVERS: "$HOME_NET"
    SQL_SERVERS: "$HOME_NET"
    DNS_SERVERS: "$HOME_NET"
    TELNET_SERVERS: "$HOME_NET"
    AIM_SERVERS: "$EXTERNAL_NET"
    DC_SERVERS: "$HOME_NET"
    DNP3_SERVER: "$HOME_NET"
    DNP3_CLIENT: "$HOME_NET"
    MODBUS_CLIENT: "$HOME_NET"
    MODBUS_SERVER: "$HOME_NET"
    ENIP_CLIENT: "$HOME_NET"
    ENIP_SERVER: "$HOME_NET"
    include: suppress.yaml
```

Finally load a larger ruleset, like ET/open.

Related issues:

Copied from Bug #4407: threshold: slow startup on threshold.config with many ...	**Closed**

History

#1 - 04/06/2021 12:22 PM - Jeff Lucovsky

- Copied from Bug #4407: threshold: slow startup on threshold.config with many addresses in suppression added

#2 - 04/26/2021 02:31 PM - Victor Julien

- Target version changed from 6.0.3 to 5.0.7

#3 - 04/29/2021 01:58 PM - Jeff Lucovsky

- Status changed from Assigned to In Progress

Cherry-pick: 11f9cc6, e873632, 02ceac8, 2893b04

#4 - 05/01/2021 01:38 PM - Jeff Lucovsky

- Status changed from In Progress to In Review

https://github.com/OISF/suricata/pull/6100

#5 - 05/03/2021 12:07 PM - Jeff Lucovsky

- Status changed from In Review to Closed