Description
Suppress rules like the following:
suppress gen_id 1, sig_id <id>, track by_dst, ip fe80::/16

fail with the following:
6/1/2013 -- 10:02:28 - <Error> - [ERRCODE: SC_ERR_PCRE_MATCH(2)] - pcre_exec parse error, ret -1, string , track by_dst, ip fe80::/16

This is because DETECT_SUPPRESS_REGEX is only valid for IPv4 addresses:
#define DETECT_SUPPRESS_REGEX "^,\s*track\s*(by_dst|by_src)\s*,\s*ip\s*(\[[\d.:/]+)*\s*$"

Adjusting this to the following seems to fix the issue:
#define DETECT_SUPPRESS_REGEX "^,\s*track\s*(by_dst|by_src)\s*,\s*ip\s*(\[[\da-f.:/]+)*\s*$"

I used '\[[\da-f.:/]+'. Could also probably use '[[xdigit:]./]+' but OTOH I wasn't sure if that would allow A-F and how suricata would handle addresses with upper case if it did.

History
#1 - 01/06/2013 11:18 AM - Jamie Strandboge
- File fix-ipv6-suppress.patch added

Here is a patch against 1.4 for the above.

#2 - 01/09/2013 10:26 AM - Victor Julien
The regex needs to handle the "case", so I think it should be A-Fa-f.

I prefer patches through github, care to do one?

#3 - 01/11/2013 07:26 AM - Jamie Strandboge
I submitted an updated patch using https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Contributing_to_Suricata. Not sure if it was required for a patch of this size, but I also signed the contributor agreement.

#4 - 01/11/2013 07:27 AM - Jamie Strandboge
I should've mentioned, I used `git send-email --to oisf-devel@openinfosecfoundation.org ...` before I subscribed to oisf-devel@, so it may need to be moderated.

#5 - 01/14/2013 07:17 AM - Victor Julien
- Status changed from New to Closed
- Assignee set to Jamie Strandboge
- Target version set to 1.4.1

Merged into master and master-1.3.x, thanks a lot Jamie.

I did some minimal testing with suppress rules to confirm it works, which it does.

Files