Suricata - Bug #90

http_method content modifier is broken

02/12/2010 08:37 AM - Will Metcalf

Status: Closed
Priority: Normal
Assignee: Victor Julien
Category:
Target version: 0.8.1
Affected Versions:
Effort:
Difficulty:
Label:

Description
processing the attached pcap the following signature should not fire at all, yet I get around 280 alerts although this number varies.

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"http_method is broken"; flow:to_server; content:"GET"; http_method; uricontent:"/some/content"; nocase; sid:2; rev:2;)

sudo src/suricata c suricata.yaml -r ../fpsid15481.pcap -l ./ -s blah.rules

[11866] 12/2/2010 -- 08:59:36 - (log-httplog.c:225) <Info> (LogFileLogExitPrintStats) -- (Outputs) HTTP requests 1

History

#1 - 02/12/2010 01:05 PM - Brian Rectanus
- Assignee changed from OISF Dev to Brian Rectanus

I'll look into it.

#2 - 02/17/2010 01:55 AM - Brian Rectanus
Looks like the same issue affects http_cookie.

#3 - 02/18/2010 11:41 AM - Victor Julien
- Assignee changed from Brian Rectanus to Victor Julien

I think it's related to the SigMatchReplace code somehow. I'll work on this today.

#4 - 02/18/2010 01:07 PM - Victor Julien
- Status changed from New to Closed

Will be fixed in new master.

Files
fpsid15481.pcap 473 KB 02/12/2010