Suricata - Bug #4286

FN occurs when using negated isdataat with http_cookie keyword

02/01/2021 06:32 PM - Jason Taylor

Status: New
Priority: Normal
Assignee:
Category:
Target version:
Affected Versions: 4.1.10
Effort:
Difficulty:
Label:

Description
Given a sample of traffic such as:

GET /somestuff HTTP/1.1
Accept: */*
Cookie: id=234524dst35e
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0000; Windows NT 5.1; SV1)
Host: google.com

We would expect the following to work:

alert http $HOME_NET any -> $EXTERNAL_NET any (flow:established.to_server; content:"id="; depth:3; isdataat:!13,relative; http_cookie;)

However, the rule does not fire as expected in any of the 4.0.x, 4.1.x, 5.x versions I tested on.

If we switch the rule to use http.cookie, the rule works as expected.

Related issues:
Is duplicate of Bug #2479: http_cookie negation fails if no cookie in traffic

New 04/05/2018

History
#1 - 03/11/2021 08:55 PM - Philippe Antoine
- Is duplicate of Bug #2479: http_cookie negation fails if no cookie in traffic added