**Suricata - Bug #1424**

**DNS EVE-log produces answers with incorrect direction**

03/19/2015 12:14 PM - Antti Tönkyrä

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Victor Julien</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td></td>
</tr>
<tr>
<td>Affected Versions:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Effort:</td>
<td></td>
</tr>
<tr>
<td>Label:</td>
<td></td>
</tr>
</tbody>
</table>

**Description**

EVE-Log sometimes produces DNS answers with incorrect direction (the server appears to be the dest when it should actually be the source).

Reproduced using

```bash
while [ 1 ]; do host pingtimeout.net ns1.pingtimeout.net; sleep 0.1; done
```

I have also attached pcap that replicates the issue on my local git head suricata. Below is an example of the wrong output.

```json
{
    "alerts": [],
    "data": {
        "dest_ip": "81.90.68.112",
        "dest_port": 53,
        "dns": {
            "id": 31443,
            "rdata": "81.90.68.114",
            "rrname": "pingtimeout.net",
            "rrtype": "A",
            "ttl": 3600,
            "type": "answer"
        },
        "event_type": "dns",
        "flow_id": 37465680,
        "pcap_cnt": 49,
        "proto": "UDP",
        "src_ip": "10.100.0.20",
        "src_port": 47589,
        "timestamp": "2015-03-19T17:05:17.163591"
    },
    "source": "suricata",
    "tags": []
}
```

```json
{
    "alerts": [],
    "data": {
        "dest_ip": "81.90.68.112",
        "dest_port": 53,
        "dns": {
            "id": 52955,
            "rdata": "81.90.68.114",
            "rrname": "pingtimeout.net",
            "rrtype": "A",
            "ttl": 3600,
            "type": "answer"
        },
        "event_type": "dns",
        "flow_id": 37467504,
```
"pcap_cnt": 61,
"proto": "UDP",
"src_ip": "10.100.0.20",
"src_port": 53278,
"timestamp": "2015-03-19T17:05:17.454712"
},
"source": "suricata",
"tags": []
}

History
#1 - 03/19/2015 12:15 PM - Antti Tönkyrä
Note that normal suricata eve-log input is encapsulated in data key in my example out.

#2 - 03/19/2015 12:18 PM - Antti Tönkyrä
And version info:
2.1dev (rev e250040)

#3 - 03/19/2015 12:26 PM - Antti Tönkyrä
Also happens with 60a4965

#4 - 05/21/2015 04:47 AM - Victor Julien
- Status changed from New to Assigned
- Assignee set to David Cannings
- Target version set to 3.0RC1

#5 - 05/21/2015 05:59 AM - David Cannings
Confirmed in both live and pcap mode. Packet captures were taken from the same physical interface but not at the same time.

From the same pcap, here's two example sessions (one with vlan tags, one without):

{ "timestamp": "2015-05-21T11:30:00.962978+0100", "flow_id": 22189344, "pcap_cnt": 6031, "event_type": "dns", "src_ip": "10.X.X.X", "src_port": 65077, "dest_ip": "10.Y.Y.Y", "dest_port": 53, "proto": "UDP", "dns": { "type": "answer", "id": 7442, "rcode": "NXDOMAIN", "rrname": "u.03.s.sophosxl.net", "rrtype": "SOA", "ttl": 9 } }
{ "timestamp": "2015-05-21T11:30:01.467133+0100", "flow_id": 22312464, "pcap_cnt": 6078, "event_type": "dns", "vlan": 1, "src_ip": "10.X.X.X", "src_port": 50545, "dest_ip": "10.Y.Y.Y", "dest_port": 53, "proto": "UDP", "dns": { "type": "answer", "id": 53770, "rcode": "NOERROR", "rrname": "iplayerhelp.external.bbc.co.uk", "rrtype": "CNAME", "ttl": 1797, "rdata": "bbcplayer.metafaq.com" } }

From live capture:

{ "timestamp": "2015-05-21T10:17:27.866919", "flow_id": 140034661246416, "in_iface": "eth2", "event_type": "dns", "vlan": 1, "src_ip": "10.X.X.X", "src_port": 41341, "dest_ip": "10.Y.Y.Y", "dest_port": 53, "proto": "UDP", "dns": { "type": "answer", "id": 20985 } }
{ "timestamp": "2015-05-21T10:17:27.867699", "flow_id": 140034661247088, "in_iface": "eth2", "event_type": "dns", "src_ip": "10.X.X.X", "src_port": 39122, "dest_ip": "10.Z.Z.Z", "dest_port": 53, "proto": "UDP", "dns": { "type": "answer", "id": 20985 } }

Note that there are also correct log entries, for example:


The incorrect log entries greatly outnumber the correct ones in pcap mode. My sample is small and not statistically significant. The below is from a 1.2MB pcap:

-> % jq -c 'select(.dns.type=="answer") | select(.src_port==53)' eve.json | wc -l
3 # correct

-> % jq -c 'select(.dns.type=="answer") | select(.dest_port==53)' eve.json | wc -l
9897 # incorrect

And from the live capture:

-> % jq -c 'select(.dns.type=="answer") | select(.src_port==53)' dns.log | wc -l
4149 # correct
Live capture used 2.1beta2, pcap used 2.1dev (rev 0e2a4c0).

#6 - 11/24/2015 08:45 AM - Victor Julien
- Target version changed from 3.0RC1 to 70

#7 - 11/22/2016 01:05 PM - Jason Ish
I propose we close this. I confirmed that I could replicate it with rev 0e2a4c0, but I am not able to replicate with 3.2RC1.
Appears it was fixed by this commit 133485937952d8ed106eae840f517edf53024e19 (though I'm not sure why...)

#8 - 11/23/2016 08:16 AM - Victor Julien
That commit shouldn't affect it, how did you determine that?

#9 - 11/23/2016 08:34 AM - Jason Ish
You're right. I limited my back testing to commits on the dns files, it could have been in another commit leading up to that one. I'll re-check.

#10 - 11/23/2016 08:36 AM - Victor Julien
Maybe a git bisect could be useful. It can be automated if you have a test case that returns good/bad.

#11 - 11/23/2016 10:21 AM - Jason Ish
This is the commit: https://redmine.openinfosecfoundation.org/projects/suricata/repository?utf8=%E2%9C%93&branch=master&tag=&rev=2f0e0f17dbb4f289f045ab38cf13dc2ef209a148

#12 - 11/24/2016 07:47 AM - Victor Julien
- Status changed from Assigned to Closed
- Assignee changed from David Cannings to Victor Julien
- Target version deleted (70)

Guess I fixed it then ;)

Files

| suritest.pcap | 9.15 KB | 03/19/2015 | Antti Tönkylä |