### Suricata - Bug #2437

#### rust/dns: Core Dump with malformed traffic

02/12/2018 07:52 AM - Nick Price

<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>Jason Ish</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td>4.1beta1</td>
</tr>
<tr>
<td>Affected Versions:</td>
<td></td>
</tr>
</tbody>
</table>

**Description**

Experiencing a panic with malformed DNS traffic. Here's the relevant trace data. Looking at dns.rs, nothing really jumps out at me that seems like it'd cause a panic here.

I'll keep digging and see if I can come up with anything further.

---

```plaintext
#10 0x00000000000070d637 in core::panicking::panic () at /checkout/src/libcore/panicking.rs:51
No locals.
#11 0x000000000006028ff in suricata::dns::dns::{impl}::set_event (self=0x7fb97edc9ec0, event=MalformedData) at src/dns/dns.rs:358
    tx = 0x7fb979c9ada98
    len = 2
    self = 0x7fb97edc9ec0
    event = MalformedData
#12 0x0000000000060383b in suricata::dns::dns::{impl}::parse_response (self=0x7fb97edc9ec0, input=...) at src/dns/dns.rs:421
    response = {header = {tx_id = 55792, flags = 31898, questions = 32697, answer_rr = 0, authority_rr = 56128, additional_rr = 31898}, queries = {buf = {ptr = {pointer = {__0 = 0x2}, _marker = {<No data fields>}}, cap = 140434636200768, a = {<No data fields>}}, len = 140434810584624}, answers = {buf = {ptr = {pointer = {__0 = 0x6010bd <core::slice::{{impl}}::iter_mut<suricata::dns::DNSTransaction>+269>}, _marker = {<No data fields>}}, cap = 140434810584736, a = {<No data fields>}}, len = 6630918}, authorities = {
    buf = {ptr = {pointer = {__0 = 0x2}, _marker = {<No data fields>}}, cap = 140434636200432, a = {<No data fields>}}, len = 140434636200432)
    self = 0x7fb97edc9ec0
    input = {data_ptr = 0x7fb9fc0217b6 "$230A\250\a", length = 512}
#13 0x0000000000060496c in suricata::dns::rs::rs_parse_response (_flow=0x7fb76d3ecfe0, state=0x7fb97edc9ec0, _pstate=0x7fb97da33990, input=0x7fb9fc0217b6 "$230A\250\a", input_len=512, _data=0x0) at src/dns/dns.rs:613
    buf = {data_ptr = 0x7fb9fc0217b6 "$230A\250\a", length = 512}
    _flow = 0x7fb76d3ecfe0
    state = 0x7fb97edc9ec0
    _data = 0x0
    _pstate = 0x7fb97da33990
    input = 0x7fb9fc0217b6 "$230A\250\a"
    input_len = 512
```

### History

**#1 - 02/12/2018 07:54 AM - Nick Price**

Forgot to add, this is 4.0.3

**#2 - 02/12/2018 07:57 AM - Jason Ish**

Do you have a pcap that demonstrates this?

Thanks.

**#3 - 02/12/2018 08:24 AM - Nick Price**

Haven't been able to get one thus far because I only have a four-hour window and this happened overnight, but I'm going to keep my eye on it and try
to pull pcaps if I see it fall over again.

#4 - 02/12/2018 01:02 PM - Jason Ish
Did you get a panic message? Something like:

```rust
thread '<unnamed>' panicked at 'attempt to add with overflow', src/dns/dns.rs:358:9
```

An overflow is the only case I can think of that would cause a panic at this line.

#5 - 02/12/2018 02:04 PM - Jason Ish
Nick, after some further thought, you must be seeing a lot of malformed DNS traffic as its hitting 65k per DNS state. If you are able to, even if privately, I'm wondering if you could share a sample of your DNS traffic for testing. Maybe its not corrupt and just been decoded as corrupt. Or it could actually be corrupt, or something thats not DNS, but looks close enough to trigger the parser.

#6 - 02/12/2018 04:02 PM - Jason Ish
- Status changed from New to Assigned
- Assignee set to Jason Ish

#7 - 02/13/2018 03:27 AM - Victor Julien
- Description updated
- Target version set to 4.1beta1

#8 - 02/13/2018 03:28 AM - Victor Julien
- Subject changed from Core Dump with malformed DNS traffic to rust/dns: Core Dump with malformed traffic

#9 - 02/14/2018 08:52 AM - Victor Julien
- Status changed from Assigned to Closed

https://github.com/OISF/suricata/pull/3239