Suricata - Security #2947

**rust/dhcp: panic in dhcp parser (master)**

04/30/2019 08:24 AM - Victor Julien

<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>5.0beta1</td>
</tr>
<tr>
<td>Affected Versions:</td>
<td>4.1.3</td>
</tr>
<tr>
<td>CVE:</td>
<td>2019-10052</td>
</tr>
</tbody>
</table>

### Description

From reporter:

```plaintext
==14370== ERROR: libFuzzer: deadly signal
...  
/home/sirko/Projects/CI/fuzzing/suricata-fuzzing.2/rust/src/dhcp/parser.rs:126:23
#17 0x56083d83ff5b in suricata::dhcp::parser::parse_option::hab72aeff1560bad1 /home/sirko/Projects/CI/fuzzing/suricata-fuzzing.2/rust/src/dhcp/parser.rs:126:23
#18 0x56083d80582b in suricata::dhcp::parser::dhcp_parse::h5f41b0fc5736d132 /home/sirko/Projects/CI/fuzzing/suricata-fuzzing.2/rust/src/dhcp/parser.rs:205:22
#19 0x56083d7e4e8f in suricata::dhcp::dhcp::DHCPState::parse::h7ace958910b14aac /home/sirko/Projects/CI/fuzzing/suricata-fuzzing.2/rust/src/dhcp/dhcp.rs:146:14
#20 0x56083d72dfbc in rust_fuzzer_test_input /home/sirko/Projects/CI/fuzzing/suricata-fuzzing.2/rust/fuzz/fuzz_targets/fuzz_dhcp.rs:7:4
#21 0x56083d9b2744 in libfuzzer_sys::test_input_wrap::_$u7b$$u7b$closure$u7d$$u7d$::h29c9181044b7489b
/home/sirko/.cargo/git/checkouts/libfuzzer-sys-e07fde05820d7bc6/4a41319/src/lib.rs:11:8
#22 0x56083d9f984d in std::panicking::try::do_call::hd66afc279650fe66
/rustc/0f88167f89ffe321590c5148f21b7d51d44388d/src/libstd/panicking.rs:293:39
#23 0x56083da0af88 in __rust_maybe_catch_panic /rustc/0f88167f89ffe321590c5148f21b7d51d44388d/src/libpanic_abort/lib.rs:29:4
NOTE: libFuzzer has rudimentary signal handlers.
Combine libFuzzer with AddressSanitizer or similar for better crash reports.
SUMMARY: libFuzzer: deadly signal
```

The error is from an attempt to parse len - 1 bytes without first checking that len is > 0.

### Related issues:

Copied from Security #2902: rust/dhcp: panic in dhcp parser

Closed

### History

**#1 - 04/30/2019 08:24 AM - Victor Julien**

* Copied from Security #2902: rust/dhcp: panic in dhcp parser added

**#2 - 04/30/2019 01:08 PM - Victor Julien**

* Status changed from Assigned to Closed
* Private changed from Yes to No

[https://github.com/OISF/suricata/releases/tag/suricata-5.0.0-beta1](https://github.com/OISF/suricata/releases/tag/suricata-5.0.0-beta1)

**#3 - 09/01/2020 09:49 AM - Victor Julien**
- Tracker changed from Bug to Security
- Effort deleted (low)
- Difficulty deleted (low)
- CVE set to 2019-10052
- Git IDs updated