Suricata - Security #2904

rust/ftp: panic in ftp parser

03/25/2019 03:25 PM - Jason Ish

<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>4.1.4</td>
</tr>
<tr>
<td>Affected Versions:</td>
<td>4.1.4</td>
</tr>
<tr>
<td>Git IDs:</td>
<td>ad551189274b50206344e0fde72e4300247bc</td>
</tr>
</tbody>
</table>

CVE: 2019-10055

Description

From reporter:

```
==14001== ERROR: libFuzzer: deadly signal
...
#16 0x561102d178e8 in suricata::ftp::ftp_pasv_response::h60c6b1ddc3e5372 /home/sirko/Projects/CI/fuzzing/suricata-fuzzing.2/rust/src/ftp/mod.rs:54:16
#17 0x561102ce4475 in rs_ftp_pasv_response /home/sirko/Projects/CI/fuzzing/suricata-fuzzing.2/rust/src/ftp/mod.rs:63:10
#18 0x561102c2bf4b in rust_fuzzer_test_input /home/sirko/Projects/CI/fuzzing/suricata-fuzzing.2/rust/fuzz/fuzz_targets/fuzz_ftp.rs:6:4
#19 0x561102e99dd4 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
#20 0x561102ee0ed in std::panicking::try::do_call::hd66afc279650fe66
/rustc/0f88167f89ffe321590c5148f21b7d51d44388d/src/libstd/panicking.rs:293:39
#21 0x561102ef30f8 in __rust_maybeCatch_panic /rustc/0f88167f89ffe321590c5148f21b7d51d44388d/src/libpanic_abort/lib.rs:29:4
```

The passive response decoder returns a u16, however the method of calculating the port value can create a value greater than a u16 can hold leading to a panic.

Related issues:

Copied to Security #2949: rust/ftp: panic in ftp parser (master)

History

#1 - 04/30/2019 08:25 AM - Victor Julien
- Copied to Security #2949: rust/ftp: panic in ftp parser (master) added

#2 - 04/30/2019 12:28 PM - Victor Julien
- Status changed from Assigned to Closed

https://github.com/OISF/suricata/releases/tag/suricata-4.1.4

#3 - 04/30/2019 12:54 PM - Victor Julien
- Private changed from Yes to No

#4 - 09/01/2020 09:16 AM - Victor Julien
- Tracker changed from Bug to Security
- CVE set to 2019-10055
- Git IDs updated

09/09/2020