Suricata - Security #2896

smb 1 create andx request does not parse the filename correctly (master)

03/22/2019 11:34 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>Victor Julien</td>
</tr>
<tr>
<td>Category:</td>
<td>Target version: 5.0beta1</td>
</tr>
<tr>
<td>Affected Versions: 4.1.3</td>
<td>Git IDs: cc50908f8d8beabaae3a60ee72412d704a024c2d7f7a41412d6fe0fbf2855c38ae9d6d02eb63adb21</td>
</tr>
<tr>
<td>CVE: 2019-10051</td>
<td></td>
</tr>
</tbody>
</table>

**Description**

I noticed that for the filenames of smb 1 create_andx_requests the first character of the filename was missing. I have isolated a flow from a pcap which it was pretty clear the first character was missing: Filename 'rowser' != 'browser' in packet 14.

```
```

In the function parse_smb_create_andx_request_record in smb1_records.rs the second _skip is skipping 1 byte too much.

"_skip2: take!(8)" should be "_skip2: take!(7)"

From after the parsing of the create_options we should skip:

- impersonation (4)
- security_flags (2)
- byte_count (1)
- file_name (file_len)

**Related issues:**

- Copied from Security #2894: smb 1 create andx request does not parse the file...
- Closed

**History**

#1 - 03/22/2019 11:34 AM - Victor Julien
- Copied from Security #2894: smb 1 create andx request does not parse the filename correctly. added

#2 - 03/22/2019 12:00 PM - Wesley van der Ree
Pull request: [https://github.com/OISF/suricata/pull/3734](https://github.com/OISF/suricata/pull/3734)

#3 - 03/25/2019 01:23 PM - Victor Julien
- Status changed from Assigned to Closed

[https://github.com/OISF/suricata/pull/3746](https://github.com/OISF/suricata/pull/3746)

#4 - 09/01/2020 09:56 AM - Victor Julien
- Tracker changed from Bug to Security
- Effort deleted (low)
- Difficulty deleted (low)
- CVE set to 2019-10051
- Git IDs updated

09/06/2020