**Suricata - Bug #4925**  
*Rule error in SMB dce_iface and dce_opnum keywords*

12/22/2021 01:30 AM - Shivani Bhardwaj

<table>
<thead>
<tr>
<th>Status</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>High</td>
</tr>
<tr>
<td>Assignee</td>
<td>Eloy Pérez</td>
</tr>
<tr>
<td>Category</td>
<td></td>
</tr>
<tr>
<td>Target version</td>
<td>6.0.5</td>
</tr>
<tr>
<td>Affected Versions</td>
<td>6.0.1</td>
</tr>
<tr>
<td>Effort</td>
<td></td>
</tr>
</tbody>
</table>

**Description**

The SMB dce_iface and dce_opnum keywords don't match.

Following rule and the associated pcap can be used to test this behavior:

```
alert smb any any -> any any (\ 
  msg: "SMB-DCE EnumPrinterDrivers";\ 
  dce_iface: 12345678-1234-abcd-ef00-0123456789ab;\ 
  dce_opnum: 10;\ 
  sid: 1;\ 
}
```

**Related issues:**

Copied from Bug #4767: Rule error in SMB dce_iface and dce_opnum keywords

**History**

#1 - 12/22/2021 01:30 AM - Shivani Bhardwaj
- Copied from Bug #4767: Rule error in SMB dce_iface and dce_opnum keywords added

#2 - 02/09/2022 10:17 AM - Eloy Pérez
- Assignee changed from Shivani Bhardwaj to Eloy Pérez

#3 - 03/02/2022 05:59 AM - Shivani Bhardwaj
- Status changed from Assigned to In Review

#4 - 03/07/2022 06:08 AM - Shivani Bhardwaj
- Status changed from In Review to Closed

Closed by [https://github.com/OISF/suricata/pull/7104](https://github.com/OISF/suricata/pull/7104)

**Files**

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Date</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>test-smb-dcerpc.pcapng</td>
<td>13.4 KB</td>
<td>10/20/2021</td>
<td>Eloy Pérez</td>
</tr>
</tbody>
</table>