Suricata - Bug #4927

dcerpc dce_iface just match a packet

12/22/2021 01:33 AM - Shivani Bhardwaj

| Status:    | Closed          |
| Priority:  | High            |
| Assignee:  | Eloy Pérez      |
| Category:  |                |
| Target version: | 6.0.5          |
| Affected Versions: | 6.0.4          |

Description
The dce_iface dcerpc keyword just match the packet following the bind.

```alert dcerpc any any -> any any (\  
  msg: "DCE Netlogon";  
  flow: to_server;  
  dce_iface: 12345678-1234-abcd-ef00-01234567cffe;  
  sid: 1;  
}
```

Related issues:
Copied from Bug #4769: dcerpc dce_iface just match a packet

History

#1 - 12/22/2021 01:33 AM - Shivani Bhardwaj
- Copied from Bug #4769: dcerpc dce_iface just match a packet added

#2 - 12/22/2021 01:33 AM - Shivani Bhardwaj
- Label deleted (Needs backport to 5.0, Needs backport to 6.0)

#3 - 02/09/2022 10:17 AM - Eloy Pérez
- Assignee changed from Shivani Bhardwaj to Eloy Pérez

#4 - 03/02/2022 05:59 AM - Shivani Bhardwaj
- Status changed from Assigned to In Review

#5 - 03/07/2022 06:09 AM - Shivani Bhardwaj
- Status changed from In Review to Closed

Closed by https://github.com/OISF/suricata/pull/7104

Files

| test-dce-iface.pcapng | 3.34 KB | 10/20/2021 | Eloy Pérez |

Powered by TCPDF (www.tcpdf.org)