Suricata - Bug #5135

DCERPC: dcerpc.iface keyword alert results differ from 5 vs 6/master

02/19/2022 02:54 PM - Peter Manev

Status: New
Priority: Normal
Assignee: OISF Dev
Category: 
Target version: TBD
Affected Versions: 6.0.4, git master

Description
If sid 666 and 888 match there is no reason why 777 would not match.
Please see attached for comparison.

The pcap used - https://redmine.openinfosecfoundation.org/attachments/2434
6.x and master have the problem of not generating alert on sid:777
5.x is good

Files
dcerpc-perf-accuracy.txt 7.6 KB 02/19/2022

Peter Manev