Suricata - Bug #5444

dns: allow dns messages with invalid opcodes

07/18/2022 07:44 PM - Jason Ish

Status: New
Priority: High
Assignee: Jason Ish
Category: Target version: 7.0rc1
Affected Versions: 6.0.6
Effort: Difficulty:
Label: Needs backport to 6.0

Description
Current a DNS message won't be detected as DNS if the opcode is considered invalid (greater than 7). We should probably accept any opcode, and then use rules to alert on invalid opcodes.

Research: Will this detect too much non DNS as DNS?

History
#1 - 07/19/2022 07:44 PM - Jason Taylor
- File opcode8.pcap added

just adding a sample udp dns query with opcode of 8 set. With the change discussed in this ticket, a signature such as 'alert dns any any -> any any (msg:"dns opcode 8"; dns.opcode:8; sid:123; rev:1;)' run against the attached pcap would alert.

#2 - 07/22/2022 06:35 PM - Philippe Antoine
To be noted : now that https://github.com/OISF/suricata/pull/7320 got merged, if a client sends junk to a DNS server, suricata will recognize the protocol as DNS (with app_proto_tc: failed)

#3 - 07/27/2022 01:27 PM - Victor Julien
- Priority changed from Normal to High
- Label Needs backport to 6.0 added

#4 - 07/27/2022 01:28 PM - Victor Julien
@Philippe Antoine are you saying that in master this issue is resolved (by the PR you mentioned)?

#5 - 07/27/2022 01:34 PM - Philippe Antoine
That depends on how you define the issue.

If a DNS server uses invalid opcodes, as in the attached pcap, this issue is not resolved.

Files
opcode8.pcap  522 Bytes  07/19/2022  Jason Taylor