Suricata - Bug #3328
bad ip option evasion
11/07/2019 08:25 PM - Nicolas Adba

Status: Closed
Priority: Normal
Assignee: Jason Ish
Category: 
Target version: 5.0.1
Affected Versions: 5.0.0
Effort:

Description
Suricata is vulnerable to bad ip option evasions. Here are the pcaps of issue number 3286 with a bad ipv4 option.

I don't think it's exploitable in the wild because routers should drop the injected packets (I didn't test it thought).

Related issues:
Copied to Bug #3414: bad ip option evasion (4.1.x) Closed

Files
with_evasion_windows.pcap 1.26 KB 11/07/2019 Nicolas Adba
with_evasion_linux.pcap 1.43 KB 11/07/2019 Nicolas Adba
without_evasion.pcap 1.01 KB 11/07/2019 Nicolas Adba
test.rule 147 Bytes 11/07/2019 Nicolas Adba