Suricata - Security #3173
ipv4: ts field decoding oob read
09/18/2019 11:49 AM - Victor Julien

Status: Closed
Priority: Normal
Assignee: Victor Julien
Category:
Target version: 4.1.5
Affected Versions: 4.1, 4.1.1, 4.1.2, 4.1.3, 4.1.4
Git IDs: 8c399c0a5768fba2df024e6926770719b8697cc6
CVE: 2019-16411

Description
Due to a mistake in the offset at which the flags field it read, a one byte OOB read happens:

READ of size 1 at 0x6070000006f6 thread T0
#0 0x59f002 in IPV4OptValidateTimestamp /home/sirko/Projects/CI/fuzzing/_CPP/suricata/suricata-fuzzing.4.1.4/src/decode-ipv4.c:162:12
#1 0x59b2a9 in DecodeIPV4Options /home/sirko/Projects/CI/fuzzing/_CPP/suricata/suricata-fuzzing.4.1.4/src/decode-ipv4.c:378:32
#2 0x596c2c in DecodeIPV4Packet /home/sirko/Projects/CI/fuzzing/_CPP/suricata/suricata-fuzzing.4.1.4/src/decode-ipv4.c:527:9
#3 0x593032 in DecodeIPV4 /home/sirko/Projects/CI/fuzzing/_CPP/suricata/suricata-fuzzing.4.1.4/src/decode-ipv4.c:540:9

Related issues:
Copied to Security #3176: ipv4: ts field decoding oob read (5.x)

History
#1 - 09/18/2019 06:31 PM - Victor Julien
- Copied to Security #3176: ipv4: ts field decoding oob read (5.x) added

#2 - 09/24/2019 02:56 PM - Victor Julien
- Status changed from Assigned to Closed
- Private changed from Yes to No

https://github.com/OISF/suricata/commit/8c399c0a5768fba2df024e6926770719b8697cc6

#3 - 09/01/2020 09:04 AM - Victor Julien
- Tracker changed from Bug to Security
- CVE set to 2019-16411
- Git IDs updated