Suricata - Bug #5309
CIDR prefix calculation fails on big endian archs
04/27/2022 08:15 PM - Sascha Steinbiss

While trying to build 6.0.5 on Debian's s390x port, we noticed that tests segfault in the new version (see https://ci.debian.net/data/autopkgtest/testing/s390x/s/suricata/21160408/log.gz). Tracking this down, it seems that CIDRFromMask() returns -1 when trying to determine a network prefix length for a given netmask (e.g. 24 for 255.255.255.0). This causes DetectAddressParseSingle() to return NULL and hence the test to try and dereference a null pointer, causing the segfault.

I compared values passed into CIDRFromMask() via gdb on amd64 and s390x and found that they are different:

```
amd64
... Test AddressTestCutIPv401 ...
Breakpoint 1, CIDRFromMask (netmask=16777215) at util-cidr.c:34 ...

s390x
... Test AddressTestCutIPv401 ...
Breakpoint 1, CIDRFromMask (netmask=4294967040) at util-cidr.c:34 ...
```

My patch at https://gist.github.com/satta/7406fe735d8b449a4c9af73822d2bc9a fixes the code for both architectures.

Subtasks:
- Bug # 5344: CIDR prefix calculation fails on big endian archs (6.0.x backport) - Closed
- Bug # 5345: CIDR prefix calculation fails on big endian archs (5.0.x backport) - Closed

History
#1 - 04/28/2022 05:40 AM - Victor Julien
- Status changed from New to In Review
- Assignee changed from OISF Dev to Sascha Steinbiss
- Target version changed from TBD to 7.0rc1

https://github.com/OISF/suricata/pull/7332
Possibly needs backport to 5.0 as well.

#2 - 05/07/2022 01:08 PM - Jeff Lucovsky
- Label Needs backport to 5.0 added
- Label deleted (Needs backport)

#3 - 05/07/2022 01:08 PM - Jeff Lucovsky
- Copied to Bug #5344: CIDR prefix calculation fails on big endian archs (6.0.x backport) added
#4 - 05/07/2022 01:09 PM - Jeff Lucovsky
- Copied to Bug #5345: CIDR prefix calculation fails on big endian archs (5.0.x backport) added

#5 - 05/24/2022 07:50 PM - Jeff Lucovsky
- Status changed from In Review to Resolved

#6 - 07/01/2022 09:25 AM - Victor Julien
- Status changed from Resolved to Closed

#7 - 07/01/2022 09:40 AM - Victor Julien
- Label deleted (Needs backport to 5.0, Needs backport to 6.0)