### Bugreport SSHParseBanner (app-layer-ssh.c)

There is an integer and as a result a heap buffer overflow at line 99.

#### Input

If *input of the function *SSHParseBanner(SshState *state, SshHeader *header, const uint8_t *input, uint32_t input_len)* only consists only one spezial character **'\n'**, the program runs into a heap buffer overflow.

#### Reason

At **line 76** in the function *SSHParseBanner*, the program search for a "\r". If not, then match the input with a "\n". After this point line_len is "0". And this is the problem. At line 97, we subtract "-4" from line_len and we get a negativ integer. Unfortunately, input_len is an unsigned integer and smaal negativ integers are now very big unsign ed integers. The result is, that the **input_len** is much higher then the given buffer. The function *BasicSearch* needs the length and will crash by of reading to much memory space because of the high input_len value. This results in a heap-buffer-overflow.

### Related issues:

Copied to Security #2944: ssh: heap buffer overflow (master) Closed

### History

#### #1 - 04/30/2019 08:23 AM - Victor Julien
- Copied to Security #2944: ssh: heap buffer overflow (master) added

#### #2 - 04/30/2019 12:30 PM - Victor Julien
- Status changed from Assigned to Closed

https://github.com/OISF/suricata/releases/tag/suricata-4.1.4

#### #3 - 04/30/2019 12:55 PM - Victor Julien
- Private changed from Yes to No

#### #4 - 09/01/2020 09:32 AM - Victor Julien
- Tracker changed from Bug to Security
- CVE set to 2019-10053
- Git IDs updated