Suricata - Security #5023
smtp: GetLine function buffers data indefinitely if 0x0a was not found in the frag'd input
01/31/2022 11:58 AM - Shivani Bhardwaj

Status: Closed
Priority: Normal
Assignee: Shivani Bhardwaj
Category: 
Target version: 7.0.0-beta1

Affected Versions:

Git IDs:
57a7cf7a0bcc9140a326c91a21e5d21fd2
236f49
078c251deacc78b8abb40c5ab89d19c29
e31bd8
cf749fd450ca41dc001c2a1c10d8d17500
dcedce
6e800a8548d9d2699589cac6afca3c0fa7
613202
e7417a8e96fcd23fa9e3b529d7c2bb7b3
ebf928

Label:
CVE:

Severity: HIGH

Description
The code we tend to execute is

SCReturnStruct(APP_LAYER_INCOMPLETE(state->consumed, state->input_len + 1));

indefinitely.

Related issues:
Copied to Security #5027: smtp: GetLine function buffers data indefinitely if...
Closed
Copied to Security #5028: smtp: GetLine function buffers data indefinitely if...
Closed

History
#1 - 01/31/2022 12:00 PM - Shivani Bhardwaj
- Description updated

#2 - 01/31/2022 12:03 PM - Shivani Bhardwaj
- Copied to Security #5027: smtp: GetLine function buffers data indefinitely if 0x0a was not found in the frag'd input added

#3 - 01/31/2022 12:04 PM - Shivani Bhardwaj
- Copied to Security #5028: smtp: GetLine function buffers data indefinitely if 0x0a was not found in the frag'd input added

#4 - 04/16/2022 05:11 AM - Victor Julien
- Tracker changed from Bug to Security
- Severity set to HIGH

#5 - 04/19/2022 06:07 PM - Shivani Bhardwaj
- Status changed from Assigned to In Review

#6 - 04/22/2022 12:26 PM - Victor Julien
- Status changed from In Review to Closed
- Git IDs updated

#7 - 12/15/2022 11:21 AM - Victor Julien
- Private changed from Yes to No
- Label deleted (Needs backport to 5.0, Needs backport to 6.0)