Suricata - Bug #3650
FTP response buffering against TCP stream
04/15/2020 05:52 PM - Jeff Lucovsky

Status: Closed
Priority: Normal
Assignee: Victor Julien
Category:
Target version: 4.1.8
Affected Versions: 4.1.7
Effort:

Description
Now, Suricata parses FTP response packets as if they are always complete. This is not the TCP logic of streaming. We have to keep buffering until the response is complete, and we can parse multiple responses in one TCP stream in one time.

Found by running suricata-verify tests while doing TCP stream splitting

Fix proposed https://github.com/OISF/suricata/pull/4789

Related issues:
Copied from Bug #3631: FTP response buffering against TCP stream

History
#1 - 04/15/2020 05:52 PM - Jeff Lucovsky
- Copied from Bug #3631: FTP response buffering against TCP stream added

#2 - 04/16/2020 12:55 PM - Shivani Bhardwaj
- Priority changed from Normal to Immediate

#3 - 04/26/2020 06:17 PM - Victor Julien
- Assignee changed from Shivani Bhardwaj to Victor Julien
- Priority changed from Immediate to High
- Affected Versions 4.1.7 added
- Affected Versions deleted (5.0.2)

#4 - 04/27/2020 06:47 PM - Victor Julien
- Status changed from Assigned to Closed
- Priority changed from High to Normal

https://github.com/OISF/suricata/pull/4891