Flow reference count is incremented twice, leading to memory and flow bucket leaks

11/30/2012 08:49 PM - Ludovico Cavedon

Status: Closed
Priority: High
Assignee: Ludovico Cavedon
Category:
Target version: 1.3.5
Affected Versions:
Effort:
Difficulty:
Label:

Description
The reference count of flows is sometimes incremented twice in the current stable release of suricata 1.3.4, once by FlowReference(), once by FlowIncrUsecnt()

See https://github.com/cavedon/suricata/commit/49d6d4d8d672c51ee4c465c5cecf0c903af70e3 for the fix.

This does not affect the current master branch.

This looks like a major issue because flow buckets are leaked until no more buckets can be freed and suricata stalls at 100% CPU usage iterating over all flow buckets.

History
#1 - 11/30/2012 08:50 PM - Ludovico Cavedon
Pull request https://github.com/inliniac/suricata/pull/232

#2 - 12/03/2012 05:39 AM - Victor Julien
- Status changed from New to Closed
- Assignee set to Ludovico Cavedon
- % Done changed from 0 to 100

Great catch, thanks!
Merged pr/232.